Teleport

Implementing Zero Trust Security for AWS Infrastructure with Teleport

White Paper

Contents

© 2025 Gravitational Inc.; all rights reserved.

Scaling Your Infrastructure from On-premises to the AWS Cloud

The shift from monolithic on-premises architecture to independent microservices has opened a world of innovation and opportunity for organizations in virtually every industry. However, it can also create complex, siloed environments that can be challenging to manage, allowing bad actors to exploit attack surfaces.

Since the applications and workloads being migrated and managed in the cloud are not cloud-native, the Infrastructure and DevOps teams may need to manage many accounts, users, and roles. To compound the challenge, organizations often work with several system integrators (SIs) to help them migrate and manage their cloud deployments. This increases the complexity of maintaining the security and compliance of these workloads, especially when they are spread across multiple AWS accounts.

Additionally, organizations may not have the skill sets to consolidate multiple accounts for workload migrations or application modernization. To combat these issues, it is common to see enterprises engage AWS Partners to help them with long-term, strategic initiatives and day-to-day DevOps activities.

To manage infrastructure and workloads, organizations need a repeatable process for provisioning and de-provisioning access while providing only the necessary permissions for people to complete their tasks. To manage infrastructure and workloads, teams need a solution that provides just-in-time (JIT) privilege escalation based on each user's identity and access requirements.

Organizations can solve these challenges by implementing zero trust, a methodology that requires every user, device, application, and transaction to be verified first, even if the request comes from your corporate network (VPN) or virtual private cloud (VPC).

Create a Secure Way to Protect Infrastructure with Zero Trust

Zero trust's architecture involves authenticating and authorizing users and processes at every resource level. If an identity has met a base authentication for one resource, it doesn't mean that all subsequent resource requests should be allowed. Access must be valdated at each resource. NIST zero trust tenants include :

- All network traffic must be untrusted.
- Verify and secure all resources.
- Limit and strictly enforce access control.
- Inspect and log all network traffic.

DevOps teams face many challenges when implementing zero trust, including the abundance of user identities, the reliance on third-party SaaS apps, and the rise of hybrid cloud, multi-cloud, and edge computing.

© 2025 Gravitational Inc.; all rights reserved.

When implementing zero trust, many DevOps teams start with an Identity-Aware Proxy (IAP) that acts as the central nervous system of a zero trust architecture. This replaces traditional VPN-based access control mechanisms with a modern, context and identity-aware authentication and authorization approach. Instead of defining access policies per resource—such as a server, Kubernetes cluster, or application—an IAP centralizes the policy definitions and access control by mapping the identities registered with each resource. This puts DevOps teams in a better position to implement zero trust security.

Teleport integrates seamlessly with AWS to simplify the implementation of zero trust in the cloud, aligning the core principles of zero trust to provide improved security and access control.

Protect Infrastructure Through Zero Trust with Teleport

The Teleport Infrastructure Identity Platform implements trusted computing at scale, with unified cryptographic identities for humans, machines and workloads, endpoints, infrastructure assets, and AI agents. Our identity-everywhere approach vertically integrates access management, zero trust networking, identity governance, and identity security into a single platform, eliminating overhead and operational silos.

Teleport supports the broadest range of protocols and resources, including servers, databases, workloads, clouds, Kubernetes, and more. It scales from the individual engineer to the largest organization, with global data centers that ensure redundancy, fault tolerance, and low latency. The Teleport Infrastructure Identity Platform is a proven technology adopted by more than 500 organizations worldwide.

Secretless as the Future of Identity Management with Teleport

The Teleport Infrastructure Identity Platform delivers on-demand, least-privileged access to infrastructure based on cryptographic identity and zero trust, with built-in identity security and policy governance. Teleport's platform helps DevOps teams increase productivity while creating an environment more resilient to bad actors or human error security threats and empowers fast, accurate compliance reporting. Teleport goes beyond removing usernames and passwords to removing keys and other secret data, setting the foundation for a truly secretless zero trust environment.

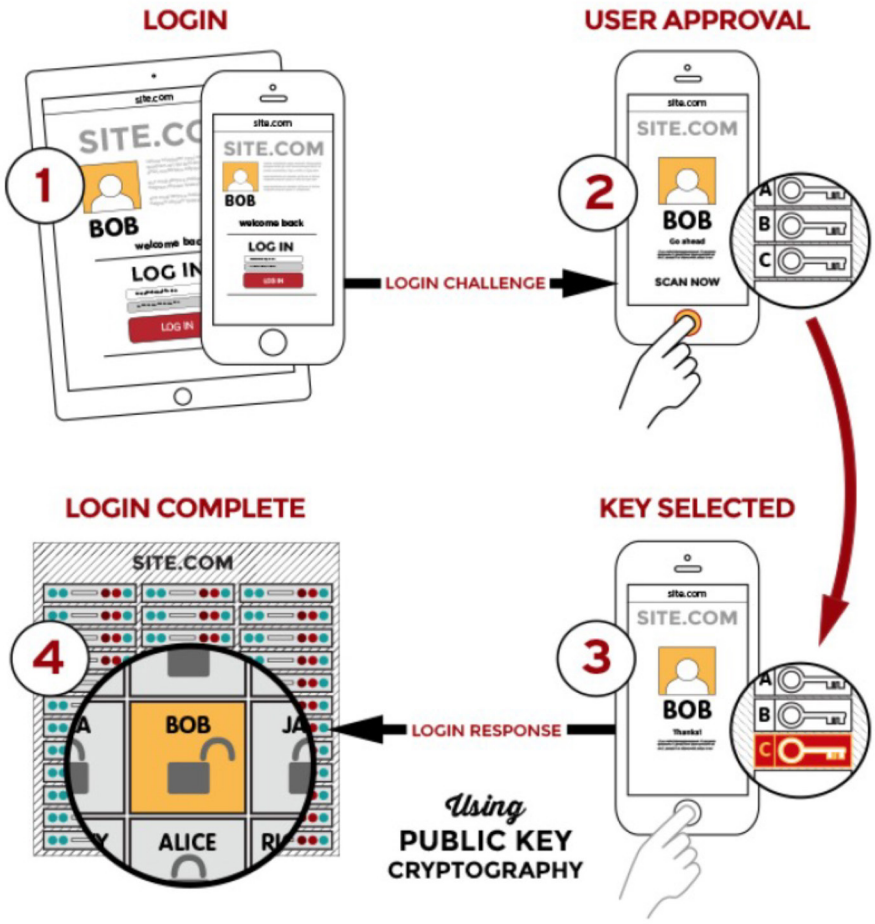
Team members get access to what they need when they need it, such as dynamic resource cataloging and effortless JIT access. They also benefit from short-lived certificates bound to biometric devices and enclaves that make the authentication process easier and more secure.

© 2024 Gravitational Inc.; all rights reserved.

FIDO Alliance

Teleport joined the FIDO Alliance to bring this improved mix of security and usability to infrastructure resources like Linux and Windows servers, databases, Kubernetes clusters, and internal applications.

Instead of storing credentials and secrets in a vault or a secure database, which is the old-school way of providing access, FIDO promotes standards based on a combination of biometric authentication and private keys that never leave secure enclaves of associated devices such as mobile phones and notebook PCs with biometric authentication.



Passwordless access based on FIDO

AWS customers using Teleport can authenticate themselves through YubiKey, Apple's Touch ID, Face ID, and Windows Hello. The Teleport Infrastructure Identity Platform manages the mapping between biometric-authenticated and target users through the sophisticated role-based access control (RBAC) engine.

To learn more about Teleport's secrets access, refer to the technical read our technical blog post.

© 2025 Gravitational Inc.; all rights reserved.

Teleport on AWS Creates a Strong Security Posture for IT Environments

Teleport provides an identity-native and context-aware access proxy designed to work seamlessly with AWS. The Teleport Infrastructure Identity Platform becomes a centralized and a single entry point for consuming various AWS services, allowing internal and external users to use it.

Teleport is tightly integrated with mainstream services such as AWS Identity and Access Management (AWS IAM), Amazon Elastic Cloud Compute (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), and Amazon Elastic Kubernetes Service (Amazon EKS). When users access these services through Teleport, they automatically comply with the policies defined by admins. Teleport closely integrates with the AWS Management Console, SDK, and AWS Command Line Interface (AWS CLI), allowing these policies to work consistently, regardless of how users access the services.

When using Teleport to centralize access to AWS, organizations get:

- **Fine-grained control of each AWS service** - DevOps teams can define precise access policies based on the user persona. For example, internal employees will get read/write access to an Amazon S3 bucket, while contractors can only read the objects in a bucket. Similarly, users can be restricted to dev/test Amazon EC2 instances while limiting access to production servers.

Teleport seamlessly works with these AWS services and many more

© 2024 Gravitational Inc.; all rights reserved.

- **Consistent and frictionless experience using AWS Management Console and AWS CLI** - Teleport delivers a consistent and frictionless experience using the AWS Management Console and AWS CLI tools based on the AWS IAM and identity federation. Users can continue to use tools they are familiar with to access AWS while complying with the policies defined by DevOps.
- **Simplified RBAC** - Teleport's RBAC is a simple yet powerful policy enforcement mechanism. By mentioning the AWS role ARNs, Teleport administrators can define fine-grained policies to allow or restrict access to various services. The same roles can be extended to manage access for Linux and Windows Amazon EC2 instances, Amazon EKS clusters, Databases such as Amazon RDS, Amazon Aurora, Amazon Redshift, Amazon ElastiCache, Amazon MemoryDB and Amazon DynamoDB, AWS Management Console and AWS CLI, and other DevOps services running on AWS such as Grafana and Kibana.
- **JIT elevated privileges** - One of the most powerful features of the Teleport Infrastructure Identity Platform is the ability to perform JIT privilege escalation. A contractor with read-only access to a production server can be given temporary, time-bound access to perform an upgrade. Integration with notification tools such as Slack and PagerDuty allows Teleport administrators to receive alerts and approve or reject privilege escalation requests.
- **Insights through AWS CloudTrail and Teleport Audit** - Teleport supports logging events directly to AWS CloudTrail. Federated login sessions are recorded in AWS CloudTrail and can be easily searched based on a Teleport or federated username. Apart from this, Teleport can be configured to log all events to Amazon DynamoDB for performing audit trails. Amazon EC2 SSH sessions are recorded in Amazon S3 buckets for playback and review.

Securing Access to AWS Management Console and AWS CLI

Secure application access is one of Teleport's key features. The Teleport Infrastructure Identity Platform protects any HTTP endpoint, such as a web application or an API. With Teleport, any private, internal web application can be securely exposed to users with full authentication and authorization even outside the corporate network or a private subnet of an Amazon Virtual Private Cloud (Amazon VPC).

Internal control panels, wikis, infrastructure dashboards, such as Lens or Grafana, and developer tools like Jenkins, GitLab, or Opsgenie are great candidates for Teleport. Teleport can also be leveraged to secure AWS Management Console access by defining application access policies.

Since the AWS Management Console is accessible through an HTTP(S) URL, it can be registered with the Teleport application agent like any other web application.

Teleport enables DevOps and engineering teams to generate custom URLs for each AWS IAM user who needs access to the management console. Users can seamlessly and automatically sign into the AWS Management Console with appropriate AWS IAM roles without explicitly entering the credentials.

Teleport uses AWS federation to generate user sign-in URLs, which relies on the AWS IAM API to get temporary security credentials. Users automatically assume the correct role associated with their identity by defining Teleport RBAC policies based on the AWS IAM roles.

© 2025 Gravitational Inc.; all rights reserved.

Teleport not only secures access to the AWS Management Console, but it can also extend it to the command line tool used by operators to automate tasks. As an identity-aware proxy, Teleport authenticates and authorizes identities based on fine-grained policies that allow or restrict access to AWS API endpoints. For example, some users may be allowed to access Amazon S3 service while restricting access to any operation targeting Amazon EC2.

Using Teleport in conjunction with the AWS Management Console and AWS CLI provides a highly efficient access control mechanism that goes beyond the IAM capabilities of AWS.

To learn more, refer to the documentation for a step-by-step guide on accessing AWS with Teleport Application Access.

Securing Amazon EC2 Instances

Amazon EC2 is one of the core building blocks of the AWS Cloud, empowering enterprises to provision Amazon EC2 instances to run diverse workloads ranging from public-facing web applications to microservices to internal line-of-business applications.

Amazon EC2 is built on the virtual networking environment called Amazon VPC. This software-defined network layer enables enterprises to create isolated network segments as a subnet. Internet-facing applications running in Amazon EC2 instances are typically provisioned in a public subnet, while Amazon EC2 instances running internal applications and sensitive workloads are launched within a private subnet.

To access the Amazon EC2 instances running in the private subnet, DevOps engineers often provision a bastion host that acts as a secure conduit between the public and private subnets. Adding specific IP addresses and SSH keys to an allowed list restricts access to the bastion host to a select group of engineers.

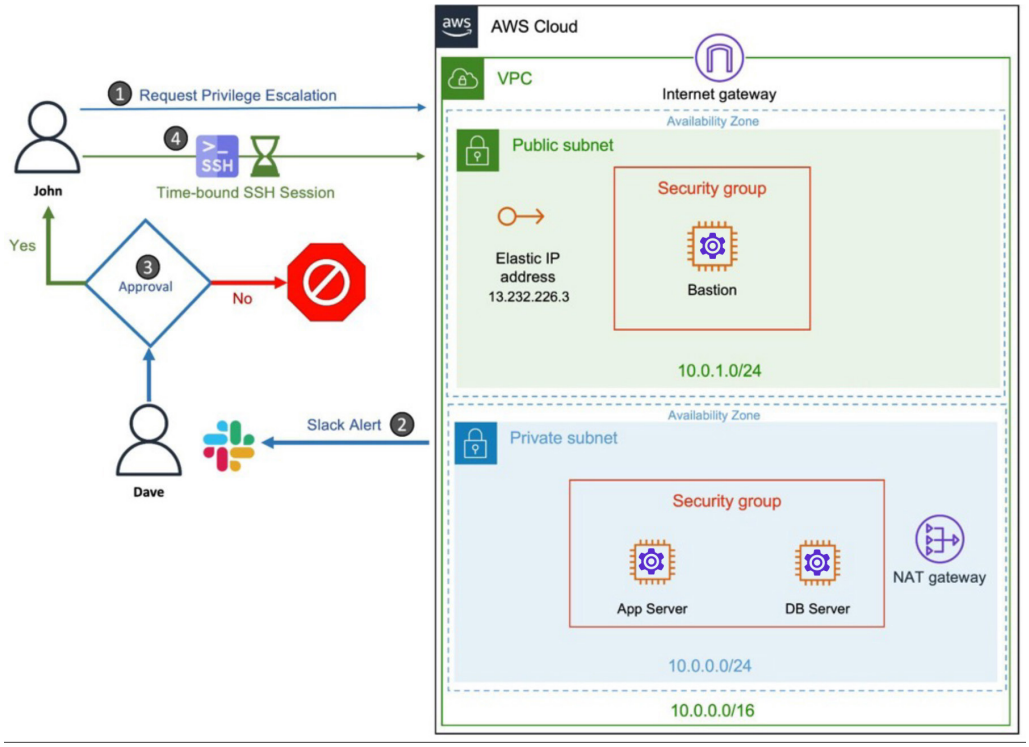
Teleport replaces the traditional bastion host as a secure and sophisticated access platform. With its identity-native access proxy, Teleport makes it possible to map existing identities with individual Linux users configured within the Amazon EC2 instances. This approach brings benefits such as fine-grained RBAC and detailed audit trails.

The first of two core components, the Teleport Infrastructure Identity Platform's access proxy, has authentication and proxy components responsible for tunneling the sessions to each registered agent. Second, each Amazon EC2 instance provisioned within the private subnet runs the Teleport agent, which communicates with the access proxy. The Teleport Infrastructure Identity Platform provides a secure alternative to the traditional bastion host by combining the centralized access proxy and the agent.

User identities within the corporate LDAP directory or an external SSO provider can be configured with Teleport to define secure access control policies. When a user logs into the Teleport Infrastructure Identity Platform, a dynamic policy is enforced allowing or restricting the user's access to one or more Amazon EC2 instances. Teleport logs all users' actions when logging into the access platform. SSH sessions are recorded as video files that can be played back to review the commands executed by individual users.

© 2025 Gravitational Inc.; all rights reserved.

Teleport supports the JIT escalation of privileges, making it possible to give users elevated rights temporarily. This is particularly helpful in scenarios where a third-party DevOps engineer will have to assume a role to perform maintenance tasks that demand root access or elevated rights. Consultants can request elevated permissions, which are sent to the approver through a messaging application such as Slack or PagerDuty. Once approved, the temporarily elevated privileges automatically expire based on a predefined time window.



Workflow for configuring JIT privilege escalation for Amazon EC2

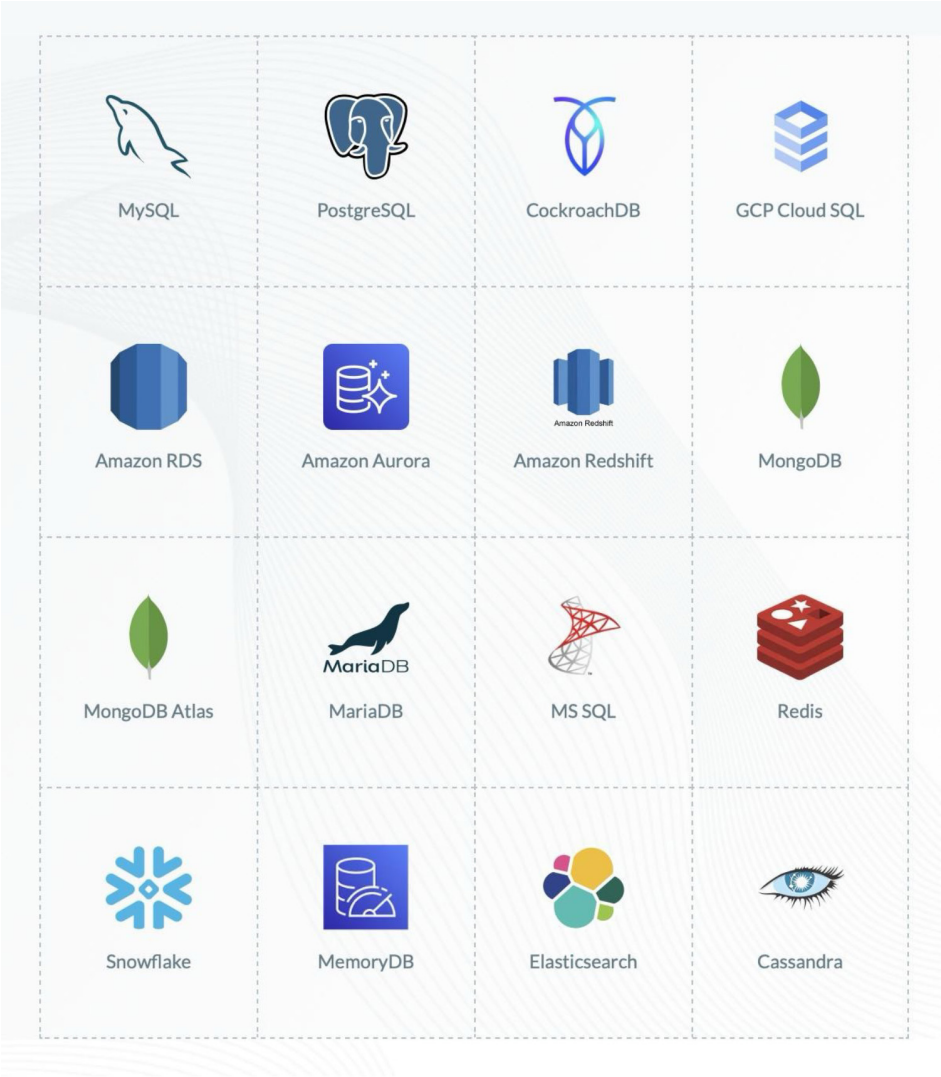
For a detailed walkthrough of the configuration of a secure bastion host based on Teleport, please refer to our series on securing Amazon EC2 infrastructure.

© 2025 Gravitational Inc.; all rights reserved.

Securing Database Access on AWS

Databases store sensitive information that needs an additional layer of protection and security. Traditional database servers have built-in authentication and authorization mechanisms but are not designed for cloud-based, multi-tenant access mechanisms. As a leading cloud provider, AWS offers over 15 purpose-built database engines, including relational, key-value, document, in-memory, graph, time series, wide column, and ledger databases. These managed databases are accessed and administered by different personas requiring varying levels of access permissions. To provide secure access to these databases in AWS, organizations need robust, fine-grained RBAC.

Whether enterprises consume them as a service or host them on Amazon EC2, AWS supports multiple flavors, and Teleport's database agent can be configured to support the diverse range of databases on AWS.



Sample of databases supported by Teleport

© 2025 Gravitational Inc.; all rights reserved.

Using an identity-native access proxy like Teleport, enterprises can apply industry best practices for database access with identity-native SSO, short-lived certificates for users or service accounts, multi-factor authentication, RBAC, and audit for all databases across all environments.

Like Amazon EC2, enterprises can securely provide access to several databases hosted on AWS launched in a private subnet of a VPC. Each user configured within the database instance can be mapped to an external identity whose access control is governed by Teleport.

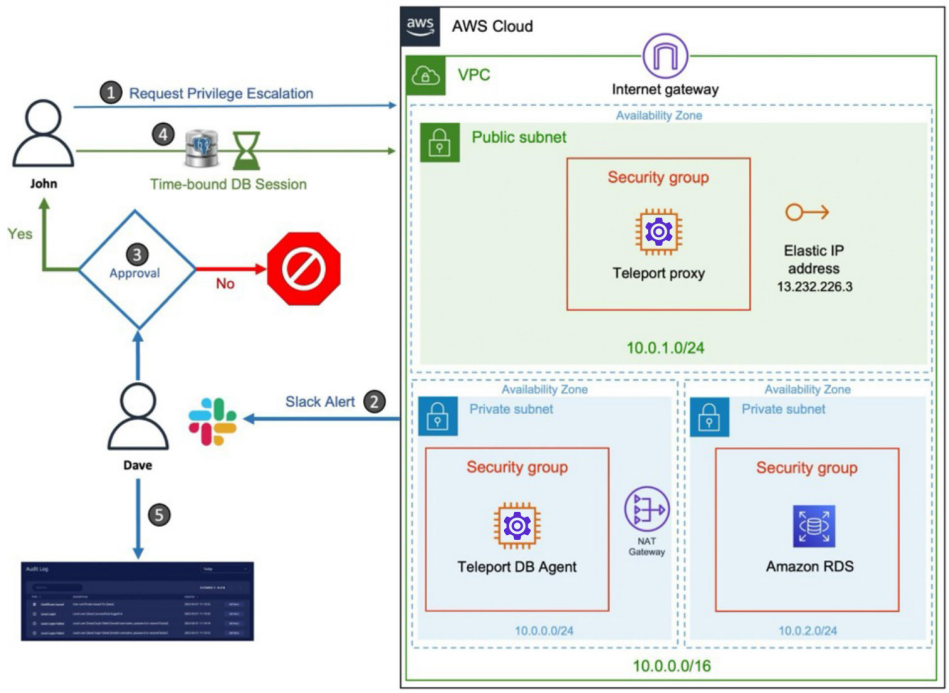
The key advantages of using Teleport to secure databases on AWS are:

- **Identity-native access** - Enforces the use of cryptographically validated identity for users and applications, removing the top attack vector: passwords and secrets.
- **Access requests** - Enables just-in-time privilege escalation for administrative tasks without having to maintain long-standing administrative or root access.
- **Single source of truth for access** - Centralizes access policy across AWS and your infrastructure to eliminate attack vectors and enforce RBAC.

The same Teleport Infrastructure Identity Platform used to manage access to Amazon EC2 can be utilized to secure your database instances on AWS. A Teleport database agent manages the communication between users and applications with the target database server.

Similar to the workflow explained in the Amazon EC2 section, Teleport can provide temporary access to database instances on AWS, whether self-hosted or consumed as an AWS service.

[Taken from the section above: “Refer to the documentation for a step-by-step guide on accessing AWS with Teleport Application Access.”]



Configuring JIT privilege escalation for database access in AWS

© 2025 Gravitational Inc.; all rights reserved.

Securing Access to Amazon EKS

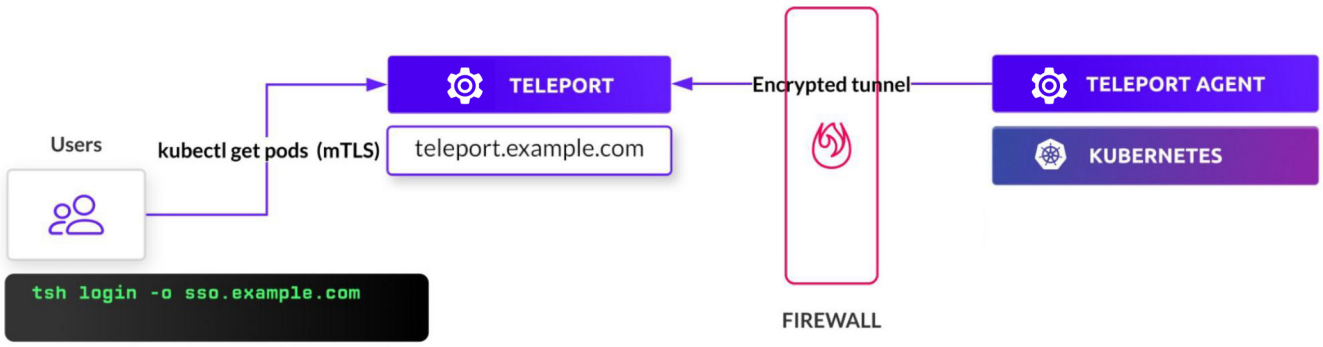
Enterprises are embracing the cloud-native paradigm for agility, scalability, composability, and portability. Kubernetes, the open-source container orchestration engine, is the foundation of modern, cloud-native workloads. AWS customers can leverage managed Kubernetes, available as Amazon EKS, or deploy a cluster based on upstream Kubernetes distribution running in a set of Amazon EC2 instances. Irrespective of how Kubernetes is deployed, securing access to the clusters is critical.

Amazon EKS is a managed Kubernetes service that runs Kubernetes in the cloud and on-premises data centers. In the cloud, Amazon EKS automatically manages the availability and scalability of the Kubernetes control platform nodes responsible for scheduling containers, managing application availability, storing cluster data, and other key tasks.

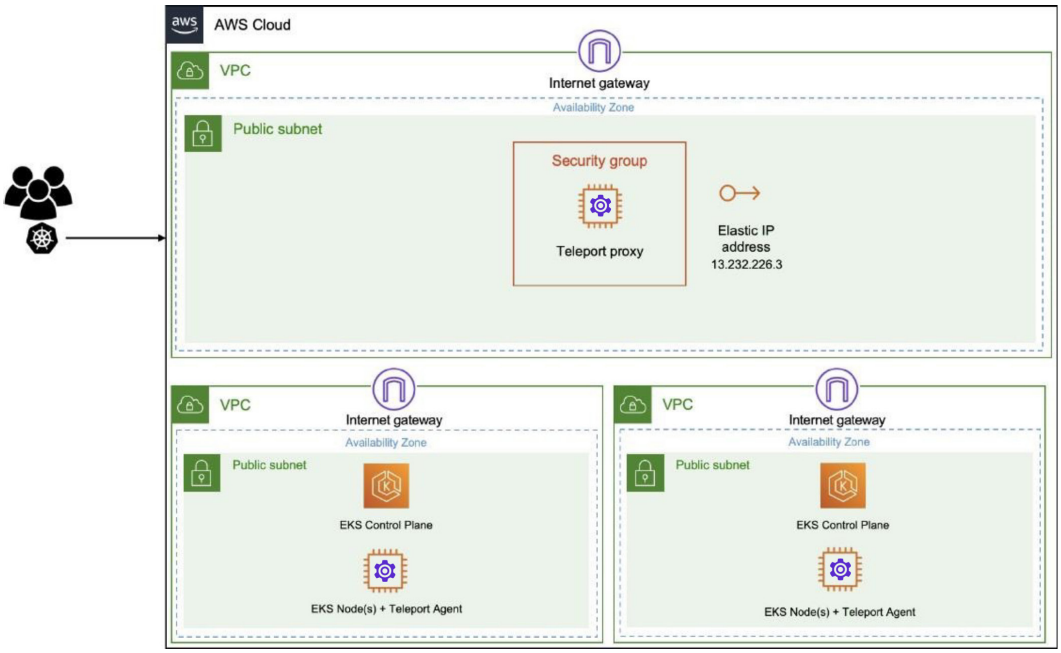
Enterprises commonly run multiple Kubernetes clusters dedicated to the development, staging, testing, and production environments. With the introduction of Amazon EKS Anywhere, enterprises can deploy Amazon EKS clusters within their data centers. They need consistent, secure, and reliable access to the Kubernetes clusters running in the public cloud and hybrid environments.

With an identity-native access platform like Teleport, enterprises can effectively manage the per-cluster policy by allowing or restricting access to individual clusters based on user persona or job function.

Enterprises can deploy the Teleport agent, available as a Helm chart, to secure the Kubernetes clusters. This agent is responsible for communicating with the Teleport Infrastructure Identity Platform running, which manages access control of other Amazon EC2 instances and databases.

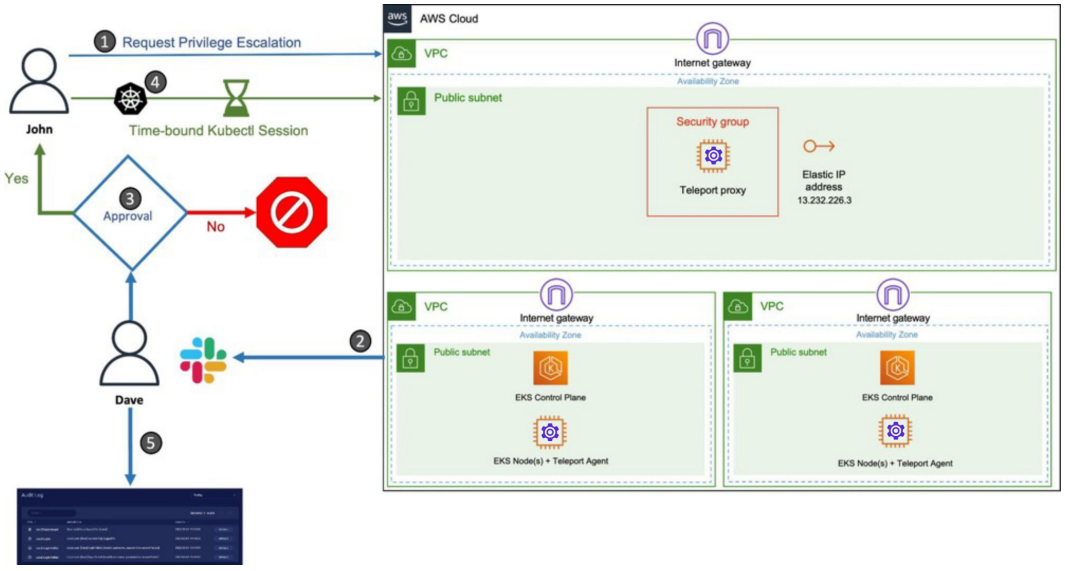


© 2025 Gravitational Inc.; all rights reserved.



Teleport integrates with Kubernetes service accounts and RBAC to provide unified access control. Developers and operators continue to use familiar command line tools such as Kubectl to access Kubernetes clusters. Behind the scenes, Teleport enforces appropriate access controls based on the identity of the users.

Managers can approve or reject requests to access clusters based on the identities and roles of the users. The diagram below depicts the workflow of a user requesting temporary access to a production Amazon EKS cluster running within Amazon VPC.



Workflow for configuring JIT privilege escalation for Amazon EKS

For a detailed walkthrough of the configuration of securing Amazon RDS with Teleport, please refer to our series on securing Amazon EKS infrastructure.

© 2025 Gravitational Inc.; all rights reserved.

Achieve Modern, Identity-first Infrastructure with Teleport on AWS

Enterprises in virtually every industry depend on AWS for their business-critical applications; protecting them from potential attacks requires moving beyond typical security approaches, such as using a bastion host or allowing IP addresses to control access. With Teleport, DevOps teams can seamlessly secure their AWS services using a zero trust, identity-native approach that increases security and improves developer productivity. Through AWS IAM, Teleport's users and roles can be directly mapped to AWS IAM roles.

With Teleport, organizations reduce friction for engineers, harden security with trusted identities and ephemeral, zero trust access, and streamline compliance, enabling organizations to pass audits with flying colors. Teleport eliminates access complexity, enabling engineers to stay focused on time to market instead of juggling credentials, SSH keys, and a myriad of access paths.

Contact the Teleport Sales Team

© 2025 Gravitational Inc.; all rights reserved.