
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STP212

Simple steps to prepare your environment for compliance

Steven Poelstra (he/him)
Sr. Startup Solutions Architect
Amazon Web Services

Conor Colgan (he/him)
Sr. Startup Solutions Architect
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Steps we'll take



Enable logging **everywhere**



Follow **least-privilege**



Measure and **enforce**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Questions we'll answer

What about compliance?

What is security, privacy, and governance?

Why should I care?

What can I do?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What about compliance?

Forms of compliance

PCI

FedRAMP

GDPR

GxP

HIPAA

HITRUST

NIST

SOC

And many more!

What are they about?

Security

Privacy

Governance and enforcement

Data integrity

Logging and monitoring

Resiliency and availability

Disaster recovery

Quality control

And many more!

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security, privacy, and governance

Security

Safeguarding data from unauthorized access

Privacy

Access policy of who is allowed, when, and for what purpose

Governance

Define why we have policies and monitor for violations



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

But why should I care?

Because your customers do

It might be easier than you think

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What can I do?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

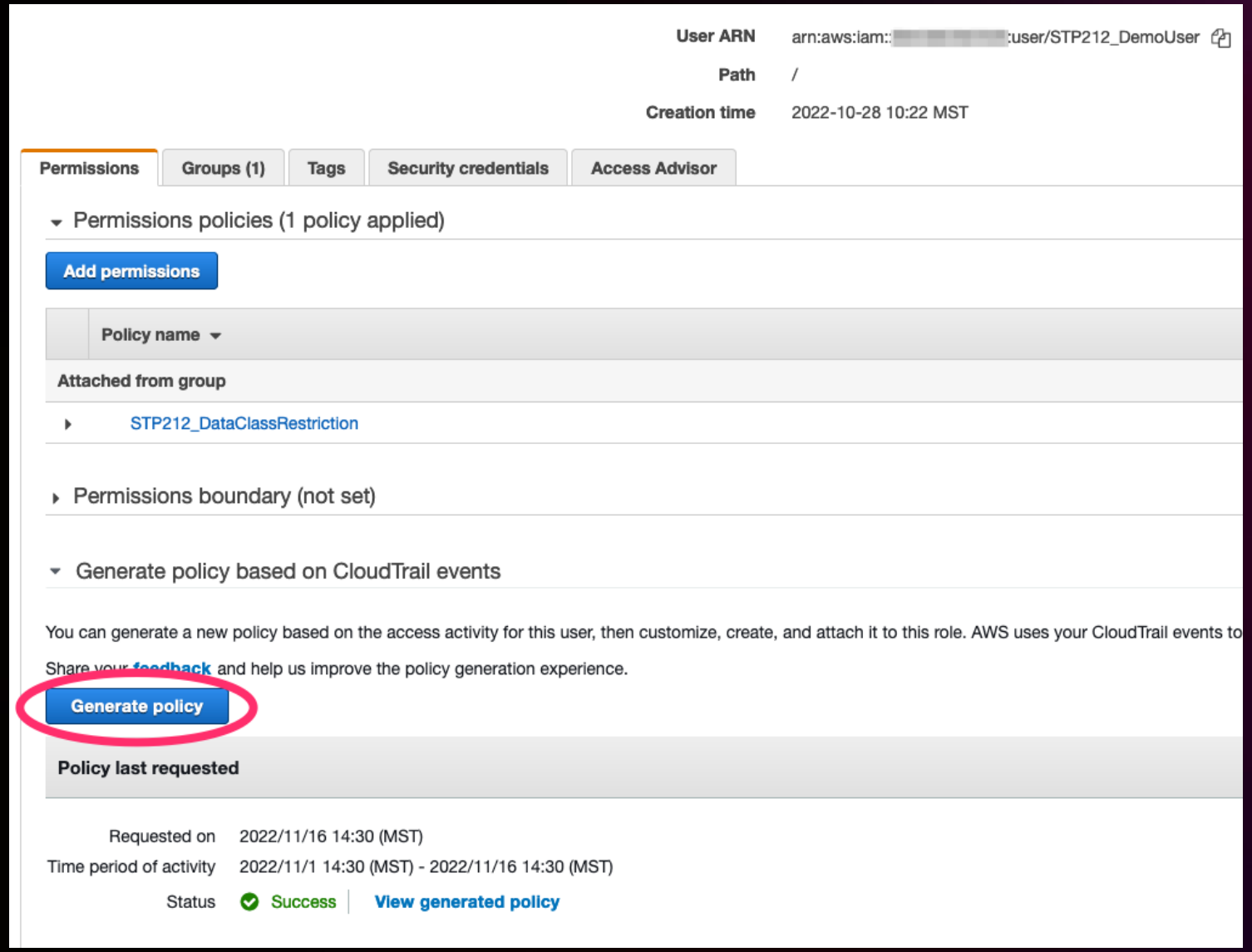
Step 1: Enable logging everywhere

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step 2: Least privilege

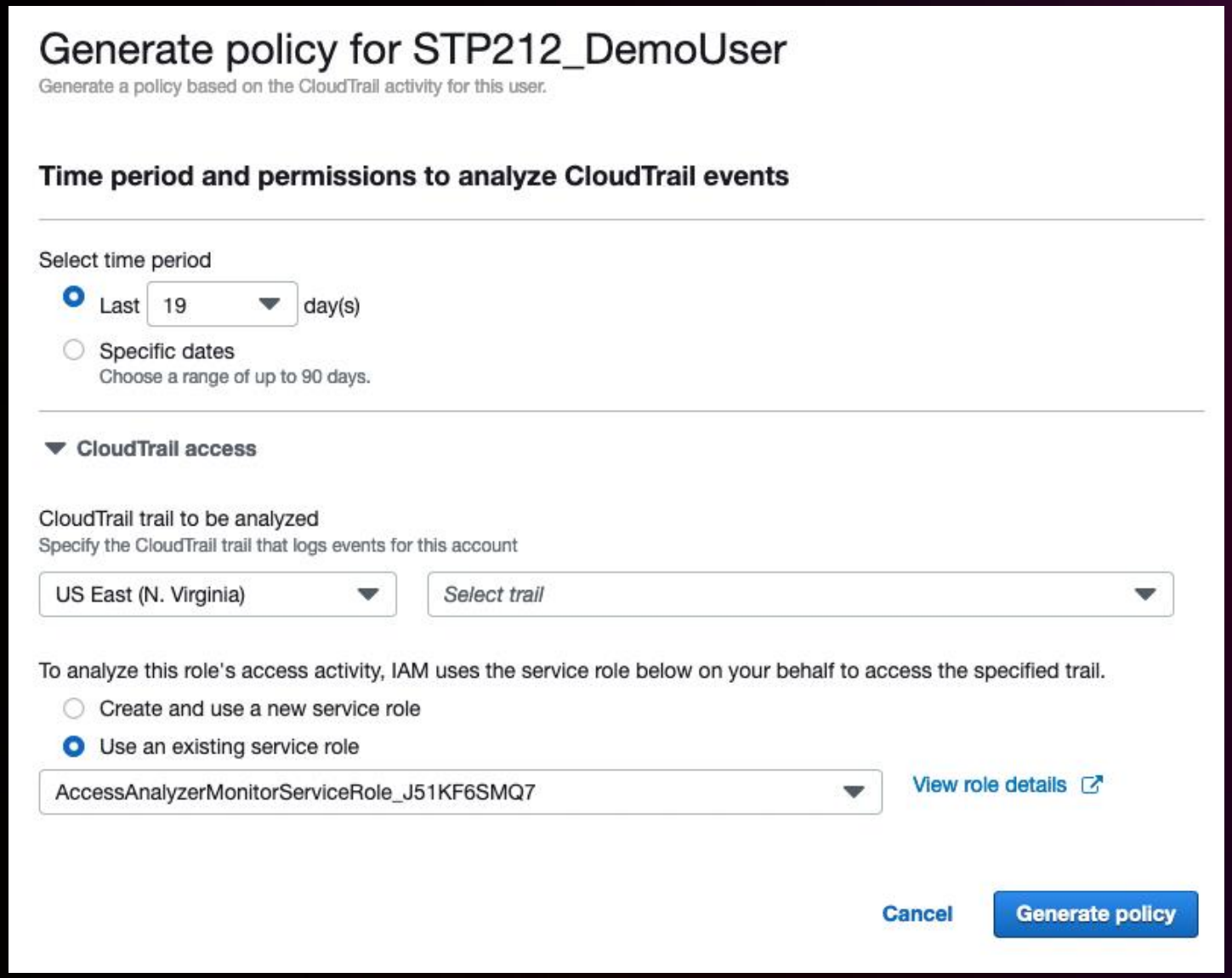
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer

Generated policy

Review permissions

Review the services and actions we found. For some services, specify the actions.

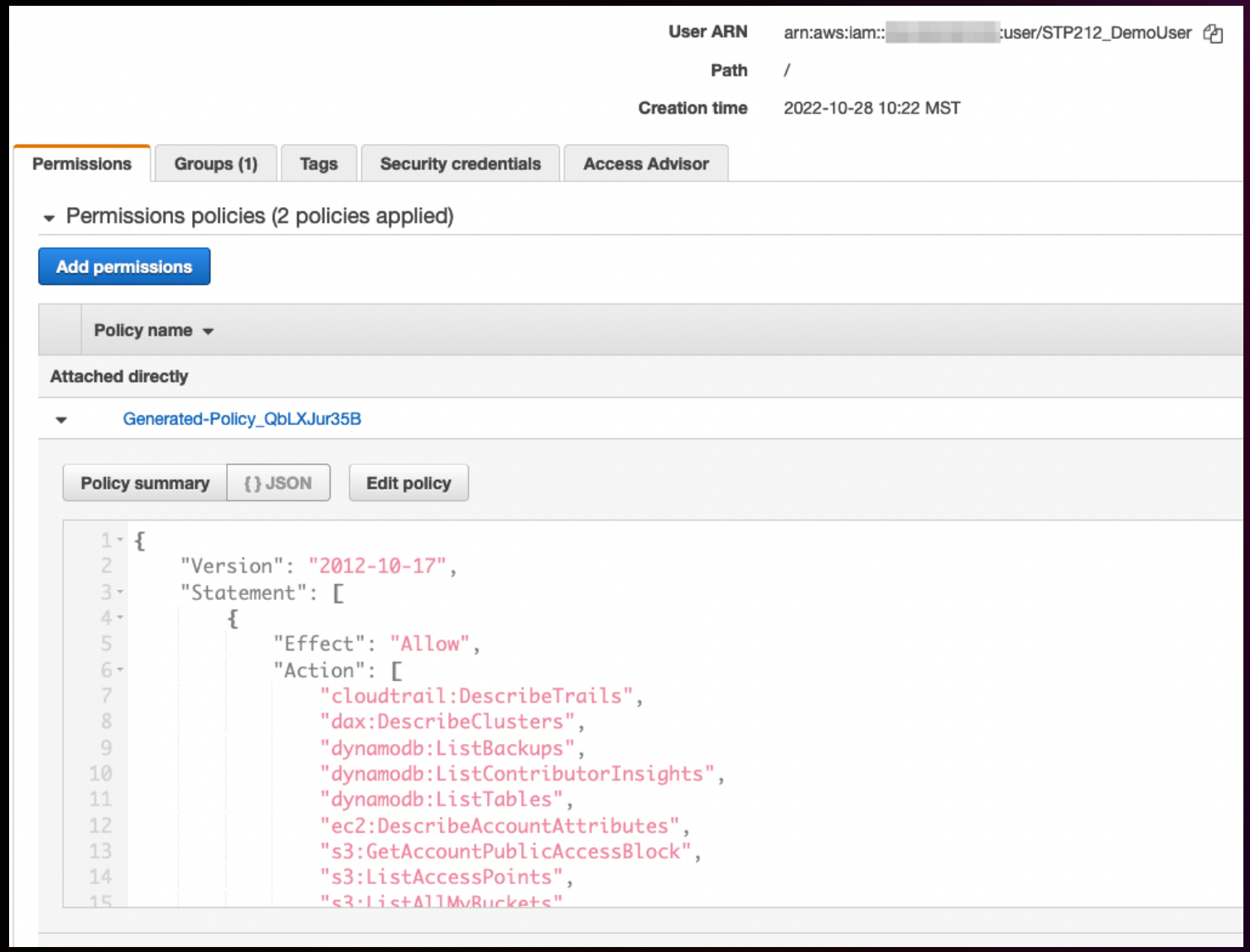
▼ Actions included in the generated policy

Service ▲	Actions used
CloudTrail	DescribeTrails.
CloudWatch	DescribeAlarms.
CloudWatch Logs	DescribeMetricFilters.
DynamoDB	ListTables, DescribeTimeToLive, ListTagsOfResource, DescribeContinuousBackups, DescribeTable, ListContributorInsights, DescribeGlobalTable, ListBackups.
DynamoDBAccelerator	DescribeClusters.
EC2	DescribeAccountAttributes.
S3	GetIntelligentTieringConfiguration, GetAccelerateConfiguration, GetBucketTagging, ListAllMyBuckets, GetBucketPolicyStatus, GetBucketOwnershipControls, GetBucketVersioning, ListMultiRegionAccessPoints, GetStorageLensDashboard, GetBucketRequestPayment, GetStorageLensConfiguration, GetBucketObjectLockConfiguration, GetAccountPublicAccessBlock, GetBucketPublicAccessBlock, GetBucketWebsite, GetBucketAcl, GetBucketPolicy, GetBucketLogging, ListAccessPoints, GetBucketNotification, GetEncryptionConfiguration.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer

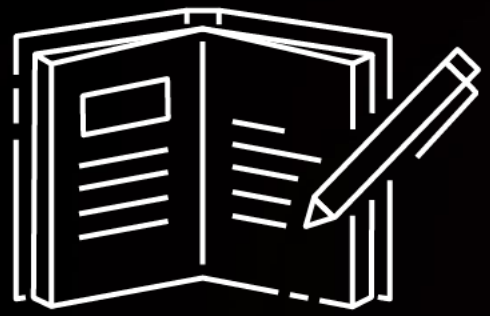


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

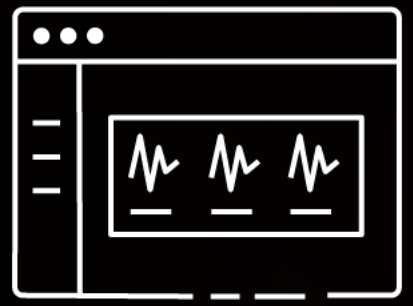
Step 3: Measure & enforce

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Defining compliance



What does **compliance** mean to you?



Now **enforce** and **measure** it

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

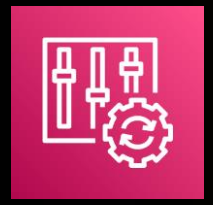
Go build your foundation



Enable **AWS CloudTrail** everywhere



Implement least-privilege with **AWS IAM Access Analyzer**



Measure and enforce with **AWS Config**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

How you can use AWS to improve logging blog

AWS IAM Access Analyzer

AWS Config Conformance Packs

AWS Startup Security Baseline

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Steven Poelstra
poelss@amazon.com

Conor Colgan
colgc@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.