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

COP334

Audit and investigate compliance violations with AWS CloudTrail Lake

Rodney Bozo

Sr. Manager, SA
AWS

Devi Paulvannan

Sr. Solutions Architect
AWS

Sravan Rachiraju

Partner Solutions Architect
AWS

Praveen Bhat

Pr. Solutions Architect
AWS

Kishore Vinjam

Sr. Partner Solutions Architect
AWS

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

Agenda

- Why AWS Cloud Operations?
- What are your compliance requirements?
- Effective ways to investigate or audit operations
- Use CloudTrail Lake to investigate compliance violations
- Build your own queries

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

Why AWS Cloud Operations?



Return on Investment (ROI)

241% ROI over 3 years*



Staff productivity

62% more efficient IT infrastructure staff



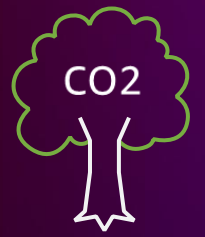
Operational resilience

57% decrease in downtime



Business agility

37% decrease in time to market



Carbon savings

88% reduction in carbon footprint of IT operations

Based on independent research of 1,500 AWS enterprise customers
*Source: "The Total Economic Impact of AWS Cloud Operations: Cost Savings And Business Benefits Enabled By Operation on AWS." May 2022. A commissioned study conducted by Forrester Consulting on behalf of Amazon Web Services.

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

Your journey to operating at cloud scale

Get started with AWS Cloud Operations

1) Setup



Establish a secure foundation for governance and compliance

2) Build and migrate



Migrate applications to the cloud or build new applications

3) Operate



Monitor application performance so you can detect and remediate noncompliance or operational risks quickly

aws

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

What are your compliance requirements?

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

Compliance frameworks



Center for Internet Security (CIS) – https://www.cisecurity.org/benchmark/amazon_web_services
Payment Card Industry Data Security Standard (PCI DSS) – https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

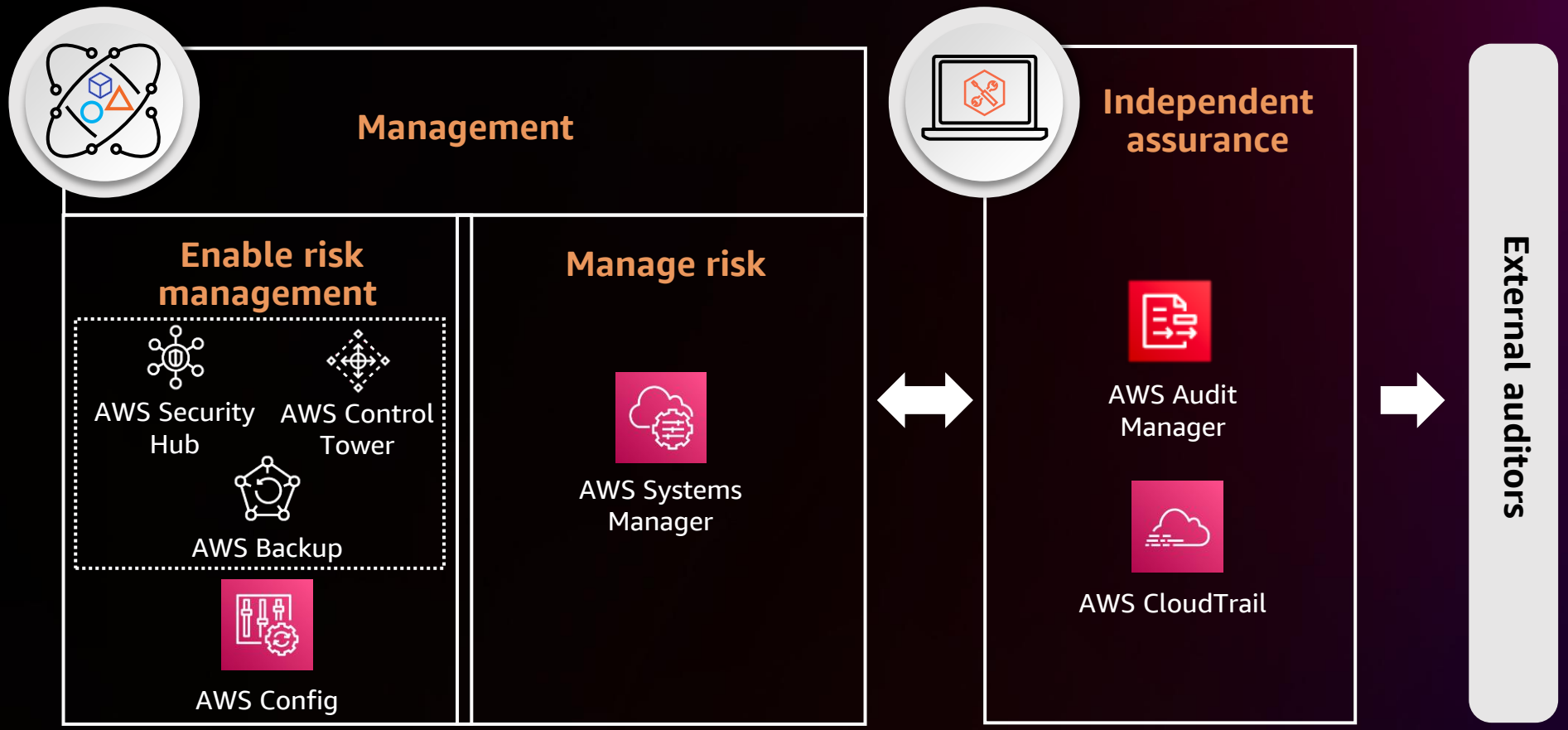
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Effective ways to investigate or audit operations

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

How AWS enables cloud compliance and assurance

- The IIA's Three Lines Model



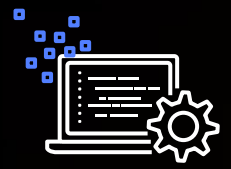
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://www.theiia.org/

AWS CloudTrail

Track user and resource activity across your AWS infrastructure for governance and auditing.

Identify and respond to unusual activity based on automated analysis.



Capture

Record activity as CloudTrail events



Store

Retain events logs in secure S3 bucket



Act

Trigger actions when important events are detected



Review

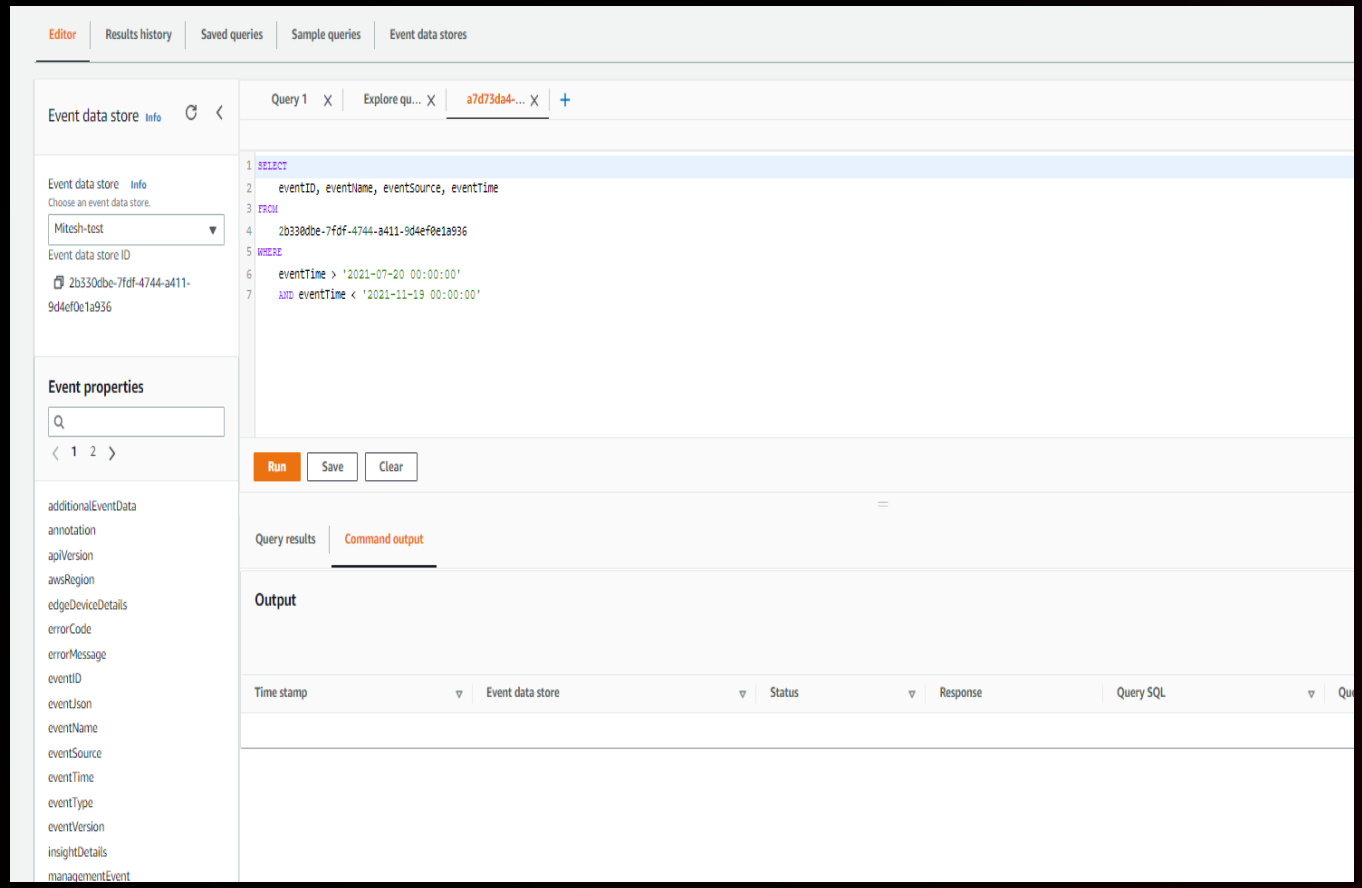
Analyze findings or recent and historical activity

aws

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

AWS CloudTrail Lake

MANAGED AUDIT DATA LAKE TO AGGREGATE, IMMUTABLY STORE, AND ANALYZE AUDIT AND SECURITY INFORMATION



Turn-key solution

Managed service with built-in analytics

Time savings

Accelerate security and operational investigations with included sample queries

Fast performance

Events are delivered within minutes and most queries completed within seconds

Cost effective

Pay for ingestion costs, including seven years of storage, and for queries run

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

AWS CloudTrail

CloudTrail Trail

(Events delivered to S3 bucket)

- Track management and data events of AWS services
- Integrates with Amazon CloudWatch, Amazon Athena, and other partner products for a DIY solution
- Customer-managed S3 bucket and policies
- CloudTrail log file validation

CloudTrail Lake

(Managed security and audit Lake)

- Track management and data events of AWS services and supported partner products (open audit events)
- Integrated SQL queries for turn-key solutions
- Managed storage with 7 years of included storage
- Immutable source of events

Free event history and lookup for 90 days of management activity

Paid insights for anomaly detection

aws

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

Use CloudTrail Lake to investigate compliance violations

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

High-level steps

Workshop URL: https://bit.ly/riv22-cop334

- Start the workshop in the provided AWS account
  - Enable CloudTrail Lake and start collecting both management and data events
  - Use SQL-like query language to get insights from the data collected
  - Create and save the query
- Use AWS Config conformance packs to enable PCI DSS compliance framework
- Build CloudTrail Lake queries to check for PCI DSS violations

aws

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

Resources

- Operating securely and safely in the cloud at scale: https://aws.amazon.com/cloudops/?blog-posts-cards.sort-by=item.additionalFields.modifiedDate&blog-posts-cards.sort-order=desc
- Working with AWS CloudTrail Lake: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-lake.html
- Getting started with CloudTrail Lake workshop: https://catalog.workshops.aws/getting-started-with-cloudtrail-lake/en-US
- Announcing AWS CloudTrail Lake – a managed audit and security lake: https://aws.amazon.com/blogs/mt/announcing-aws-cloudtrail-lake-a-managed-audit-and-security-lake/
- Compliance validation for AWS CloudTrail: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/CloudTrail-compliance.html

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

Want to see more AWS Cloud Operations?

Please complete the session survey in the mobile app



Ask us anything at our kiosks in the AWS Village Expo



Find related sessions in our re:Invent blog

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

Thank you!

Rodney Bozo

Devi Paulvannan

Sravan Rachiraju

Praveen Bhat

Kishore Vinjam



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

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