AWS re:Invent

ANT215-R

Securing your Amazon Elasticsearch Service domain

Hardik Shah
Sr. Software Engineer
Amazon Web Services

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Introduction to Amazon Elasticsearch Service (Amazon ES)
- Discuss security features of Amazon ES
- Demo
- Best security practices for Amazon ES
- Q&A

Introduction to Amazon ES

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security features of Amazon ES

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security features

Access control to Amazon ES domain

- Resource-based policy
- Identity-based policy
- IP-based policy

VPC support

- VPC resources required for domain creation
  - A VPC
  - One or more subnets
  - Optional security group
- For testing/setting up restricted access from outside VPC
  - EC2 instance
  - Internet gateway and route table
- Service linked role for elastic network interface creation

Security features

Encryption

- Encryption at rest
  - AWS Key Management Service (AWS KMS) key
  - Additional encryption for manual snapshot and error/slow logs in Amazon CloudWatch logs
- Encryption in flight
- Domain endpoint security (HTTPS enforcement and TLS version)

Amazon Cognito authentication for Kibana

- User pool
- Identity pool
- IAM role for service to create/manage Cognito resources
- External identity provider
  - Social (Facebook , Google+, Twitter, Apple, Login with Amazon)
  - SAML
  - OpenID and other custom auth provider

Demo

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Demo

1. Access control and IAM proxy setup for Kibana
2. Encryption
3. VPC and VPC tunnel for access
4. Amazon Cognito authentication for Kibana

Best practices for Amazon ES

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices

- Use multi-factor authentication (MFA) with each AWS account.
- Create an Amazon ES domain inside VPC.
- Always configure resource- or identity-based policies to secure access of your domain. (Avoid open-access policy).
- For better access control and audit, configure different IAM roles/users for different applications that interact with your domain—and for data access vs. configuration access.
- Use encryption of data at rest.
- Use encryption of data in flight (node-to-node encryption).

Security best practices

- Use SSL/TLS to communicate with AWS resources.
  Choose **RequireHTTPS** when you create domains with secure TLS protocol version.
- Configure Amazon Cognito to access Kibana endpoints, if you want to avoid a difficult setup of IAM proxy for Kibana.
- If you have set up manual snapshots for your domain, configure Amazon S3 server-side encryption with S3 managed keys to encrypt the S3 bucket you've set up as a snapshot repository.
- If you have configured your domain to publish slow logs and error logs to CloudWatch Logs, encrypt their CloudWatch Logs `log group` using the AWS KMS key.

Security best practices

- We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into domain names, index names, document types, or document IDs. Amazon ES uses these names in its Uniform Resource Identifiers (URIs). Servers and applications often log HTTP requests, which can lead to unnecessary data exposure if URIs contain sensitive information.
- Set up API and user activity logging with AWS CloudTrail.

Thank you!

Hardik Shah

Email: hardiks@amazon.com

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

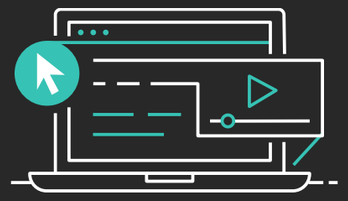


Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learn analytics with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate data analytics skills



New free digital course, *Data Analytics Fundamentals*, introduces Amazon S3, Amazon Kinesis, Amazon EMR, AWS Glue, Amazon Redshift, Amazon Athena, and AWS Lake Formation



Classroom offerings, including Big Data on AWS, feature AWS expert instructors and hands-on labs



Validate expertise with the **AWS Certified Big Data - Specialty** exam or the new **AWS Certified Data Analytics - Specialty** beta exam

Visit aws.amazon.com/training/paths-specialty/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification