
AWS
re:Invent

ANT316

Security overview for Amazon Elasticsearch Service

Carl Meadows

Senior Manager, Product Management

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common security problems with Elasticsearch

- Open source Elasticsearch has no security layer (Authn or Authz)
- Proxies and network controls are commonly used (or not)
- Does not meet audit and security compliance standards
- No logging of user actions and API access





Amazon Elasticsearch Service (Amazon ES)

Fully managed service that makes it easy to deploy, manage, and run Elasticsearch cost effectively with industry-leading reliability, scalability, and security. Powered by Open Distro for Elasticsearch.



Open Distro for Elasticsearch

100% Apache licensed, open-source distribution of Elasticsearch with plugins to deploy a secure, performant, Elasticsearch cluster. Created and supported by AWS.

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Full-text search applications

You want effective, natural-language-based search on your application data

Observability or log and security analytics

You want real-time monitoring for your infrastructure, security, application performance, and product / feature performance

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security in Amazon Elasticsearch Service

Access

Protect data with network security and encryption

Authentication

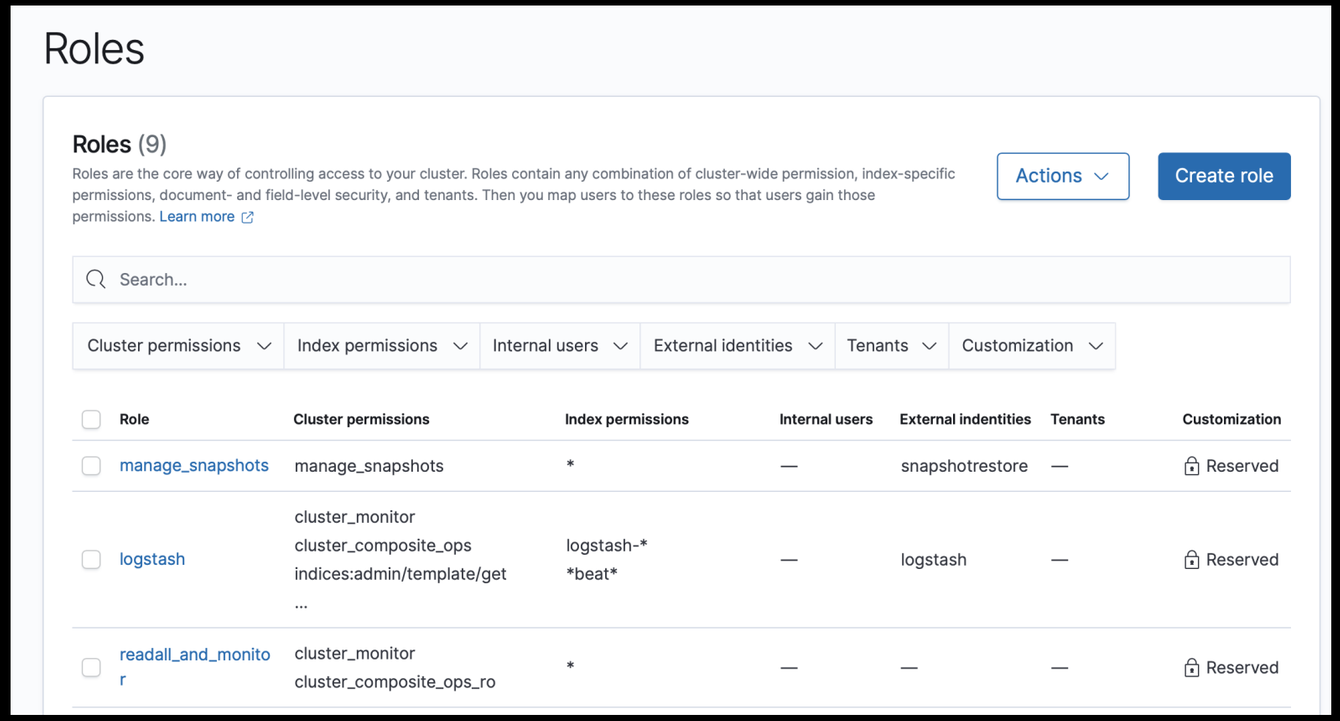
Define users; leverage your existing auth infrastructure

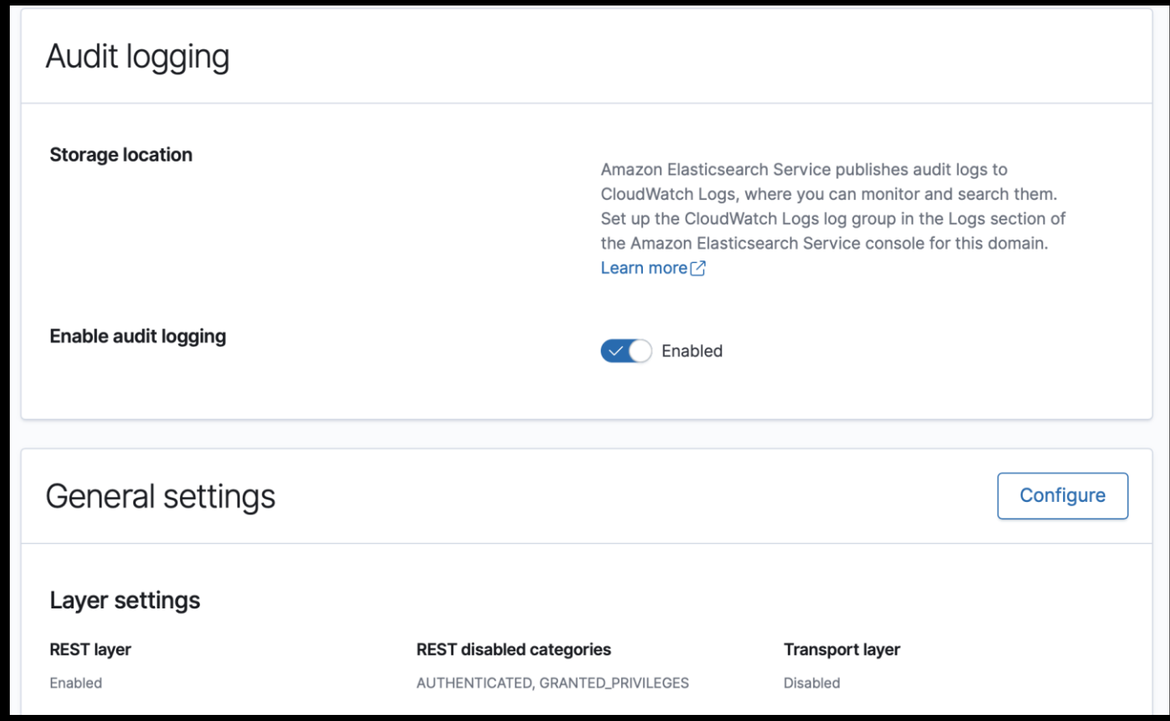
Authorization

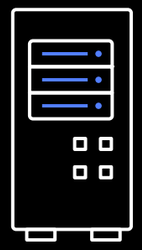
Granular access control to control user actions on your cluster

Audit

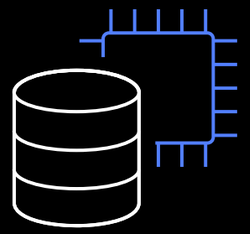
Detailed logging of data access for compliance and security incident response



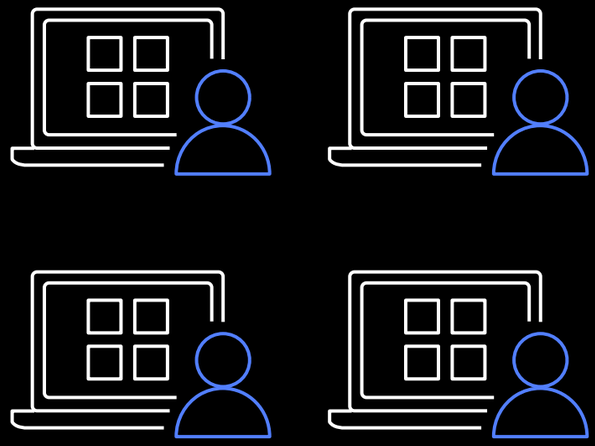




Server, application, network, AWS, and other logs

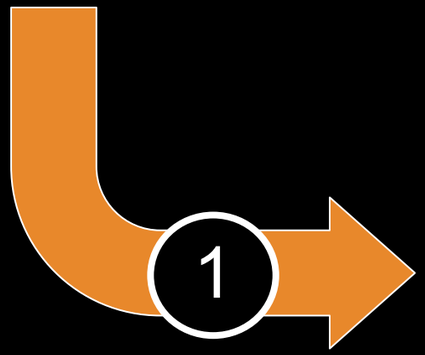


Application data



Application users, analysts, DevOps, and security

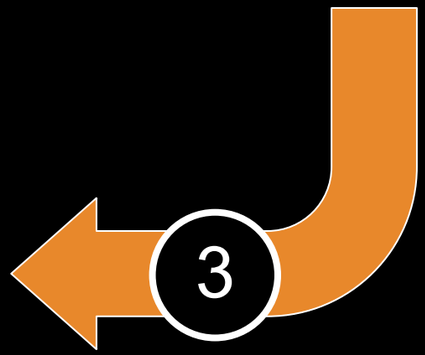
Indexed and instantly searchable



JSON documents



Amazon Elasticsearch Service Domain with index(es)



Rest APIs, clients, and Kibana

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Search, analyze, and visualize log data



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security features on Amazon ES

- Public or VPC endpoints with IAM controlled edge resource policy
- AWS CloudTrail logging of all Amazon ES configuration API calls
- Encryption in flight with minimum TLS version
- Encryption at rest with KMS and customer supplied keys
- Compliance program for PCI, HIPAA, SOC, FedRAMP, ISO, and more
- IAM authentication into Elasticsearch
- Kibana Auth via **SAML / ADFS** and Amazon Cognito
- Basic Auth (username / password)
- Fine-grained access control (index, operation, field, document)
- Kibana multi-tenancy support
- Friendly domain name with AWS Certificate Manager (ACM) integration
- Elasticsearch API audit logging

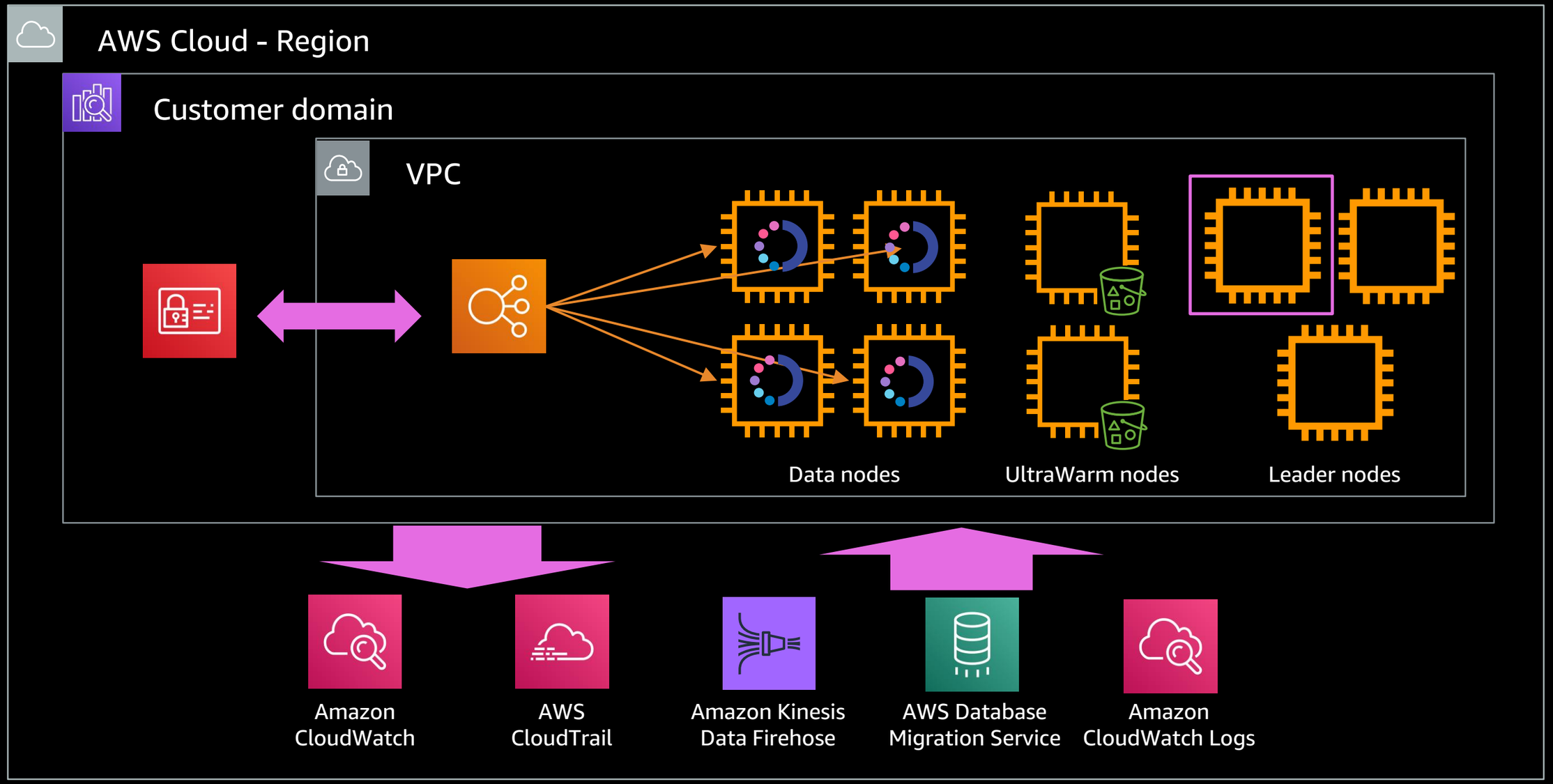




New in 2020

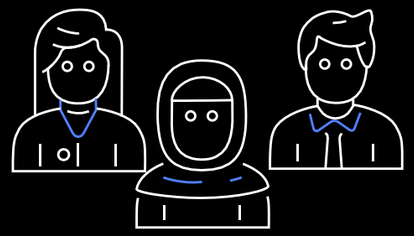
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ES deployment architecture



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon ES security core concepts



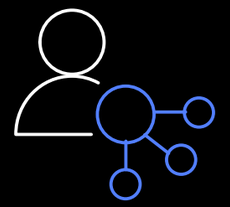
Users

Users are principals who make requests to Elasticsearch clusters; a user has credentials



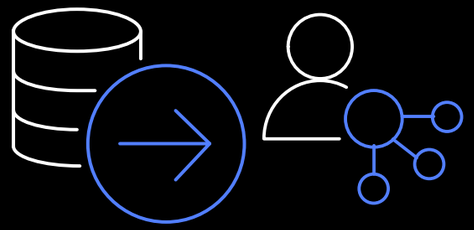
Permissions

Assign individual permissions or a group of permissions, such as creating an index (e.g., indices:admin/create)



Roles

Security roles define the scope of a set of permissions: cluster, index, document, or field



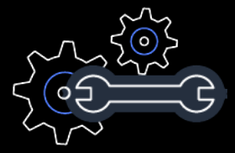
Backend roles

Additional, external roles that come from an authorization backend (e.g., SAML, IAM, ADFS)



Role mappings

Users assume roles after they successfully authenticate; role mappings map roles to users (or backend roles)



Multi-tenancy

Allow sharing of data, visualizations, and dashboards between users/roles belonging to same tenant

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multilayer authentication

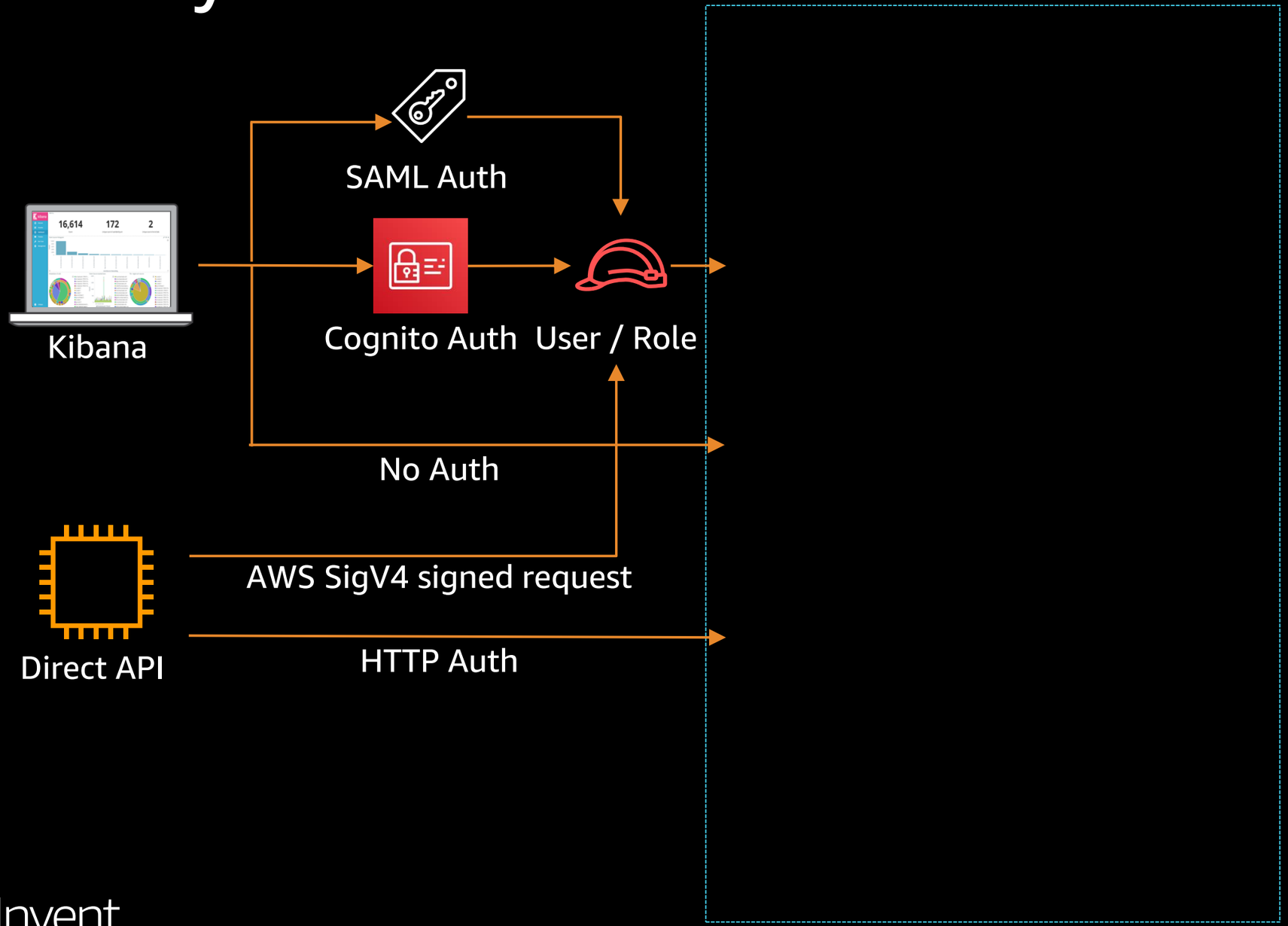


Kibana

Direct API

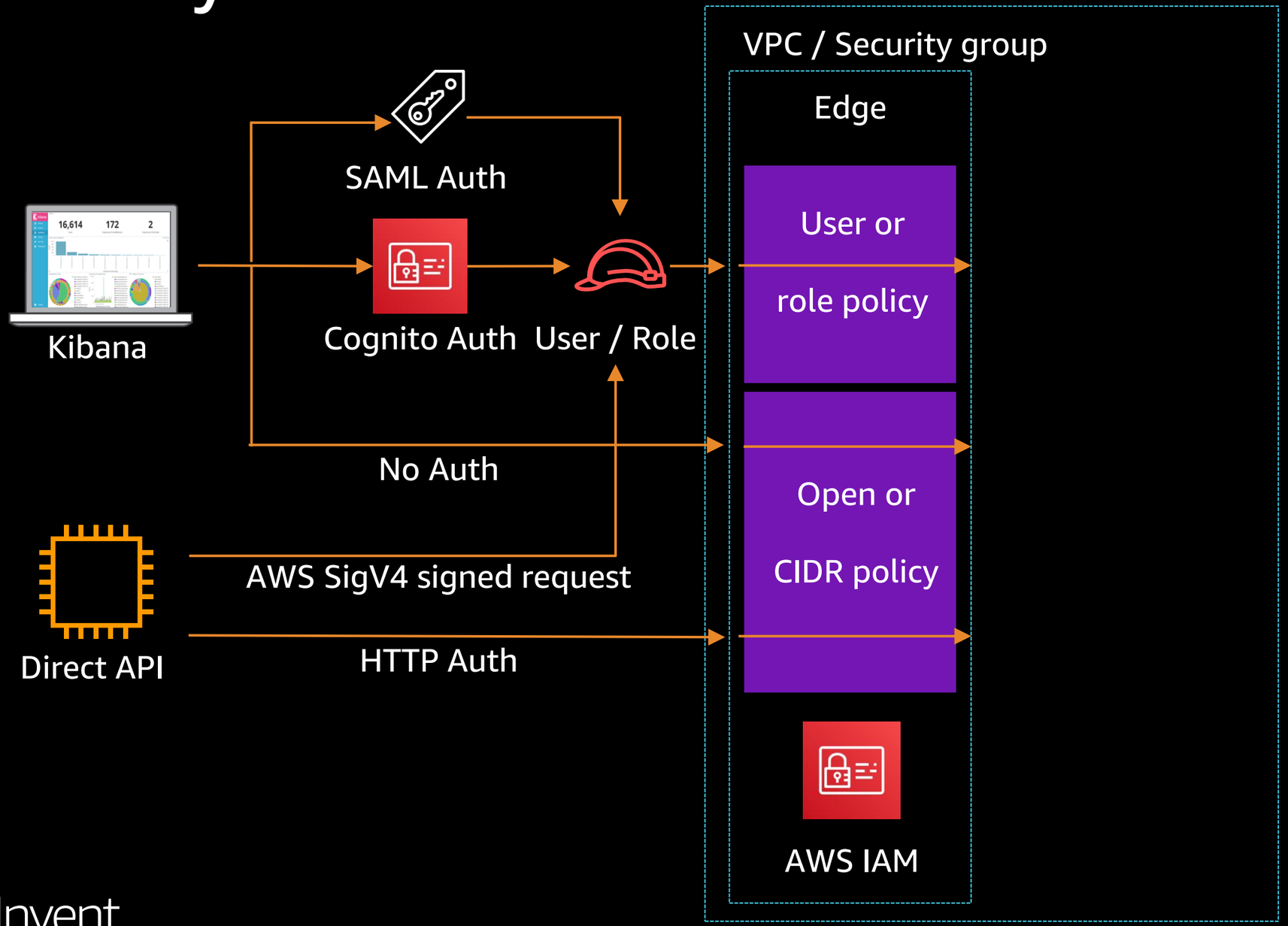
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multilayer authentication



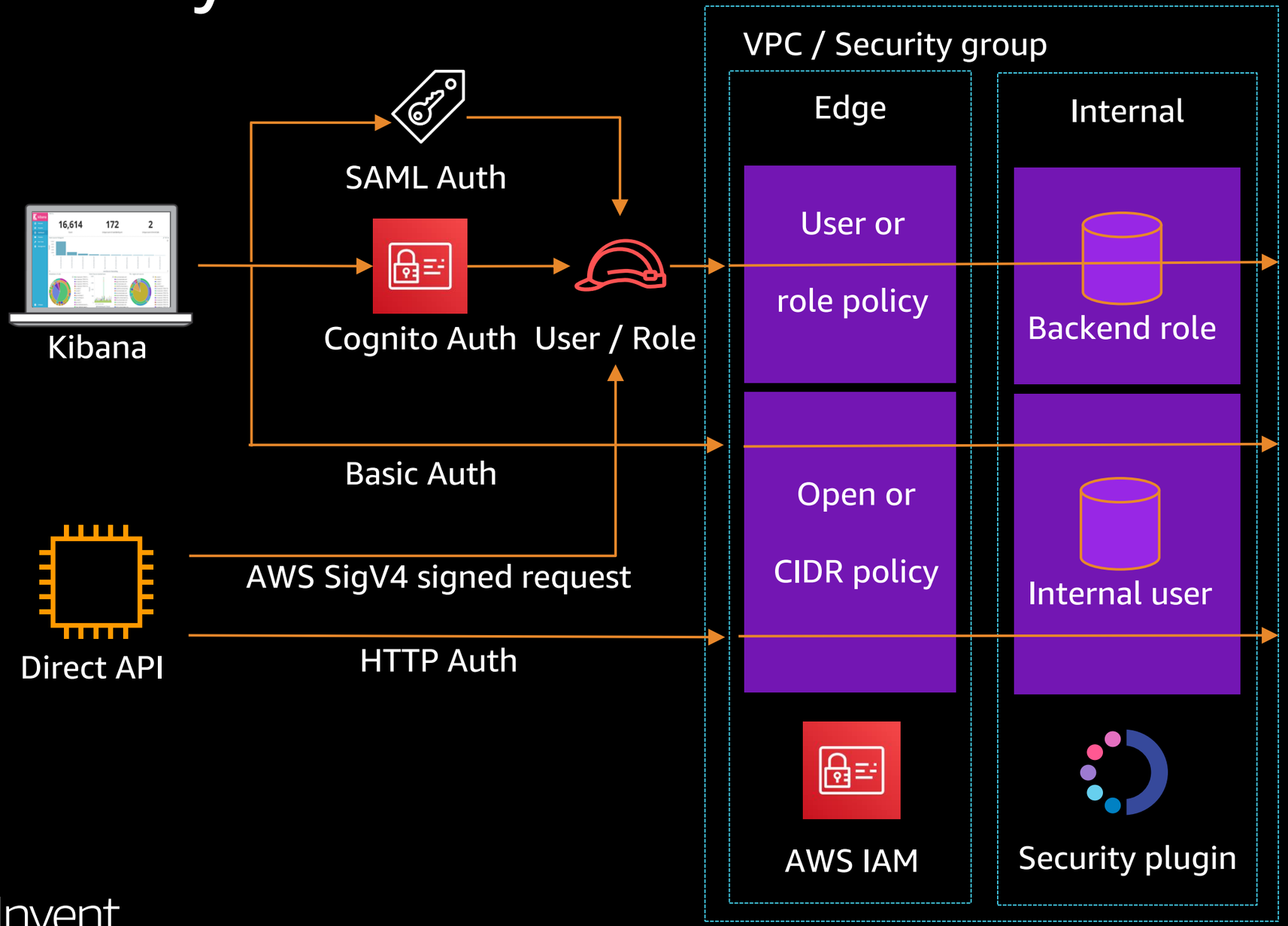
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multilayer authentication



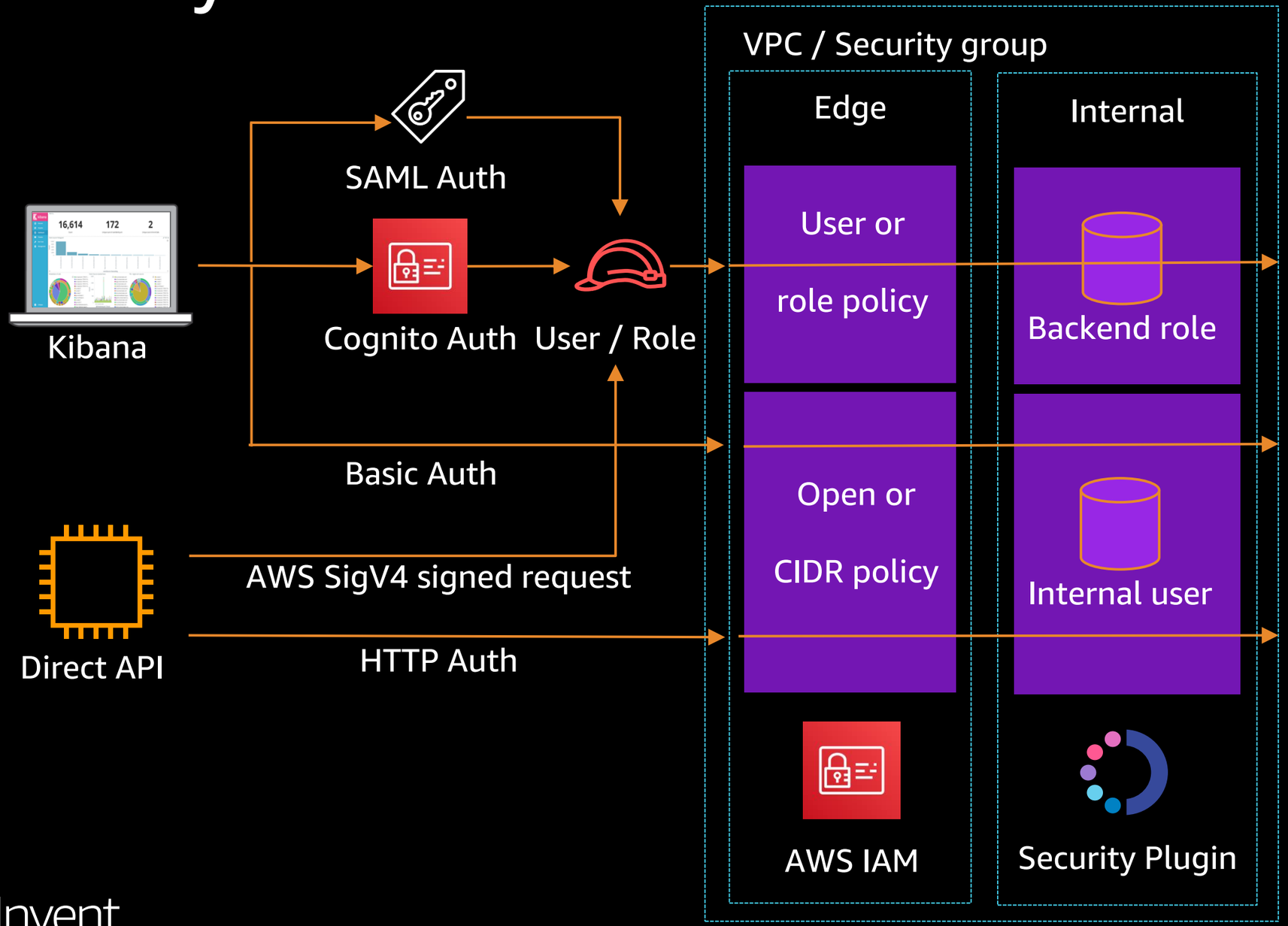
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multilayer authentication



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

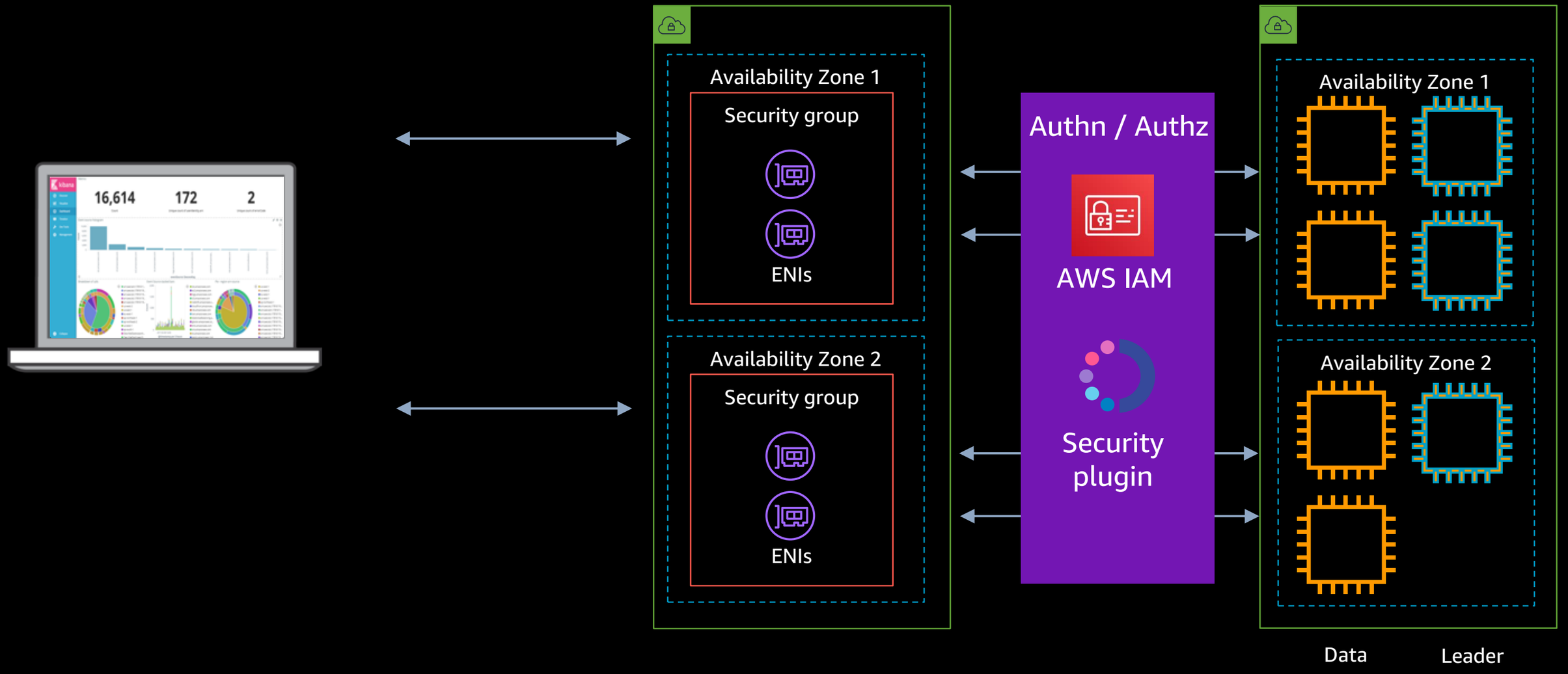
Multilayer authentication



Authenticated and access granted

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Controlling access in your VPC

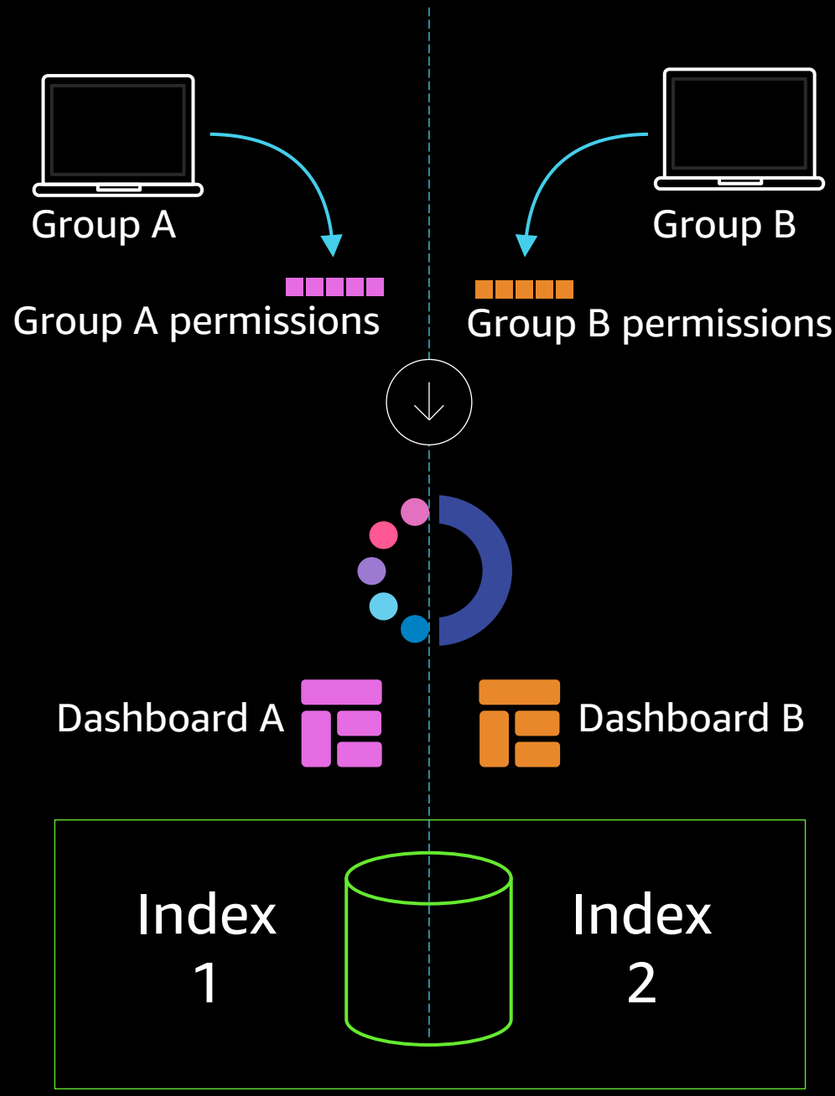


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Kibana multi-tenancy

Enable teams to share a cluster but only see their data, dashboards and visualizations

- Create tenants for Kibana (global, per-group, private)
- When using Kibana select a tenant
- Assign tenants to users to enable access
- Tenancy is not the same as access control



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define a friendly name for your domain endpoint



https://analytics.mycompany.com/_plugin/kibana

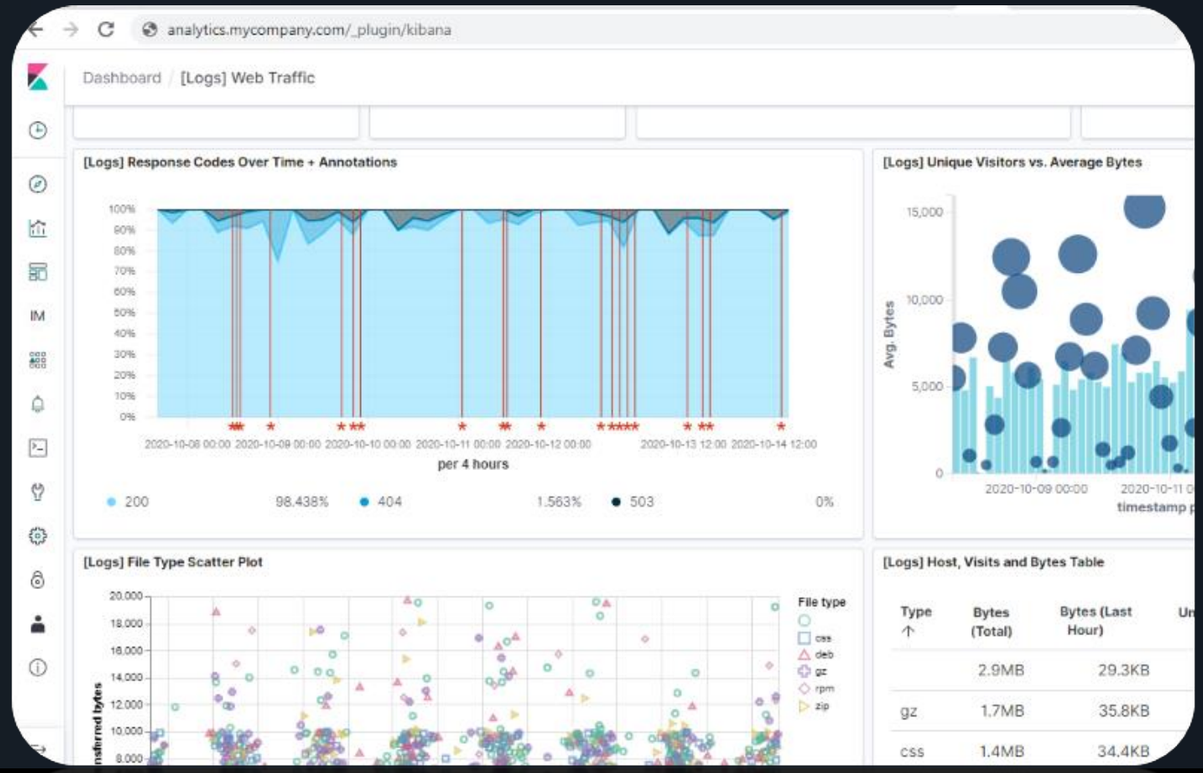
DNS

CNAME or Alias mapping in Amazon Route 53 or your preferred DNS

Amazon Elasticsearch Service Domain

Create or import an SSL certificate into AWS Certificate Manager

- ✓ Makes it easier for your users to access Kibana including SAML auth
- ✓ Allows you to move to a new domain without updating your clients



Thank you!

Carl Meadows

carlmead@amazon.com

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.