

AWS RE:INVENT

re:Cap

Agenda

- Security
- Networking
- Cloud Operations
- Storage
- Compute and Containers

Security



Dan Girard

He/Him/His
Sr. SA
Federal



Dave Wood

He/Him/His
Sr. Builder SA
Federal

Themes for AWS Security at re:Invent 2023

- Zero Trust architectures and data perimeters
- Using AI/ML in security
- Managing policies (permission policies, endpoint policies, resource policies, etc.) at scale using CI/CD/IaaS patterns
- Improving the builder experience while also accelerating security objectives

PREVIEW



IAM Access Analyzer

CUSTOM POLICY CHECKS POWERED BY
AUTOMATED REASONING

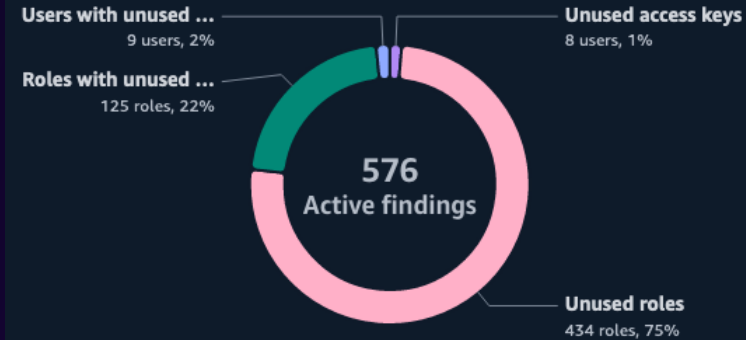
- Custom policy checks validate that IAM policies adhere to your security standards ahead of deployments
- Uses automated reasoning - security assurance backed by mathematic proof
- Helps security teams proactively detect nonconformant updates to policies



INSPECTING UNUSED ACCESS TO GUIDE YOU
TOWARD LEAST PRIVILEGE

Findings overview

An overview of unused access findings by finding type.



Accounts with the most active findings for unused access

Account

findings ▲

Findings by type

Acct Name

Acct #

61

- Unused access keys
- Unused roles
- Users with unused permissions
- Unused passwords
- Roles with unused permissions



IAM Identity Center and AWS Analytics

SIMPLIFIED DATA ACCESS VIA IAM IDENTITY CENTER



- AWS Analytics services now use trusted identity propagation with AWS IAM Identity Center
 - Amazon QuickSight, Amazon Redshift, Amazon EMR, AWS Lake Formation
 - Amazon S3 via S3 Access Grants
- Improved single sign-on experience
- Users and groups maintained in your chosen identity provider
- Enables audit of user access across services



AWS Security Hub



MAJOR DASHBOARD ENHANCEMENTS

Insights See the insights with the most results.	Accounts with the most findings (by severity) See the top accounts that are at risk by severity and by resource type.	AMIs with the most findings See the top AMIs that are at risk.
Latest findings from AWS integrations Track findings from integrated AWS services.	Accounts with the most findings (by resource type) See the top accounts that are at risk by severity and by resource type.	IAM principals with the most findings See the top IAM principals that are at risk.

New Data Visualizations

New Widgets

- Helps relate to potential threats and vulnerabilities in your AWS cloud environment
- More easily focus on risks that require your attention



NEW CENTRAL CONFIGURATION CAPABILITIES

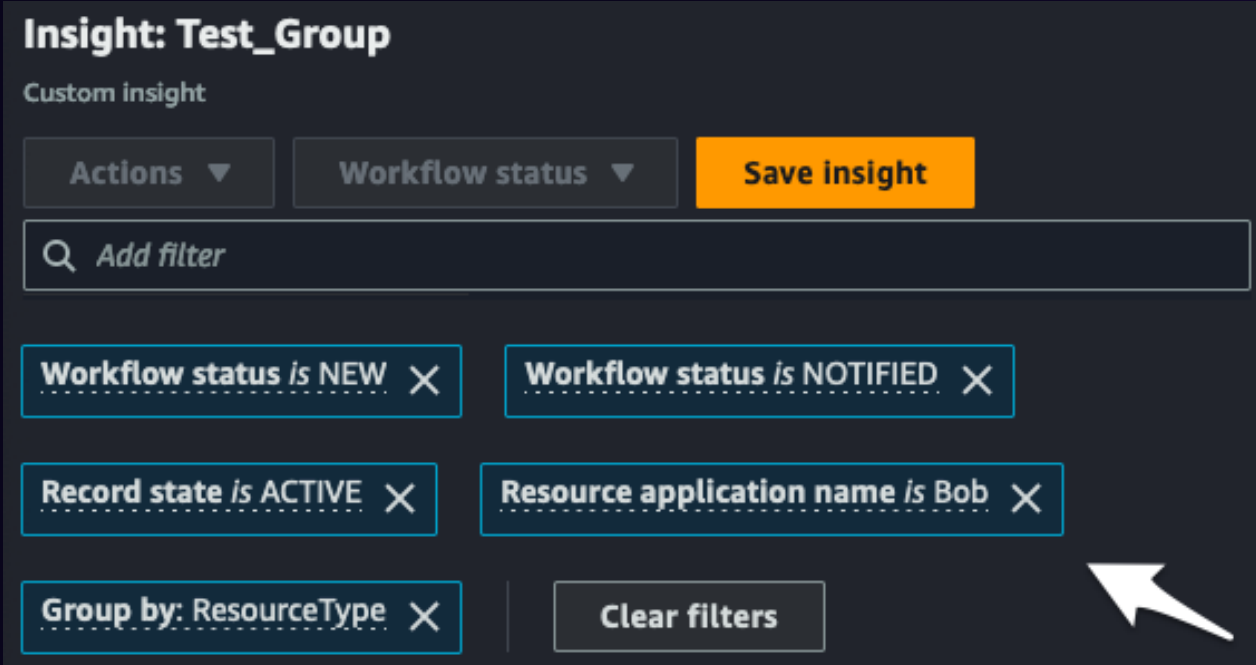
Central Enablement of Controls

- Address gaps security coverage by applying security policies in selected regions/OUs.
- Customize security posture for an account or globally, without needing to update them.



AWS Security Hub

NEW FINDING METADATA ENRICHMENT



The screenshot shows the 'Insight: Test_Group' interface in AWS Security Hub. It features a 'Custom insight' section with a 'Save insight' button. Below this are several filter options: 'Workflow status is NEW', 'Workflow status is NOTIFIED', 'Record state is ACTIVE', and 'Resource application name is Bob'. A 'Clear filters' button is also present. A white arrow points to the 'Resource application name is Bob' filter.

- Eliminates the need to build data enrichment pipelines or manually enrich metadata of security findings

- Provides better context, prioritization, to take action on your security findings
 - Adds tags, application tag and account name to every finding ingested into Security Hub
- Includes findings from Amazon GuardDuty, Amazon Inspector, and AWS IAM Access Analyzer, plus AWS Partner Network (APN) solutions



AWS GuardDuty



ECS RUNTIME MONITORING, INCLUDING AWS FARGATE

The screenshot shows the AWS GuardDuty console interface. The left sidebar contains navigation options like Summary, Findings, Usage, Malware scans, Protection plans, Accounts, Settings, Lists, and Partners. The main content area is titled 'Runtime Monitoring' and includes a 'Runtime coverage' tab. Under 'Coverage statistics', there are three metrics: Healthy EKS clusters (0/0, 100%), Healthy ECS clusters (1/1, 100.0%), and Healthy EC2 instances (0/0, 100%). Below this, there are tabs for 'EKS clusters runtime coverage', 'ECS clusters runtime coverage', and 'EC2 instance runtime coverage'. The 'ECS clusters runtime coverage' tab is active, showing a 'Clusters list (1)' with a search bar and a table containing one cluster: 'SpaceTwin-Infra-SpaceTwinCluster3D77526A-5D6rTXjgd5b2' with an account ID of 636183562745, an auto-managed agent, and a healthy status.

- Runtime threat detection for Amazon Elastic Container Service (Amazon ECS) workloads
- Centrally enable runtime threat detection using AWS Organizations
- Free for 30 days on the AWS Free Tier



RUNTIME MONITORING FOR AMAZON EC2 (PREVIEW)

PREVIEW

Amazon EC2

Currently, the Amazon EC2 instance support is in preview and automated agent configuration is not available during this time. To manage the GuardDuty security agent manually, [learn more](#)

- Runtime threat detection for Amazon EC2 workloads to help identify potential threats to EC2 instances
- Supports AWS Organizations to centrally enable coverage for



AWS Secrets Manager

BATCH RETRIEVAL OF SECRETS

- Single API call to identify and retrieve a group of secrets
 - Use a list of secret names or ARNs
 - Optional filter criteria, such as tags
- Greater simplicity to common developer workflows

```
{
  "Filters": [
    {
      "Key": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string",
  "SecretIdList": [ "string" ]
}
```



Amazon Inspector



AWS LAMBDA CODE SCANNING WITH GENERATIVE AI POWERED REMEDIATION

- Assisted code remediation using generative AI and automated reasoning
- In-context code patches for multiple classes of vulnerabilities detected during security scans for Lambda functions
- Assess Lambda code for security issues like injection flaws, data leaks, weak cryptography, or missing encryption
- Actionable security findings including affected code snippets and remediation suggestions



Amazon Inspector

PREVIEW



AGENTLESS VULNERABILITY ASSESSMENTS FOR AMAZON EC2

- Continuous monitoring of Amazon EC2 instances for software vulnerabilities
- No agent or additional software required
- Includes EC2 instances that do **NOT** have SSM Agents installed
- Leverage EBS volumes for software inventory and vulnerability assessments

The screenshot displays the Amazon Inspector console interface. The main heading is "Amazon Inspector - Assessment Runs". Below the heading, there is a description: "An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. [Learn more.](#)".

At the top of the console, there are navigation tabs: "Dashboard", "Assessment targets", "Assessment templates", "Assessment runs" (which is selected), and "Findings".

The main content area shows a table of assessment runs. The table has the following columns: "Start time", "Status", "Template name", "Findings", "Findings by severity", and "Reports". A single row is visible, representing an assessment run that started "Today at 4:50 PM (GMT+...)" and is currently in the "Collecting data" status. The template name is "Windows Servers" and the number of findings is "0".

Below the table, there is a "Max records per page:" dropdown menu set to "25". A note at the bottom right of the table area says "* refresh browser to reflect change".

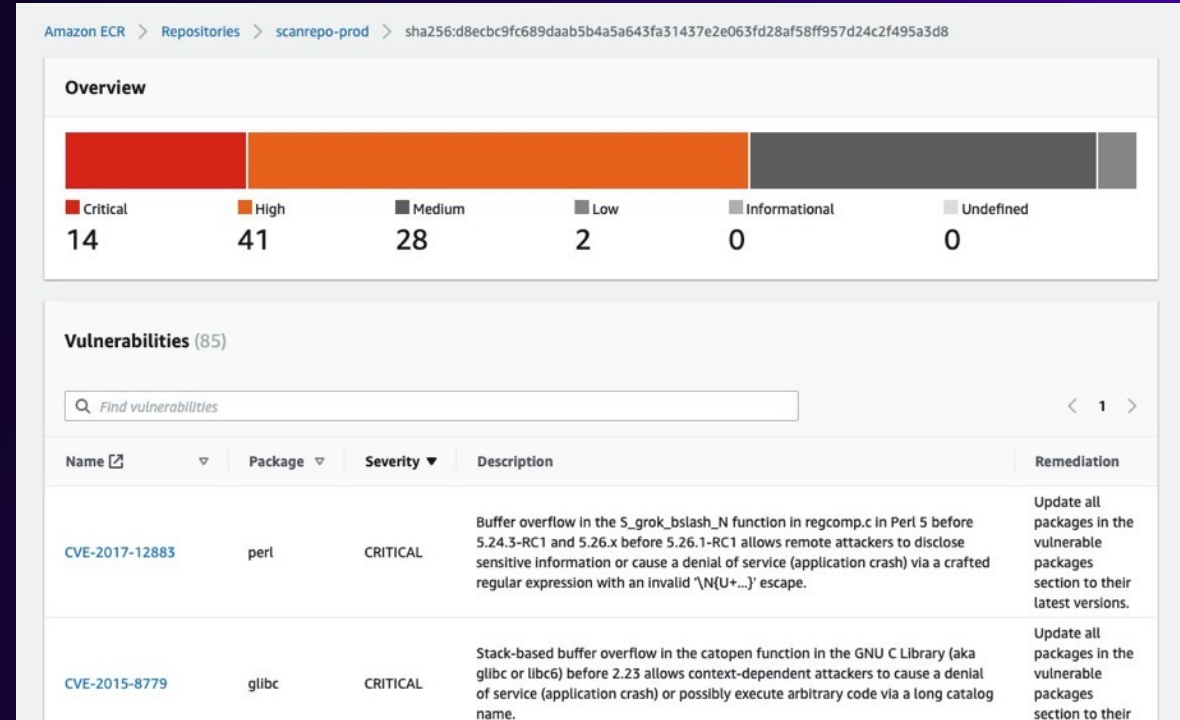


Amazon Inspector Container Assessments



AMAZON INSPECTOR ENHANCES CONTAINER IMAGE SECURITY BY INTEGRATING WITH DEVELOPER TOOLS

- Integrated with CI/CD tools
 - Provides findings within tool's dashboard
 - Pushes security earlier in the software development lifecycle.
- Can be hosted in AWS, on-premises, or hybrid clouds
- Automatically discovers EC2, container images in ECR and AWS Lambda functions
- Consolidated view of vulnerabilities across compute environments



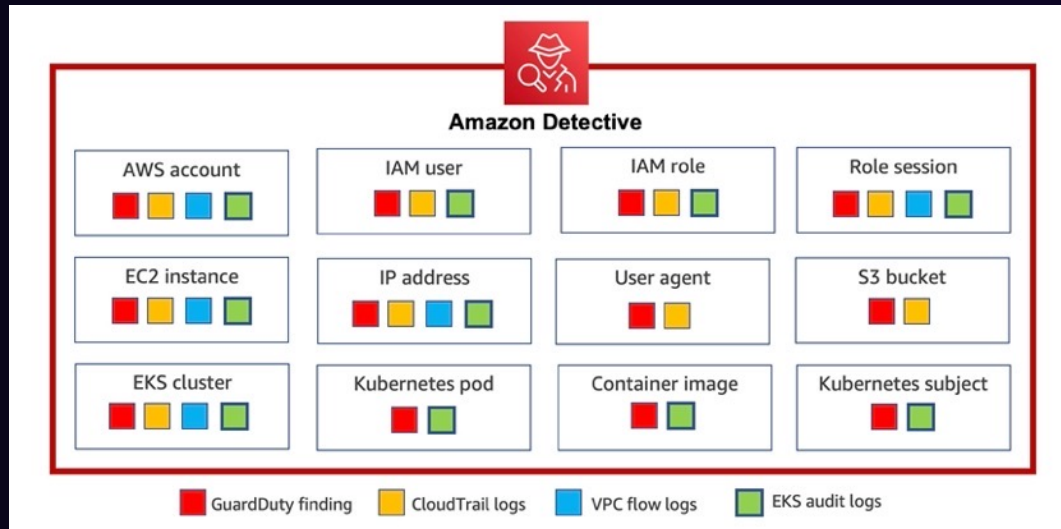
- Continuously monitors for known vulnerabilities



Amazon Detective



LOG RETRIEVAL FROM AMAZON SECURITY LAKE



- Query and retrieve logs stored in Security Lake
- Gets additional information from AWS CloudTrail logs and Amazon VPC Flow Logs
- Build data aggregations, summaries and visualizations based on security findings and activity logs



Amazon Detective

SECURITY INVESTIGATIONS FOR AMAZON GUARDDUTY ECS RUNTIME MONITORING



- Security investigations for threats detected by Amazon GuardDuty Elastic Container Service (ECS) Runtime Monitoring
- Enhanced visualizations and additional context for detections in ECS
- Improve your detection and response for potential threats to your container workloads



Amazon Detective


FINDING GROUP SUMMARIES USING GENERATIVE AI

- Provides finding group summaries using generative AI
- Automatically analyzes finding groups
- Provides insights in natural language to help accelerate security investigations
- Examine multiple activities related to potential security events




Finding groups [Info](#)

Finding groups correlate entities and security findings to the same underlying activity, and should be investigated together. The following finding groups were active around the scope time.

 **Finding group summary now powered by AI** ✕

Finding groups now utilize generative AI technology that provides insights into your investigations. Select a finding group to try it out. Learn more about Region availability in the documentation.

[Learn more](#) 

Severity ▼	Title	Observed tactics	AWS accounts	Entities
No results to display				
View all finding groups				



Amazon Detective



INVESTIGATE AWS IDENTITY AND ACCESS MANAGEMENT (IAM) ENTITIES

Visualization - new [Info](#)
This interactive visualization allows you to select and see details about each item in the finding group.

Select layout
Circle

Legend
Findings and entities

Findings	Compute	Network	Identity	Storage
Critical	EC2 instance	IP address	AWS User	S3 bucket
High	Container	Subnet	AWS Role	
Medium	EKS cluster	User agent	Role session	
Low	Container Image	VPC	Account	
Informational	K8s pod		K8s subject	
	K8s workload			

Select entities and findings (4)

- TTPs/PenTest:IAMUser/KaliLinux Medium finding
- Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS High finding
- TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration!DNS High finding
- TTPs/PenTest:IAMUser/KaliLinux Medium finding

- Automatically analyze IAM users and IAM roles
- Quickly surface potential Indicators of compromise (IoC)
- Identify users or roles involved in any known tactics, techniques, and procedures (TTP) from the MITRE ATT&CK framework
- Includes 30-day free trial



AWS Config



PERIODIC RECORDING TO TRACK RESOURCE CONFIGURATION CHANGES MORE EFFICIENTLY AT SCALE

- Capture configuration item representing most recent state over 24-hour period
 - Reduces number of changes delivered
 - Choose which resource types to track using continuous or periodic recording
 - Optional overrides to frequency of recording of individual resource types

Recording method

Recording strategy
Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Globally recorded resources (RDS global clusters and IAM users, groups, roles, and customer managed policies) may be recorded in more than this Region. [Learn more](#) You are charged based on the number of configuration items recorded. [Pricing details](#)

All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

Specific resource types
AWS Config will only record the resource types that you specify.

Resource types to record [Info](#)
Choose a resource type to record and its frequency. It also impacts the costs to your bill. If you change the recording frequency for a resource type, the configuration items that were already recorded will remain unchanged.

Resource type: Frequency:

No limits if all resource types have the same frequency.

- Both continuous and periodic recording are priced based on the number of configurations items



Networking



Dave Wood

He/Him/His
Sr. Builder SA
Federal

Honorable Mentions

NETWORKING AND CONTENT DELIVERY



- Application Load Balancer can authenticate X.509 certificate based identities with Mutual TLS support
- Application Load Balancer increases application availability with Automatic Target Weights
- Amazon Route 53 Application Recovery Controller launches zonal autoshift

Cloud Operations



Bobby Hallahan

He/Him/His

Sr. SA

Federal

New ML-powered Logs Pattern Analysis and Logs Anomaly Detection



Use **patterns** view to visualize recurring patterns when querying your logs



Compare mode helps answer "what changed" over time








Always-on **anomaly detection**: proactive notification of emerging issues

The screenshot shows the AWS CloudWatch Patterns view. At the top, there are tabs for 'Patterns (48) - new' and 'Visualization'. Below the tabs, there are buttons for 'Add to query', 'Export results', and 'Add to dashboard'. A search bar allows filtering patterns by pattern string, event count difference, difference description, or keywords. The main area displays a table of patterns with columns for 'Inspect', 'Pattern', 'Event count', 'Event count difference', 'Difference description', and 'Severity type'. The table lists several patterns, including error and warning messages, with their respective event counts and differences. Below the table, there is a 'Pattern inspect' section showing a line chart of 'Event count' over 'Time (Local)'. The chart compares the 'Main time range' (blue line) with the 'Compare time range' (orange line). Below the chart, there are tabs for 'Log samples', 'Token values', and 'Related patterns'. The 'Log samples' tab is active, showing a list of log events with their timestamps and content.

Inspect	Pattern	Event count	Event count difference	Difference description	Severity type
<input type="checkbox"/>	[ERROR] <*> Data processing of request input failed! Exception: InvalidDateTimeFormat	357	+357	New pattern	ERROR
<input type="checkbox"/>	[WARNING] <*> ApplicationName='lambda_transaction_handler' database_insert_time_ms<*> HTTP_code<*> Error	176	-4	2% decrease	ERROR
<input type="checkbox"/>	[INFO] <*> Datetime expected in epoch format, received invalid input.	357	+357	New pattern	INFO
<input type="checkbox"/>	[INFO] <*> [*requestTime'- <*>]	176	-4	2% decrease	INFO
<input type="checkbox"/>	[INFO] <*> Entering function lambda_handler(). current_epoch=<*> user_guid=<*>	234	-6	3% decrease	INFO
<input type="checkbox"/>	[DEBUG] <*> Testing Unicode compatibility. 物の置れ	1,169	-64	5% decrease	DEBUG
<input type="checkbox"/>	[DEBUG] <*> [Benchmark CodeForm] Profile activity	754	-	7% decrease	DEBUG

Always-on Anomaly Detection

Log anomalies (10) Info				
<input type="text" value="Filter anomalies by priority level, patterns or keywords"/>			Anomalies Suppressed	
Anomaly log trend	Anomaly ▲	Priority ▼	Log pattern ▼	Last detection time ▼
	Found a new pattern that does not match existing patterns, with severity: ERROR	High	[ERROR] <*> <*> Database transaction failed! Exception: InvalidTransactionInitiation	<u>2 days ago</u>
	Found a new pattern that does not match existing patterns, with severity: ERROR	High	[WARNING] <*> <*> ApplicationName='lambda_transaction_handler' database_insert_time_ms=<*> HTTP_code=<*> Error'	<u>2 hours ago</u>
	Found a new pattern that does not match existing patterns, with severity: ERROR	High	[ERROR] <*> <*> Data processing of request input failed! Exception: InvalidDatetimeFormat	<u>2 hours ago</u>
	Found a new pattern that does not match existing patterns, with severity: ERROR	High	[ERROR] <*> <*> Data processing for request failed! Exception: DataException	<u>1 day ago</u>
	Found a new pattern that does not match existing patterns, with severity: ERROR	High	[WARNING] <*> <*> ApplicationName='lambda_transaction_handler' database_insert_time_ms=<*> HTTP_code=<*> Error'	<u>3 days ago</u>

AI-powered natural language query generation

PREVIEW

Easy getting started: Generate queries to interact with your Logs and Metrics by asking questions in natural language

Develop query expertise: Provides line by line explanation of the generated query to help you learn the syntax

Iterative deep dives: Update existing queries with natural language instructions for guided query iteration

Preview available in US East (Virginia) and US West (Oregon)

The screenshot displays the AWS CloudWatch Logs Insights console. At the top, it shows the breadcrumb 'CloudWatch > Logs Insights' and a 'Monitoring account' indicator. The main heading is 'Logs Insights' with a 'Start tailing' button. Below this, there are filters for time range (5m, 30m, 1h, 3h, 12h, Custom) and 'Compare (Off)' and 'Local timezone'. A dropdown menu is open, showing 'Select up to 50 log groups.' and a 'Browse log groups' button. The query editor contains the following query:

```
1 fields @timestamp, @message, @logStream, @log
2 | sort @timestamp desc
3 | limit 20
```

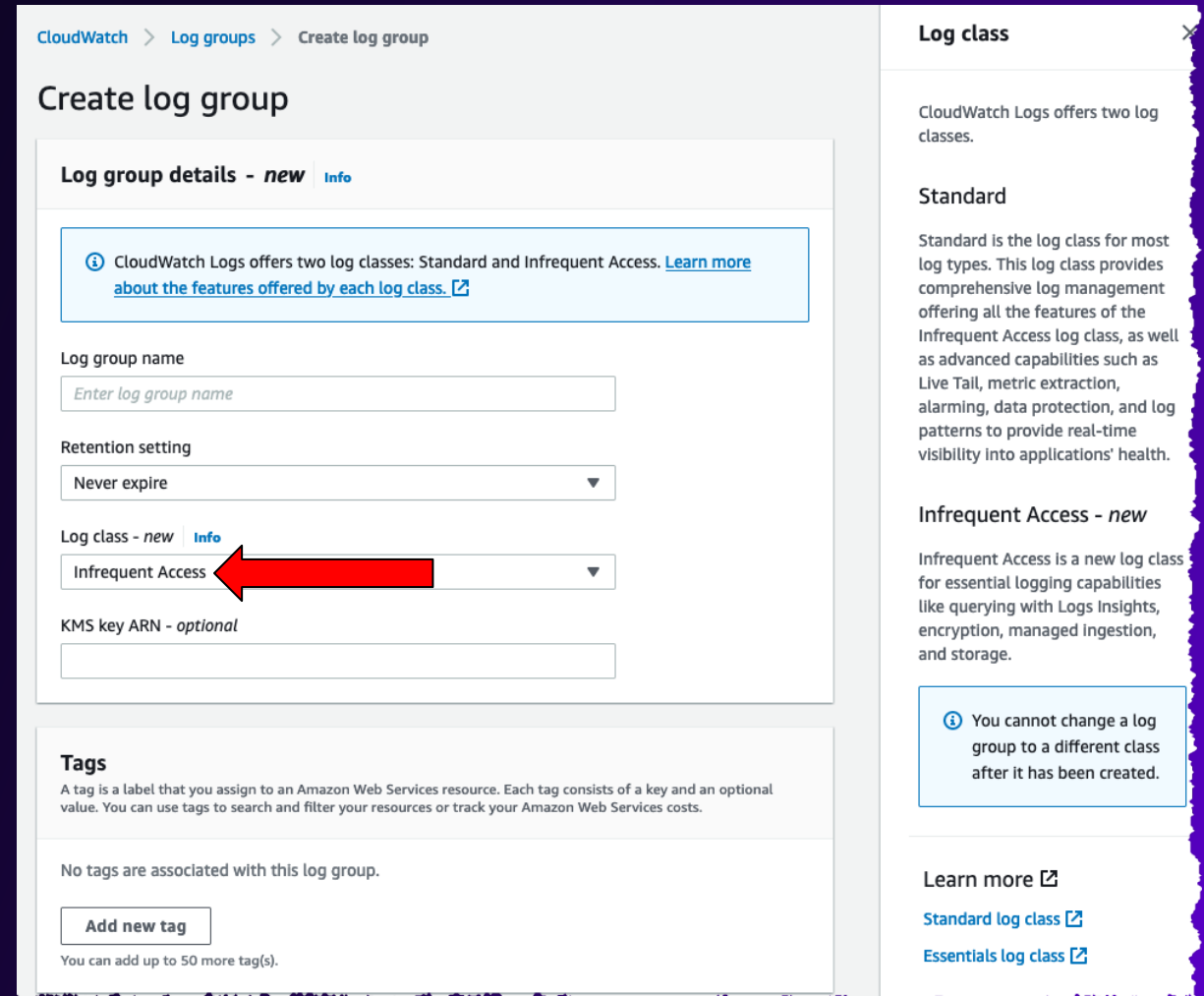
Below the query editor is an 'Assist - new' button. At the bottom of the editor are buttons for 'Run query', 'Cancel', 'Save', and 'History'. A note states: 'Logs Insights query can run for maximum of 60 minutes.' Below the editor are tabs for 'Logs (-)', 'Patterns (-) - new', and 'Visualization'. The 'Logs (-)' tab is active, showing 'Export results' and 'Add to dashboard' buttons. The main content area displays 'No results' and the instruction 'Run a query to see related events'.

CloudWatch Logs Infrequent Access

Some use cases require advanced capabilities such as metric extraction or live tailing

Many use cases require core logging capabilities such as encryption and queries

New logging class allows customers to make effective cost and feature trade-offs



CloudWatch > Log groups > Create log group

Create log group

Log group details - new [Info](#)

CloudWatch Logs offers two log classes: Standard and Infrequent Access. [Learn more about the features offered by each log class.](#)

Log group name

Retention setting
Never expire

Log class - new [Info](#)
Infrequent Access

KMS key ARN - optional

Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

[Add new tag](#)

You can add up to 50 more tag(s).

Log class

CloudWatch Logs offers two log classes.

Standard

Standard is the log class for most log types. This log class provides comprehensive log management offering all the features of the Infrequent Access log class, as well as advanced capabilities such as Live Tail, metric extraction, alarming, data protection, and log patterns to provide real-time visibility into applications' health.

Infrequent Access - new

Infrequent Access is a new log class for essential logging capabilities like querying with Logs Insights, encryption, managed ingestion, and storage.

You cannot change a log group to a different class after it has been created.

[Learn more](#)

[Standard log class](#)

[Essentials log class](#)

Efficient operations

CLOUDWATCH LOGS INFREQUENT ACCESS

CloudWatch > Log groups > Create log group

Create log group

Log group details - new [Info](#)

Log group details - new [Info](#)

CloudWatch Logs offers two log classes: Standard and Infrequent Access. [Learn more about the features offered by each log class.](#)

Log group name

Retention setting

Log class - new [Info](#)

KMS key ARN - optional

Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

[Add new tag](#)

You can add up to 50 more tag(s).

Log class

CloudWatch Logs offers two log classes.

Standard

Standard is the log class for most log types. This log class provides comprehensive log management offering all the features of the Infrequent Access log class, as well as advanced capabilities such as Live Tail, metric extraction, alarming, data protection, and log patterns to provide real-time visibility into applications' health.

Infrequent Access - new

Infrequent Access is a new log class for essential logging capabilities like querying with Logs Insights, encryption, managed ingestion, and storage.

You cannot change a log group to a different class after it has been created.

[Learn more](#)

[Standard log class](#)

[Essentials log class](#)

US-EAST-1

Standard Log Class
\$0.50 per GB

Infrequent Access Log Class
\$0.25 per GB

CloudWatch Logs Infrequent Access

	Standard	Infrequent Access
Full managed ingestion and storage	Yes	Yes
Cross-account	Yes	Yes
Encryption with AWS KMS	Yes	Yes
Log Insights	Yes	Yes
Log anomalies	Yes	No
Live Tail	Yes	No
Metrics filters and extraction	Yes	No
Data protection	Yes	No
Data ingestion pricing (us-east-1)	\$0.50 per GB	\$0.25 per GB

CloudWatch Multi Data Source Querying

Seven managed data sources available to get you started quickly

Gain visibility into hybrid and multicloud metric data in a single location

You can also create your own connector using AWS Lambda

The screenshot displays a grid of seven data source connectors in the CloudWatch console. Each connector card includes a title, a brief description, and a representative icon. The connectors are:

- Amazon OpenSearch** (checked): Leverage the Amazon OpenSearch Service search and analytics engine to derive metrics from logs and traces. Icon: Purple magnifying glass over a gear.
- Amazon Prometheus** (unchecked): Query the metrics from one of your Amazon Managed Service for Prometheus workspaces. Icon: Pink Prometheus logo.
- Amazon RDS - MySQL** (unchecked): Turn data stored in your Amazon RDS tables into metrics using SQL. Icon: Purple MySQL database icon.
- Amazon RDS - PostgreSQL** (unchecked): Turn data stored in your Amazon RDS tables into metrics using SQL. Icon: Purple PostgreSQL database icon.
- Amazon S3 - CSV** (unchecked): Display metrics data from a CSV file stored in an Amazon S3 bucket. Icon: Green bucket icon.
- Custom - getting started template** (unchecked): Starting point to create your own connector. Icon: Orange AWS Lambda icon.
- Azure Monitor** (unchecked): Query the metrics of your Azure Monitor account. Icon: Blue cloud icon.
- Prometheus** (unchecked): Query the metrics of your own Prometheus installation. Icon: Red Prometheus logo.

CloudWatch Multi Data Source Querying

Amazon Prometheus [Info](#)

Fill in the following form to configure your data source.

Data source name

The name will allow to sort your data sources alphabetically in the data source selector of the **All metrics** page.

Maximum 122 characters. Valid characters in data source name include "0-9A-Za-z-"

Workspace

VPC connection

Connect to a VPC to access private resources during invocation.

 Do not use a VPC Use a VPC

Amazon Prometheus

Query the metrics from one of your Amazon Managed Service for Prometheus workspaces.



CloudWatch Application Signals

Best practice prebuilt dashboards for service operators

Automatic integration between Application Signals and Container Insights

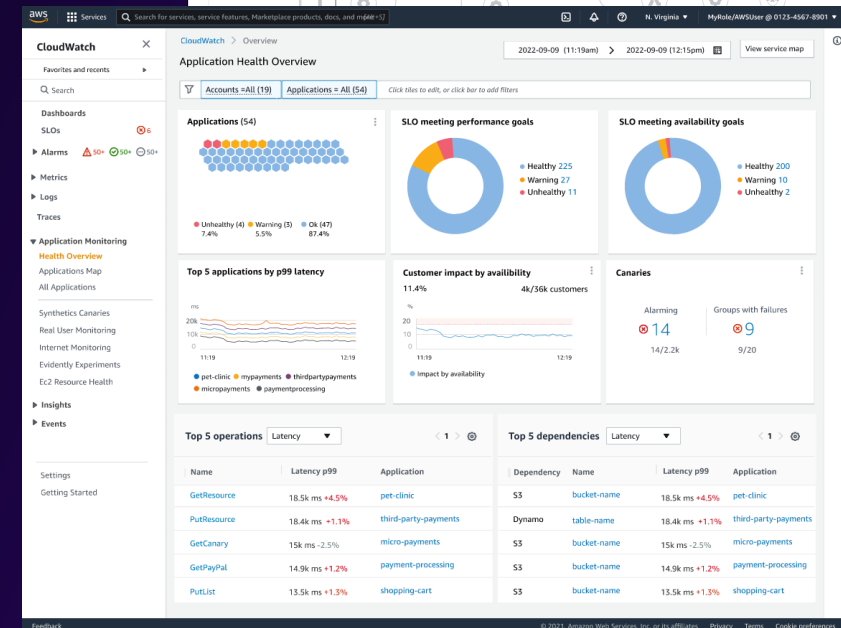
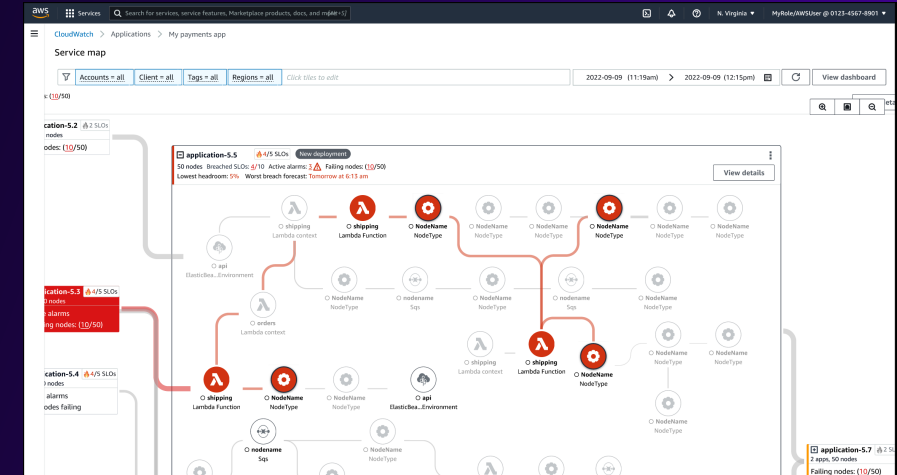
Monitor application resiliency against customer expectations and reduce alarm noise



Amazon CloudWatch Application Signals

PREVIEW

- **Out of box**, curated APM health assessment, diagnostics, **and triage experiences** across service, client, synthetic and underlying resources with a simplified container monitoring experience.
- Visualize **application topology** to better understand dependencies
- **Automatic integration** between application signals and **container insights**
- Monitor application **resiliency** against **customer expectations** and reduce alarm noise



myApplications on AWS

CENTRAL CONSOLE VIEW TO HELP MANAGE AND MONITOR ASPECTS OF YOUR APPLICATION ON AWS

The screenshot shows the AWS Console Home page. At the top, there is a navigation bar with the AWS logo, a 'Services' menu, a search bar, and a 'Select a Region' dropdown. Below the navigation bar, the main content area is titled 'Console Home' and includes a 'Reset to default layout' button and an 'Add widgets' button. The 'Applications (2)' widget is on the left, showing a 'Create application' button, a region selector set to 'us-east-2 (Current ...)', and a search bar for 'Find applications'. Below this is a table with columns for Name, Description, Region, and Origin. Two applications are listed: 'EasyLogistics' and 'HRHubApplication'. The 'Recently visited' widget is on the right, displaying a grid of service icons including Service Catalog, RDS, S3, Amazon DataZone, EC2, Systems Manager, AWS Private Certificate A..., Billing, Amazon OpenSearch Ser..., Support, Amazon Braket, and ElastiCache. A 'View all services' link is at the bottom of this widget.

Name	Description	Region	Origin
EasyLogistics	Web applicat...	us-east-2	This ac
HRHubApplication	People mana...	us-east-2	This ac

Create applications

Define applications and organize its resources

Access your applications

Quickly access applications from widgets

Compare application metrics

Compare key metrics like costs, performance, and security

Monitor & manage applications

Health and performance with alarms, canaries, SLO

AWS Control Tower Updates

DIGITAL SOVEREIGNTY, REGION DENY AND NEW CONTROL TOWER API



65 new controls to make easier to discover and validate data sovereignty requirements



Region deny feature at the OU level allowing more granular control of region usage. In support of sovereignty requirements



API based access to perform programmatic interactions with landing zone, configuring and detecting drifts, reduce time to setup, improve consistency and reduce manual overhead

AWS Compute Optimizer



GET RECOMMENDATIONS TO OPTIMIZE YOUR USE OF AWS RESOURCES

Helps avoid over- and under-provisioning

Four types of AWS resources:

EC2, EBS, ECS, Lambda

Adjust CPU headroom and threshold preferences

Limit the types of instance families/size recommendations

New 32-day lookback window (analysis period)



AWS Config, CloudTrail and Systems Manager

EXTENDING GOVERNANCE, MANAGEMENT, AND CONTROLS FUNCTIONALITY

AWS Config and CloudTrail



Config Periodic Recording caters for environments that have ephemeral resources or an elevated number of changes to be recorded



Ability to search AWS resources in Config using natural language, not having to write Config queries
(Preview)



CloudTrail Lake zero-ETL to Athena for query, visualization with QuickSight fine grained access with Lake Formation

AWS Systems Manager



Automation for Low Code Runbook: Drag and drop automation actions and AWS APIs and connect them as steps, Features a guided flow, best practices, and error highlighting



Integration with CodeGuru enables security scanning giving admins confidence that scripts used by automation are safe to use
(Preview)

AWS Console-to-Code

PREVIEW

GENERATE CODE FOR CONSOLE ACTIONS



- Simple, fast and cost-effective
- Generate code from console actions in preferred format, such as CloudFormation, or AWS CDK
- Captures your actions and workflows
- Follows AWS guided best practices

Amazon Q

OPTIMIZE EC2 INSTANCE TYPE SELECTION

PREVIEW

- Get suggestions from Amazon Q when launching an EC2 instance in the console

Compare instance types

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual machines that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and the flexibility they can meet.

Currently selected instance type: t2.xlarge

Get advice on instance type selection from Amazon Q ✕

Tell us more about your requirements to generate instance type suggestions

We will use Amazon Q, a generative AI assistant, to generate instance type suggestions

Use Case

Workload type

Priority

CPU Manufacturers

Instance type	VCPU	Memory (GiB)	Storage (GiB)	Network (Gbps)
t1.micro	1	0.25	16	0.1
t2.nano	1	0.5	16	0.1
t2.micro	1	1	16	0.1
t2.xlarge	4	16	16	10

Amazon Q

Can you suggest me EC2 instance families with lowest cost for deploying Web/App Server for Web Hosting use case? Use the format below to create the final output: EC2 Instance Selection Assistant Recommends Instance Families: Comma separated list of recommended Instance Families only goes here. EC2 Instance Selection Assistant reasoning for recommendations: Bullet list of step-by-step reasoning for the EC2 Instance Selection Assistant recommendations goes here. Do not skip steps.

EC2 Instance Selection Assistant Recommends Instance Families: M7g, C7g, T4g

EC2 Instance Selection Assistant reasoning for recommendations:

1. The question asks for EC2 instance families with lowest cost for deploying a Web/App server for web hosting use case.
2. Instance families based on the Graviton platform like M7g, C7g, C6g, T4g, M6g are well suited for this workload and use case due to their high performance and lower costs

Storage



Kevin Shaw

He/Him/His
Sr. SA
Federal

Amazon S3 Express One Zone

OBJECT STORAGE FOR DATA PROCESSING AND CRITICAL APPS USING S3 DATA THAT CAN BE RECREATED



For compute-intensive workloads

A faster authentication and access model to a single zone creates a compute-optimized consumption model



Single-digit millisecond latency

One zone S3 storage class that delivers the fastest data access speed and highest performance of any cloud object storage for customers' most latency-sensitive applications



Most frequently accessed data

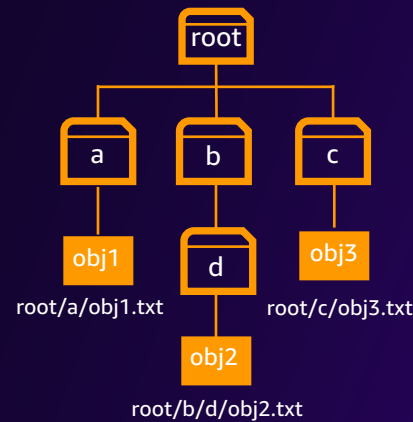
Designed for *request intensive applications* – ML training and inference, interactive analytics, media content creation



10x faster + 50% lower request costs

Data access speeds up to **10x faster**, and request costs up to **50% lower** than S3 Standard. Fully elastic with no storage provisioning and no prefix level limits (hundreds of thousands of TPS)

Enables file system-like performance on S3 using directory buckets



Ready for Partner Integration



Amazon EMR on EC2 (Spark)

Up to **4.0x** performance improvement



Amazon Athena (SQL)

Up to **2.1x** performance improvement



Amazon SageMaker (File Mode)

Up to **1.64x** performance improvement



Amazon S3 Access Grants



MAP IDENTITIES IN DIRECTORIES SUCH AS ACTIVE DIRECTORY, OR AWS IAM

- Define access permissions to data in Amazon S3 by prefix, bucket, or object
 - Map users from corporate directory
 - AWS IAM Identity Center
 - IAM principals
 - End-user identities appear in logging and auditing
 - Integrated with AWS analytics services
 - Amazon EMR
 - Amazon Athena
 - Data access is a three-step process





Accelerate Amazon S3 data transfer

- Up to 85% faster GETs and 71% PUTs to S3.
- This change is automatically included latest AWS CLI and Python SDK.
- S3 transfer will be accelerated by default for these instance types
 - p4d.24xlarge, p5.48xlarge and p4de.24xlarge (preview)
 - trn1n.32xlarge, trn1.32xlarge
- Want to use this on more instances? Add S3 flags to your `~/.aws/config` file or use:
 - `aws configure set default.s3.preferred_transfer_client crt`
- You can set it manually

Amazon EFS price and performance updates



SERVERLESS, FULLY ELASTIC, NFS FILE STORAGE

- New Amazon EFS Archive storage class
 - Available in EFS Elastic throughput mode only,
- Amazon EFS Infrequent Access (IA) storage class price reduced by 36%
 - All EFS throughput modes
- Now supports up to 250,000 read IOPS and up to 50,000 write IOPS per file system
- Amazon EFS Replication now supports failback

AWS Backup updates

CENTRALLY MANAGE AND AUTOMATE DATA PROTECTION



- AWS Backup now supports Amazon Elastic Block Store (EBS) Snapshots Archive



- AWS Backup launches support for restore testing



AWS B2B Data Interchange



AUTOMATE AND TRANSFORM ELECTRONIC DATA INTERCHANGE (EDI) DOCUMENTS AT SCALE

- Translate EDI documents stored in Amazon S3
- Supports open representation formats like XML or JSON.
- Save time and costs by reusing mapping templates for multiple transactions across trading partners
- Pair with AWS event-driven services



AWS Elastic DR validation automation



SCALABLE, COST-EFFECTIVE APPLICATION RECOVERY TO AWS

- AWS Elastic Disaster Recovery (AWS DRS) provides recovery of on-premises and cloud-based servers
- Automate validations when launching EC2 instances for recovery and drills
- Use the post-launch actions feature to perform a validation
 - Includes Amazon-provided pre-defined actions
 - Configure many in desired sequence order
 - Executed via AWS Systems Manager documents
 - i.e. Windows PowerShell or Linux shell scripts



Honorable Mentions

STORAGE

- Mountpoint for Amazon S3 CSI driver is now generally available
- Mountpoint for Amazon S3 now supports the Amazon S3 Express One Zone storage class
- Amazon FSx for ONTAP now supports creating Multi-AZ file systems in Shared VPC participant accounts
- Amazon FSx for OpenZFS now supports on-demand data replication across file systems



Compute and Containers



Jeff Hunter

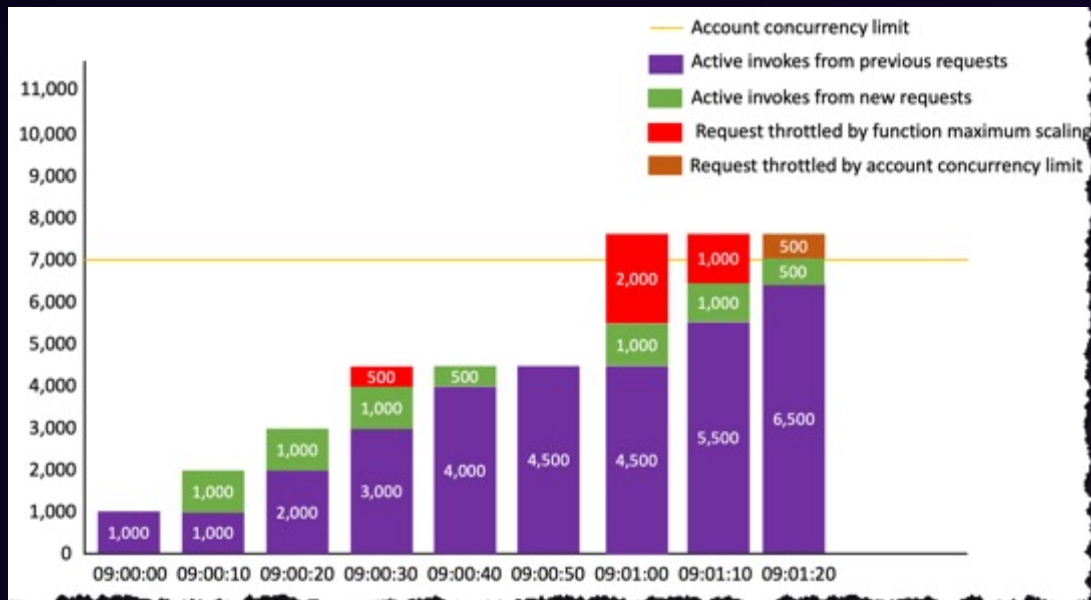
He/Him/His

Sr. SA

Federal

Lambda Scaling Improvements

HIGH VOLUME AND RAPID SCALING LAMBDA IS EVEN FASTER AT SCALING YOUR INVOCATIONS



This graph shows a function receiving requests and processing them every 10 seconds with an account concurrency limit set to 7,000 concurrent requests. Each function scaling-up rate is fixed to 1,000 concurrent executions every 10 seconds.



Scale up at a 12x faster rate



Scale up to a rate of 1,000 concurrent executions every 10 seconds (to account concurrency limit)



Available in all commercial AWS Regions



Enabled by default for all functions that are invoked synchronously, at no additional cost.

AWS Application Composer for VS Code

DRAG-AND-DROP INTERFACE FOR APPLICATION DESIGN IN YOUR IDE



- Use AWS Application Composer directly in VS Code
- Quickly iterate your applications' logic and infrastructure
- Connect AWS services into an application architecture through application composer's visual canvas
- Quickly get started with any of CloudFormation's 1000+ resources



EXPLORER

UNTITLED (WORKSPACE)

- demo-1
 - src
 - demo-pub-sub.yaml



Show All Commands

Go to File

Find in Files

Start Debugging

Toggle Terminal

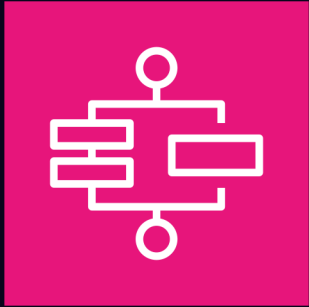
OUTLINE

TIMELINE

GO

AWS Step Functions App Composer Integration

AWS STEP FUNCTIONS WORKFLOW STUDIO IS NOW AVAILABLE IN AWS APPLICATION COMPOSER



- Unified visual infrastructure as code builder
- Seamless transition between authoring workflows and defining resources
- Create and manage all resources at any development stage
- Visualize full application in AWS Application Composer
- Zoom into the workflow details all in a single interface

AWS Step Functions Updates



BEDROCK APIS, EXTERNAL ENDPOINTS & TESTING OF TASK STATES

- Integrate 3rd party APIs and services like Stripe, GitHub and Salesforce
 - No longer need Lambda function to call endpoints
- New Test States API
 - Test your task states individually without the need to deploy or execute the state machine
- Optimized Integrations for Amazon Bedrock
 - Invoke a model and run inferences with provided input
 - Text, image and embedding models
 - Create fine tuning jobs to customize a base model

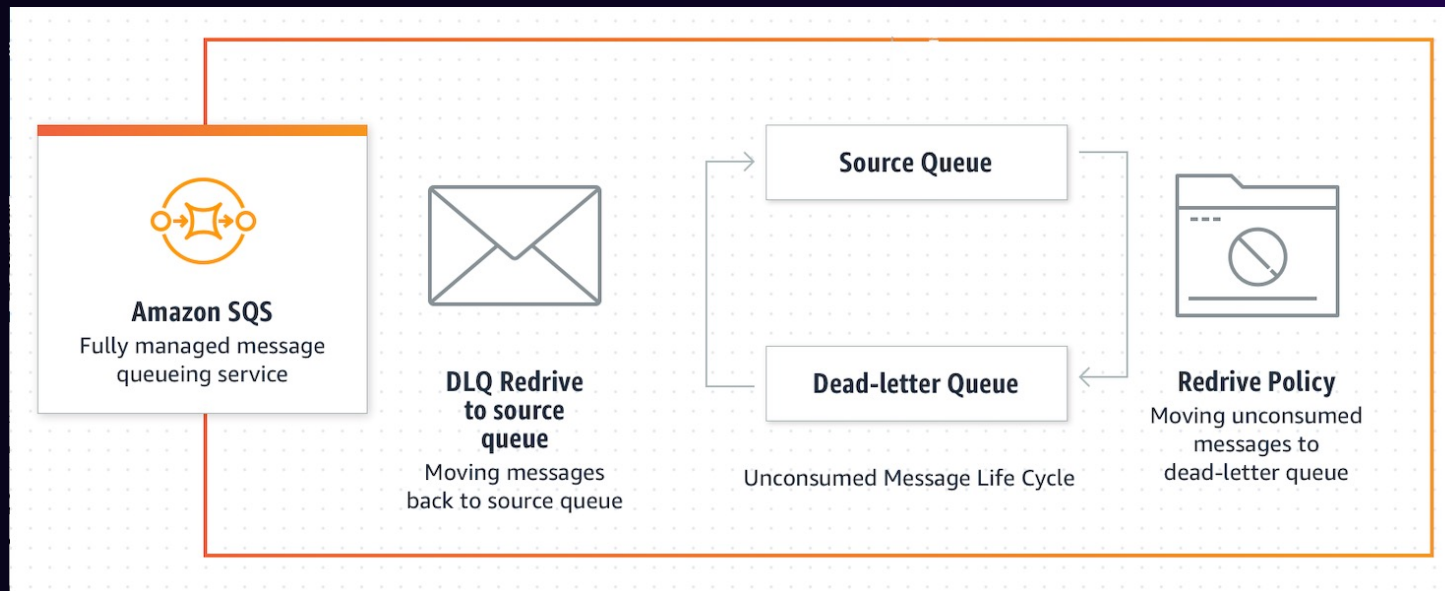


Amazon SQS FIFO Queue Updates



SQS FIRST-IN, FIRST-OUT QUEUES

- Process up to 70,000 TPS per API action
 - Available in US East (N. Virginia), US West (Oregon), and Europe (Ireland)
- Dead letter queue redrive support for Amazon SQS FIFO queues



Honorable Mentions

COMPUTE

- [Preview] Amazon EC2 High Memory U7i instances
- [Preview] New Amazon EC2 R8g instances powered by AWS Graviton4 processors
- New NVIDIA GPU-based Amazon EC2 instances
- Amazon EC2 Trainium2 Instances
- ENA Express supports 58 new instances with sizes as small as 16 vCPUs



Prometheus Agentless Collector – Amazon EKS

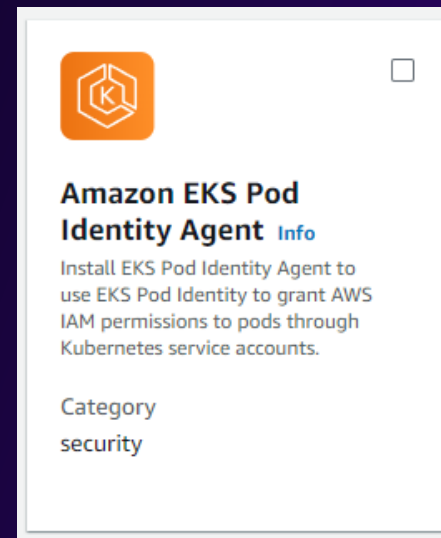
- Fully Managed agentless collector
- Removes undifferentiated heavy lifting
- Automatically **Discover** and **Collect** metrics for:
 - Amazon EKS
 - Infrastructure
 - Kubernetes ApiServer



Amazon EKS Pod Identities

- Simplifies how cluster administrators configure Kubernetes applications to obtain AWS IAM permissions
- Enhancements:
 - Independent Operations
 - Reusability
 - Scalability
- Available as an EKS Add-on

```
"Principal": {  
  "Service": "pods.eks.amazonaws.com"  
}
```



Amazon EKS Upgrade Insights

- Provides insights into impact of a successful upgrade of a cluster
- Built on Best Practices
- Scans clusters against a list of potential Kubernetes version upgrades

Upgrade insights (1) [Info](#)

The table below lists the insight checks performed by EKS against this cluster, along with their associated statuses. EKS automatically refreshes the status of each Insight, which can be seen in the last refresh time column.

Q Filter insights by name, version or status < 1 >

Name	Insight status	Version	Last refresh time (UTC-05:00)	Last transition time (UTC-05:00)	Description
Deprecated APIs removed in Kubernetes v1.29	✔ Passing	1.29	3 hours ago	November 23, 2023, 11:19	Checks for usage of deprecated APIs that are scheduled for removal in Kubernetes v1.29. Upgrading your cluster before migrating to the updated APIs supported by v1.29 could cause application impact.



Amazon EKS simplified controls

- Supports EKS clusters and Kubernetes Objects directly from an API
- Define Access Management configurations using IaC tool
 - Cloudformation
 - Terraform
 - AWS Cloud Development Kit (CDK)



Amazon EKS Cluster Health Status Details

- Provides diagnose, troubleshooting, and remedy issues with Amazon EKS clusters
- Provides information about
 - Issue Types
 - Descriptions
 - Affected resources in the cluster

Health issues (1)		
Issue type	Description	Affected resources
AccessDenied	EKS cluster role doesn't have sufficient permission on resources associated with your cluster.	arn:aws:kms:us-east-1:██████████:key/deede606-fb0f-██████████



Thank you!



Please complete the session survey



Dan Girard
Security



Dave Wood
Security
Networking



Bobby Hallahan
Cloud
Operations



Kevin Shaw
Storage



Jeff Hunter
Compute
Containers

