AWS re:Invent

ANT214-R1

VPC flow logs and Amazon Elasticsearch Service

Vishnu Madanarajagopal

Senior Manager, Software Development
Amazon Elasticsearch Service

AWS re:Invent

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

aws

Agenda

VPC flow logs overview

Log ingestion overview

Log ingestion pipeline

Configuring VPC flow logs to Amazon Elasticsearch Service

Demo/hands-on

VPC flow logs overview

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

What are VPC flow logs?

- A feature that captures information about IP traffic to and from network interfaces in your VPC
- VPC flow logs can help you with:
  - Diagnosing overly restrictive security group rules
  - Monitoring the traffic that is reaching your instance
  - Determining the direction of the traffic to and from the network interfaces

How to create VPC flow logs

- You can create a flow log for a VPC, a subnet, or a network interface; if you create a flow log for a subnet or VPC, each network interface in that subnet or VPC is monitored

- To create a flow log, you specify:
  - The resource for which to create the flow log
  - The type of traffic to capture (accepted traffic, rejected traffic, or all traffic)
  - The destinations to which you want to publish the flow log data

Example VPC flow log

Flow Logs Format

<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>

In this example, SSH traffic (destination port 22, TCP protocol) to network interface eni-1235b8ca123456789 in account 123456789010 was allowed:

2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010 1418530070 ACCEPT OK

Log ingestion overview

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

Amazon Elasticsearch Service



Amazon Elasticsearch Service (Amazon ES) is a **fully managed service** that makes it easy to deploy, manage, and scale Elasticsearch and Kibana in the AWS Cloud

Benefits of Amazon ES



Supports OS APIs and Tools

Drop-in replacement with no need to learn new APIs or skills



Easy to Use

Deploy a production-ready Elasticsearch cluster in minutes



Scalable

Resize your cluster with a few clicks or a single API call



Secure

Deploy into your VPC and restrict access using security groups and IAM policies



Highly Available

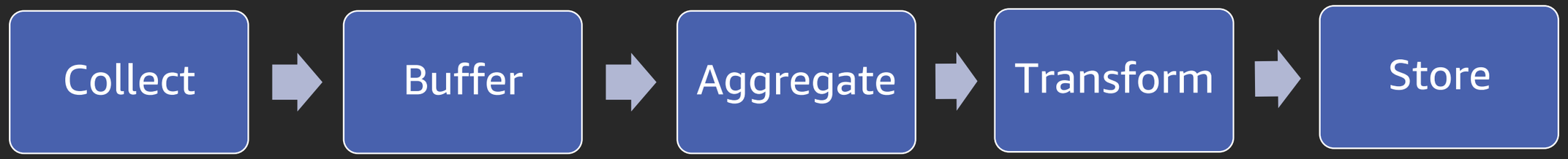
Replicate across Availability Zones, with monitoring and automated self-healing



Tightly Integrated

Seamless data ingestion, security, auditing and orchestration

Overview of delivering logs to Amazon ES



Log collectors: Popular options

AWS native Agent-based	Open source Agent-based	Open source JVM-based
 Amazon CloudWatch agent		
 Amazon Kinesis agent		
		

Log buffers: Popular options

AWS native



Amazon CloudWatch



Amazon Simple Queue Service



AWS IoT



Amazon Kinesis Data Streams



Amazon Simple Storage Service



Amazon Kinesis Data Firehose

Open source/AWS service









Amazon Managed Streaming for Kafka

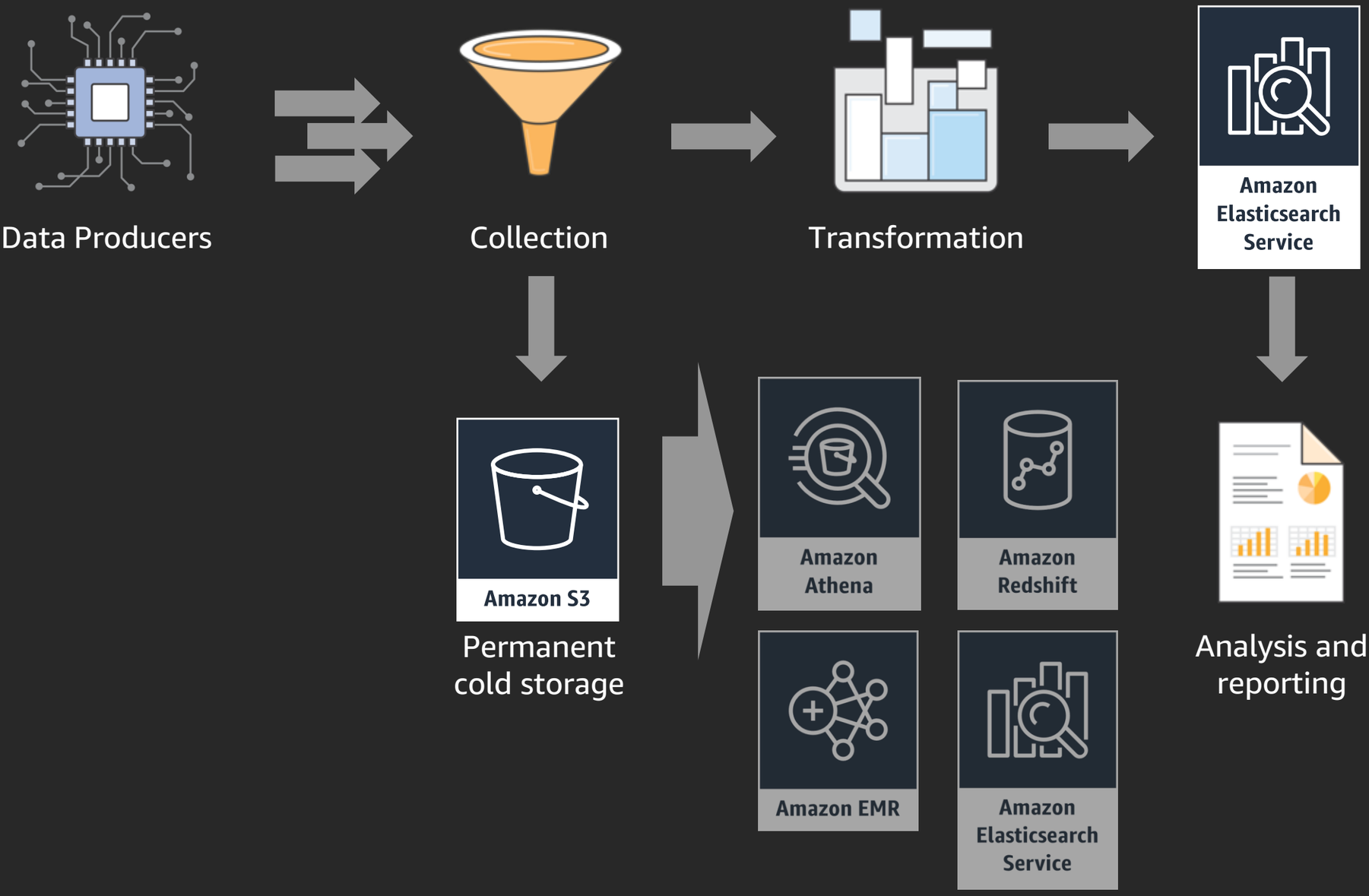


Amazon ElastiCache for Redis

Log aggregators: Popular options

AWS native	Open source Agent-based	Open source JVM-based
 AWS Lambda		

Log analytics flow



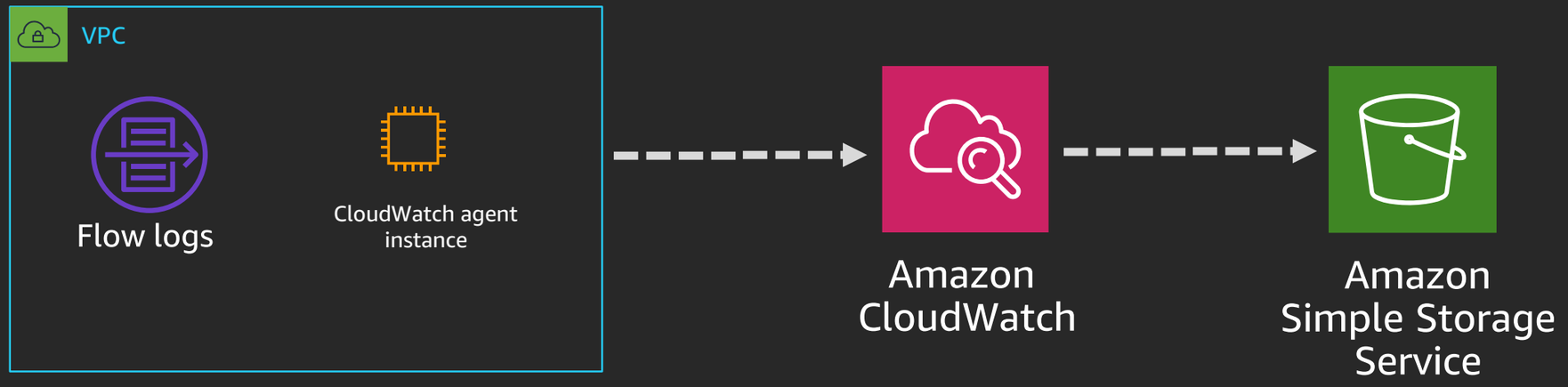
Configuring VPC flow logs to Amazon Elasticsearch Service

AWS re:Invent

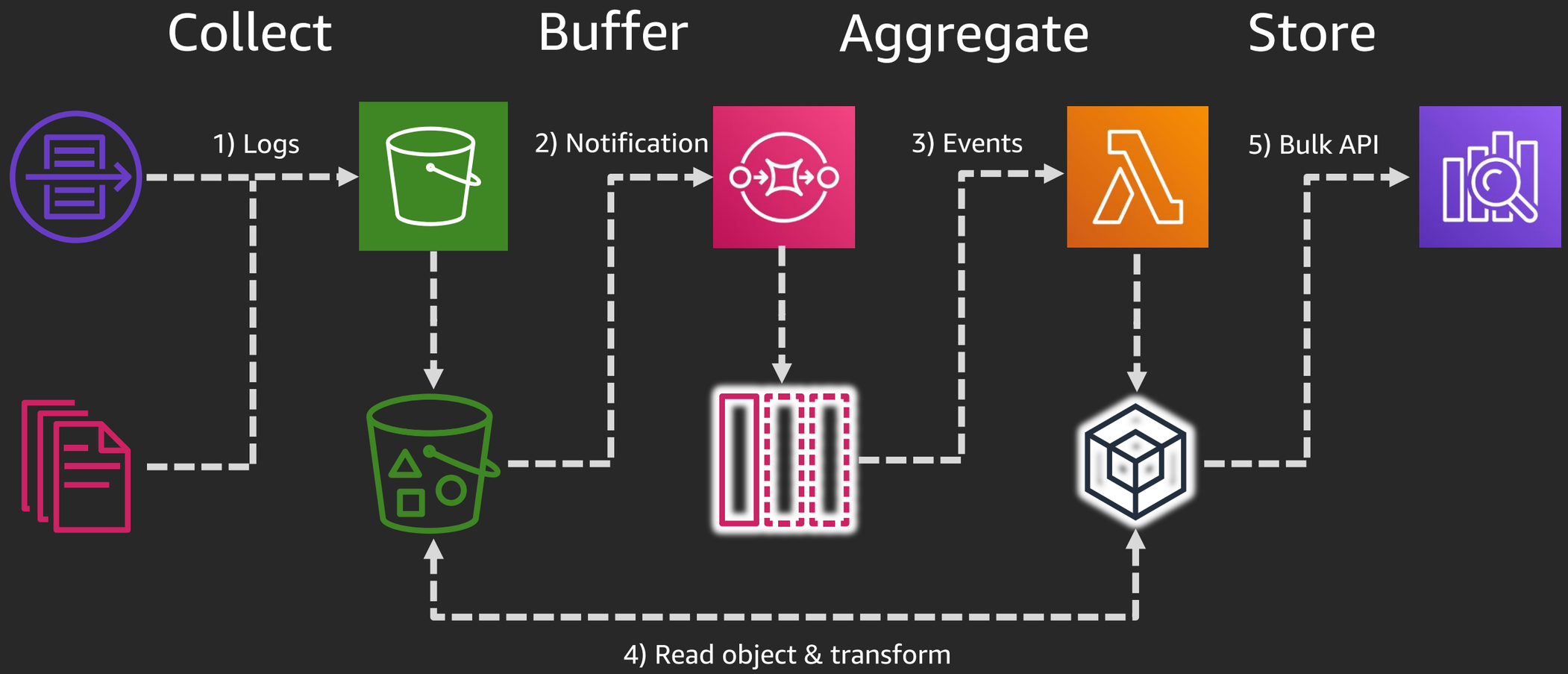
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

VPC flow logs to Amazon S3 bucket



Amazon S3 event notifications approach

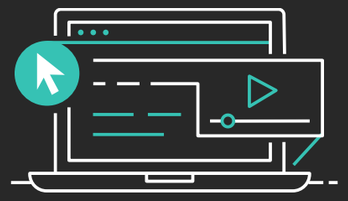


Demo

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

Learn big data 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, and Amazon Redshift



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

Thank you!

Vishnu Madanarajagopal

madanara@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.