Speaker 1 (00:00):

This is episode 602 of the AWS Podcast released on July 10th, 2023. Podcast confirmed. Welcome to the official AWS Podcast.

Simon Elisha (00:16):

Hello and welcome back to the AWS Podcast. Simon Elisha with you, great to have you back. And I'm joined by of course, my two very good co-hosts. Firstly, Hawn Nguyen-Loughren. G'day Hawn, how you on doing?

Hawn Nguyen-Loughren (00:25):

Doing awesome.

Simon Elisha (00:26):

That's great. And Jillian Forde, how are you doing?

Jillian Forde (00:29):

G'day, Simon. I only say that when you say g'day. We don't say that in the US.

Simon Elisha (00:34):

Yeah, it wouldn't work otherwise.

Jillian Forde (00:35):

But I want to, though, now when I hear you say it.

Simon Elisha (00:38):

Well you can. There's no reason why you can't. And we probably will get your bells today that we've been talking about the last two episodes. They might actually appear live on the show, because we started a little bit earlier today, so we'll have to see if they peel out.

Jillian Forde (00:52):

That's right. Yeah, they're they're coming in. They're always excited for the update show.

Simon Elisha (00:57):

Exactly. Well we have lots and lots of updates, though. I think there's about 84 different things to cover, so we will move at a fairly rapid clip.

(01:05):

Firstly, we'll talk a bit about some of the analytics updates. AWS Glue Studio now provides data previews for Glue streaming jobs, and AWS Glue can now detect 250 sensitive entity types from over 50 countries. So that's really useful for PIR and that sort of stuff.

(01:23):

Amazon Redshift has improved the experience for encrypting the data warehouse, and it provides comprehensive encryption capabilities to protect your data at rest. Now it further enhances the experience of encrypting the warehouse with RA3 node types by reducing the overall encryption time

and improving the availability of the warehouse during the encryption process. It's at least five times faster. That's a big speed increase.

(01:49):

Amazon EMR now publishes events for insufficient instance capacity errors. EMR on EKS now supports custom job scheduling. Now this is the addition of Volcano and Apache Unicorn as job schedulers when running EMR on EKS using Spark Operator and Spark Submit. Now Amazon EMR on EKS enables customers to run open source big data frameworks like Apache Spark on Amazon EKS, and using a custom job scheduler for Spark Jobs lets you have fine grain capacity management and faster pod provisioning at scale. And EMR on EKS now also supports container log rotation for Apache Spark, and EMR also supports price capacity optimized allocation strategies for EC2 Spot instances. My regular reminder that if you're not using Spot, you should.

(02:39):

Amazon Kinesis Data Firehose can now deliver streaming data to Amazon Redshift Serverless. So with just a few clicks, you can more easily ingest, transform, and reliably deliver streaming data into Amazon Redshift Serverless without building and managing your own data ingestion and delivery infrastructure. And a reminder, Kinesis Data Firehose is a fully managed surface that automatically scales to match the throughput of your data without ongoing administration.

(03:06):

Database Lake Formation and Glue Data Catalog now support cross region table access. So if you're working in a global, multi-region world, you're good. And Amazon Managed Grafana now supports open search Trace Analytics. In Amazon Open Search Service, you can also now skip unavailable clusters during your cross cluster search. So if it's not available, you don't go to it. And Database Clean Room has added some new capabilities to make it easier to collaborate at scale.

Jillian Forde (03:36):

Up next: application integration.

(03:39):

Serverless application developers can now build app sync powered applications in AWS Serverless Application Model with the new serverless GraphQL API Resource Abstraction.

(03:52):

AWS App Sync is a managed service that makes it easier to build scalable APIs that connect to applications to data, with a GraphQL endpoint. With a single resource, everything necessary can be provided for a typical app sync GraphQL API definition, including the API schema, the resolver pipeline functions, and data sources. SAM CLI Support is also included to allow the API schemas', the resolvers', and pipeline function's code files to automatically be packaged and uploaded to S3. Amazon MQ now supports cross region data replication for active MQ brokers.

(04:37):

And two updates from Step Functions. So AWS Step Functions launches, versions and aliases, and AWS Step Functions Ads Integration for seven services, including Amazon VPC Lattice.

(04:51):

And finally, Amazon AppFlow announces the release of four new data connectors for SaaS applications. The new data connectors enable you to transfer your data from Adobe Analytics, Blackbaud Raiser's Edge, Coupa, and Google BigQuery, providing connectivity to business planning solutions. These Amazon

AppFlow Integrations make it easier for you to enrich or hydrate your data lakes, gain actionable insights, and streamline analysis and reporting.

Hawn Nguyen-Loughren (05:24):

Now for the topic of all the things compute.

(05:26):

Amazon EC2 Instance Connect supports SSH and RDP connectivity without public IP address. I'm super excited about this one. With EC2 Instance Connect endpoint, EIC Endpoint, customers now have SSH and RDP connectivity to their EC2 instances without using public IP addresses. In the past, customers assigned public IPs to their EC2 instances for remote connectivity. With EIC endpoints, customers can have remote connectivity to their instances in private subnets, eliminating the need to use public IPV4 addresses for connectivity. Previously, customers had to create bastion hosts to tunnel SSH or RDP connections to instances with private IP addresses. Using bastion hosts involves operational overhead of patching, managing and auditing, as well as additional costs. EIC Endpoint eliminates the cost of operational overhead of maintaining bastions. EIC endpoint combines AWS Identity and Access Management, IAM, based access controls to restrict access to trusted principles with network-based controls, such as security groups rules, and provides an audit of all connections via AWS Cloud Trail, helping customers improve their security postures.

(06:37):

To get started, simply add an EIC endpoint to a subnet in your VPC with a few clicks from AWS Management Console AWS CLI or SDK. Once added, you can set up the related IAM permissions for your users and connect to your instance using a client of your choice, which is very handy and secure.

Simon Elisha (06:56):

It is. I actually used this yesterday, Hawn, and super easy to set up, and just even less things to worry about, which is good.

Hawn Nguyen-Loughren (07:03):

And less painful, too. You don't have to set up a bastion host. Win.

Simon Elisha (07:07):

Love it.

Hawn Nguyen-Loughren (07:07):

Awesome. Amazon EC2 Dedicated Host now supports targeted allocations in AWS Outposts rack.

(07:15):

AWS Lambda supports starting from timestamp for Kafka event sources. AWS Lambda now supports starting from specific timestamp when using Amazon Managed Streaming for Apache, Kafka, MSK, or self-managed Kafka as event source. Previously, Kafka event source mapping could only have starting positions from TRIM_HORIZON or LATEST. Now with starting from a timestamp, you can start processing messages at a precise point in time. This is useful for a situation like disaster recovery where you need a new consumer to quickly start processing where you previously left off, which is crucial for transactional level resiliency.

(07:53):

Announcing Amazon EC2 Hpc7g instances. AWS announces the general availability of Amazon Elastic Compute Cloud Amazon EC2 Hpc7g instances. Amazon EC2 Hpc7g instances are powered by AWS Graviton processors, which are custom arm-based processor designed by AWS.

(08:14):

Arm-based architecture are known for their high core counts with better performance per watt and energy efficiency, owing to simple instruction risk that generate less heat, offering better heat dispensation. EC2 Hpc7g instances deliver up to 60% better performance over comparable previous generation instances for compute-intensive, high-performing compute Hpc workloads, such as weather and computational fluid dynamics, CFD.

(08:42):

Announcing Amazon EC2 7g in Instances, generally available. And this is powered by the latest generation AWS Graviton processors. Amazon EC2 7g in Instances features the fifth generation AWS Nitro cards, and deliver the highest network bandwidth. The best packet processing performance, and the best price performance for network intensive workloads.

PART 1 OF 4 ENDS [00:09:04]

Hawn Nguyen-Loughren (09:00):

And the best price performance for network intensive workloads. C7gn instances offer up to 200 gigabyte network bandwidth and up to 3x higher packet processing performance per VCPU versus comparable current generation X86 base network optimized instances.

(09:18):

Amazon EC2 C7gn instances are built on AWS Nitro System. The Nitro System is a collection of AWS design hardware and software innovation that enables the delivery of efficient and flexible cloud service with enhanced security, isolated multi-tenancy, private networking, and fast local storage.

(09:39):

Introducing Amazon EC2 M7a instances preview. Elastic Network Adapter (ENA) Express now supports 10 new instances. ENA Express is a networking feature that uses AWS scalable reliable diagram SRD protocol to improve network and performance in two key ways: higher single flow bandwidth and lower tail latency for network traffic between EC2 instances.

(10:04):

SRD is a proprietary protocol that delivers these improvements through advanced congestion control, multi-pathing, and packet reordering directly from the Nitro card, which is wicked cool.

(10:16):

And ECR Basic Scanning now uses version three of common vulnerability scoring system, CBSS framework. Amazon ECR Elastic Container Registry Basic Scanning feature will use common vulnerability scoring system, CVSS version three information where determining the severity for new common vulnerabilities and exposure, CVEs.

(10:37):

This enables customers to get the most recent severity information for vulnerabilities in their ECR container images. We use CVSS information to determine the severity of a vulnerability when the upstream distribution source code does not have this information. I'm really excited about this one because some of my customers are always looking for ways to secure their containers.

Jillian Forde (10:57):

We've got four updates on customer engagement and four from the Amazon Connect team. This includes reductions of Australia toll-free inbound minutes by 54%, from 0.054 cents per minute to 0.025 cents per minute. And New Zealand toll-free inbound minutes by 52%, from 0.2205 cents per minute to 0.1069 cents per minute. Amazon Connect Contact Lens now offers screen recording. And Amazon Connect now publishes new contact lifecycle events for callbacks. And Amazon Connect launches search APIs for three more resources.

Simon Elisha (11:46):

Awesome. Cool updates there. Let's move into the world of storing your data in a database.

(11:52):

We are now launching the preview of the AWS database encryption SDK, which is an update to the existing Amazon DynamoDB encryption client, which enables you to include client-side encryption in your DynamoDB workloads.

(12:05):

With this launch, you can more easily perform attribute level encryption, enabling you to encrypt specific attribute values before storing them in your DynamoDB table. This lets you protect sensitive data in transit and in rest as data cannot be exposed unless decrypted by your application.

(12:22):

This new release also lets you easily search on encrypted attributes without decrypting the entire database beforehand. So this lets you find the right information quickly to download your application while your data remains securely encrypted within the database.

(12:36):

The AWS database encryption SDK makes it easy to let your customers bring their own encryption keys to your application, giving them direct ownership over their data by controlling the encryption key designed with multi-tenancy in mind, you can use the different encryption key providers across a single database table to safely isolate data.

(12:54):

In conjunction with AWS key management service, you can use the KMS key policies to enforce clear separation between the authorized users who can access specific encrypted attributes and those who cannot. Now, this is compatible with Amazon DynamoDB and is available in Java under the developer preview.

(13:12):

Amazon RDS for SQL Server now supports minor versions 2014, 2016, 2017 GDR, 2017 CU31 GDR, and 2019 CU20. And Amazon RDS for MariaDB supports minor versions 10.6.14, 10.5.21, and 10.4.30. And Amazon RDS for MySQL supports minor versions at 5.7.42 and 8.033. And Amazon RDS for Oracle now supports migration via RMAN Transportable Tablespaces.

(13:43):

Now those quick set of updates is really a reminder to you to keep patching your stuff. Remember, if you use RDS, you can set it to automatically do minor upgrades during maintenance windows of your own choosing.

Hawn Nguyen-Loughren (13:57):

And for one of my favorite topics, developer tools. Announcing nightly builds of Amazon Corretto. Amazon Corretto nightly builds are now available at downloads.corretto.aws for Linux, Windows, and Mac platforms.

(14:10):

Developers can now test the latest OpenJDK community code and bug fixes without waiting for the next quarterly release. Binaries for Corretto 8, 11, 17 and the latest feature release, Corretto 20 are being built, combining the latest stable end development code from the next release of the OpenJDK projects.

(14:28):

Early access builds of upcoming releases will also be available prior to GA. Release and fast debug builds, which contains assertion on JVM state and correctness are also available.

(14:40):

And Amazon Code Guru Security is now available in preview. AWS announces the preview release of Amazon CodeGuru Security, a static application security testing SAST tool that uses machine learning to help you identify code vulnerabilities and provide guidance you can use as a part of remediation. CodeGuru Security also provides in-contact code patches for certain classes of vulnerabilities, helping you reduce the effort required to fix code vulnerabilities.

(15:08):

I really like this one because by performing deep, semantic analysis of your application code, CodeGuru Security detects vulnerabilities with a low false positive rate, enabling your engineering and security teams to be more efficient while triaging findings.

(15:23):

CodeGuru Security flags a wide range of issues such as log injection, hard-coded credentials and resource leaks, and is designed to integrate at different stages of the development workflow like Code Repository, CIC Pipeline, container registry, et cetera.

Jillian Forde (15:39):

Up next, front end web and mobile. This one is really handy for startups that are building React apps. So, AWS Amplify announces the UI builder Figma plugin, empowering design and development teams to seamlessly collaborate within a Figma file.

(15:56):

Use this plugin within the Amplify UI kit to easily theme your components, upgrade to new UI kit versions, and generate and preview React code from your designs directly in Figma.

(16:11):

So go from design to code in seconds by generating clean rack code directly inside Figma and see a live preview of the code running before adding it to your application. Then open the code in Codesandbox for easy editing and reviewing. Or copy the code and add to your React application to get pixel perfect front end code.

(16:32):

Amazon Location Service adds support for place categories and Amazon Location Service now support geofence metadata.

Hawn Nguyen-Loughren (16:42):

And for machine learning, Amazon SageMaker inference recommended now in AWS console gives recommendation at model creation, which is awesome sauce.

(16:53):

Transform data into ML feature using SageMaker feature store feature processing.

(16:59):

Amazon Personalized now supports filtering selected items by properties of the input item.

(17:05):

Amazon Personalized now supports VPC endpoints.

(17:09):

And Amazon Recognition improves face search accuracy with user vector, which is really neat.

Simon Elisha (17:17):

Now moving on to controlling all the things management and governance. AWS Security Hub announces enhanced management capabilities with AWS CloudFormation.

(17:26):

There is now the ability to have tagging support for AWS purchase order management. And this is the general availability of attribute-based and resource-based access control for purchase orders created in the AWS console.

(17:40):

This launch allows you to tag your POs that are created on the AWS console and control access to a resource level with IM policies. The AWS console also offers the ability to manage those resource tags.

(17:53):

AWS CloudFormation launches a new perimeter on stack failure for the create change set API that allows customers to control the rollback behavior of change sets.

(18:02):

Customers use change sets.

PART 2 OF 4 ENDS [00:18:04]

Simon Elisha (18:00):

... control the rollback behavior of Changesets. Customers use Changesets to preview the impact of a stack operation on active resources, and customers can deploy Changesets with an execute change set operation. With this launch, customers can modify the actions that cloud formation will take when change set execution is unsuccessful. This allows customers to reduce manual intervention during retries of change set executions. And AWS config now supports 21 more resource types for services including AWS Amplify, AWS App Mesh, App Runner, AppStream 2.0, Keyspaces for Apache, Cassandra, Code Artifact, Elastic Compute Cloud, et cetera, et cetera. There's a lot more in there. Amazon CloudWatch Logs announces a new log insights dedup command, so you can pull out those duplicates when you don't need them. And AWS Systems Manager quick setup enables automatic updates for EC2 launch agents. So just a few clicks and you get all the updated versions of things.

(19:02):

My friendly reminder, patch your stuff. AWS Trusted Advisor adds new fault tolerance checks to make sure all the best things are happening in your account. And we're happy to announce simplified cross account management of operational issues in a AWS Systems Manager Ops Center. So again, much easier to view across an entire organization. Available now is the general availability of the integration between AWS Control Tower and AWS Security Hub. You can now enable over 170 Security Hub detective controls that mapped to related control objectives from AWS Control Tower. AWS control tower now detects when you disable a control from Security Hub, which results in a drifted control state. With this drift detection capability, it's simpler for you to monitor the deployment state of your controls and take appropriate actions to manage the security posture of your AWS Control Tower environment.

(19:54):

Well-Architected has introduced profiles. Now this allows customers to tailor their Well-Architected reviews based on their business goal. This feature creates a mechanism for continuous improvement by encouraging customers to review their workloads with certain goals in mind first, and then complete the remaining Well-Architected review questions. So customers can create a profile by answering a set of predefined questions related to the current business goals. Once the profile is applied to a workload, customers are then presented with a set of prioritized, well-architected questions that are aligned to their desired outcomes. Customers can also share their profiles with other accounts and with AWS organizations to help them scale their business priorities across their organization.

(20:35):

This is super important. If you're not using Well-Architected, it's a free tool in your account. You should use it because it asks those really interesting questions about how your system is built and operated. But often there's too many questions and you're sort of like, well, which ones do I pay attention to? This helps you with that. AWS CloudTrail Lake has launched curated dashboards for visualizing the top cloud trail trends. AWS Control Tower has added 10 new AWS Security Hub Controls, and we're really excited to announce service scoped free tier pricing rules for a AWS billing conductor.

Jillian Forde (21:08):

We've got one update on media services. So AWS Elemental Media Convert releases bandwidth reduction filter for HEVC and AVC. Now on to migration and transfer. AWS Application Discovery Service introduces Amazon EC2 recommendations. AWS Transfer Family now supports Quantum Safe Public Key Exchange for SFTP file transfers. Quantum Safe Public Key Exchange helps protect your file transfers from threats such as Harvest Now, Decrypt Later attacks that record present day traffic from decrypting once cryptographically relevant Quantum computers become available. AWS Transfer Family has earned the official Drummond Group AS2 cloud certification seal. Drummond Group is an independent provider of testing and certification services for various industry standards and protocols. This certification verifies that AWS Transfer Family's AS2 capabilities are compatible and interoperable with 14 third party AS2 vendors commonly used for B2B communication. And AWS transfer Family announces structured JSON log format.

Simon Elisha (22:33):

Some quick updates in the world of networking and content delivery. Amazon VPC CNI now supports IPv6 egress for pods in IPv4 enabled kubernetes clusters. AWS Elastic Disaster Recovery now supports VPC configuration recovery, and AWS Verified Access adds a new logging functionality to improve troubleshooting.

Jillian Forde (22:57):

Now partners. So AWS Partners now have deeper insights into their AWS business through the AWS Partner Analytics Dashboard, which is accessible from AWS Partner Central. The dashboard provides Alliant leads for partners at the validated or differentiated with a 360 degree view of their AWS business, including opportunity pipeline, funding benefits and pipeline revenue. And we are excited to highlight AWS Partner Software Solutions with AWS Built-in, including new infrastructure as code that integrates automatically with AWS Foundational Services to help customers achieve their long-term goals in the cloud.

(23:41):

AWS Built-in software uses a well architected modular code repository designed to add value to partner software solutions. AWS Built-in partner solutions, leverage key building blocks called Cloud Foundational Services across multiple domains such as identity, security and operations. AWS Built-in Partner Solutions minimize the time it takes for a customer to figure out the best AWS services to adopt. Regardless of use case or category, partners help determine the best foundational AWS services to maximize the performance of their software and bring the most value to the customer experience. By streamlining the integration process, we empower customers to fully harness the benefits of foundational AWS native services while taking advantage of the rich functionality and capabilities of AWS Partner Software Solutions.

Hawn Nguyen-Loughren (24:38):

Now, for our highest priority topic. Security, identity and compliance, AWS announces AWS Payment Cryptography. Now this is very useful for some of my FinTech customers, especially in the payment space, because this service simplifies your implementation of cryptography operation used to secure data in payment processing application for debit, credit and stored value cars in accordance with various Payment Card Industry, PCI, network, and American National Standard Institute, ANSI, Standards and Rules. Financial service providers and processors can replace their on-premises hardware security module, HSM, with this elastic service and move their payment specific cryptography and key management function to the cloud. AWS Payment Cryptography also streamlines payment key management by generating keys, importing and exporting through electronic means, and automating key management, store, rotate, backup and recovery. AWS Payment Cryptography can help you meet your compliance need by managing the underlying physical HSM infrastructure and key management requirements.

(25:43):

Additionally, this service can help you by integrating with AWS tools for authorization, AWS Identity and Access Management and auditing AWS collateral. Amazon inspector announces the general availability of code scan for AWS Lambda function. Amazon Inspector now supports code scanning of Lambda function, expanding the existing capability to scan Lambda functions and associate layers for software vulnerabilities in application package dependencies. With this expanded capability, Amazon Inspector now also scan your custom proprietary application code within a Lambda function for code security vulnerabilities, such as injection flaws, data leaks, weak cryptography, or missing encryption based on AWS Security best practices.

(26:27):

AWS announces software bill of materials export capability in Amazon Inspector. Amazon Inspector now offers the ability to export consolidated Software Bills Of Material, SBOMs, for all Amazon Inspector monitored resources across your organization, in industry standard formats including Cyclone DX and

SPDX. With this new capability you can use automated and centrally managed SBOMs to gain visibility into key information about your software supply chain. This includes details about software packages used in the resource along with associated vulnerabilities.

PART 3 OF 4 ENDS [00:27:04]

Hawn Nguyen-Loughren (27:00):

... Resource along with associated vulnerabilities. Amazon Verified Permission is now generally available. [inaudible 00:27:08] is announcing the general availability of Amazon Verified Permission, service for fine grain authorization and permission management for application that you built. Verified Permission use Cedar, and open source language for access control, allowing you to define permissions as easy to understand policy, use Verified Permission to support role and attribute based access control in your applications. Now this is really cool because you can use Verified Permissions to decouple permissions from your application logic and build more secure applications faster with centralized policy stores, reusable policy templates, and policy testing. AWS IAM Identity Center now supports automated user provisioning for Google Workspaces. Amazon Detective extends finding groups to Amazon Inspector. Amazon Guard Duty enhances console experience with finding summary view. AWS WAF Fraud Control announces account creation fraud prevention, a managed protection for AWS WAF that is designed to prevent creation of fake or fraudulent accounts.

(28:08):

Fraudsters use fake accounts to initiate activities such as abusing promotional and signup bonuses, impersonating legitimate users, and carrying out phishing attacks. These activities can lead to several direct or indirect costs, such as damage customer relationships, reputational loss, and exposure to financial fraud. Account Creation Fraud Prevention protects your account signup or registration pages by allowing you to continuously monitor requests for anonymous digital activity and automatically block suspicious requests based on request identifiers and behavioral analysis. I really like this one for that extra layer of protection. AWS Security Hub announces enhanced management capabilities with AWS Cloud Formation, announcing general availability of AWS controlled towers, integration with Security Hub. AWS Control Tower adds 10 new AWS security hub controls. AWS Security Hub launches six new security controls, and announcing AWS Security Hub automation rules. AWS Security Hub, a cloud security posture management service that performs security best practices, checks, aggregate alerts, and facilitates automated remediation, now features a capability to automatically update or suppress findings in near real time.

(29:21):

You can now use automation rules to automatically update various fields and findings, suppress findings, update findings' severity and workflow status at notes and more. Announcing third party risk and CSV exports in AWS Audit Manager. And finally, announcing the AWS Global Partner Security Initiative. AWS announces the AWS Global Security Initiative, which provides global systems integrators, GSI partners, the opportunity to jointly develop innovative and transformational security and compliance service with AWS, delivering on the promise of actionable security data, leveraging the power of generative AI. This initiative focused on security services and managed services for multi-cloud enterprises seeking cyber resilient environments to reduce risk and meet regulatory obligations. There are four priority use cases that are part of the AWS Global Partner Security Initiative. One, managed detection and response, MRD. Two, cyber resiliency, emergency recovery. Three, security led cloud migration. And four, continuous regulatory compliance.

Simon Elisha (30:27):

And today we're going to wrap up with the good old fashioned topic of storage. Amazon S3 announces dual layer service side encryption for compliance workload. I'm super excited for some of my customers about this one. So customers can now apply two independent layers of service side encryption to objects in Amazon S3, dual layer server side encryption with key stored in the AWS key management service is designed to meet National Security Agency, CNSSP 15, for [inaudible 00:30:57] compliance and data arrest capability package version five, which is guidance for two layers of [inaudible 00:31:03] encryption. Amazon S3 is the only cloud object storage service where customers can apply two layers of encryption at the object level, and control the data keys used for both layers. S3 features such as DSSE-KMS are vetted and acceptance views on top secret workloads, which benefits all customers globally. DSSE-KMS simplifies the process of applying two layers of encryption to your data without having to invest in infrastructure required for client site encryption.

(31:32):

Each layer of encryption uses a different implementation of the 256-bit advanced encryption standard with Galois/Counter Mode, the ASGC algorithm. DSS-KMS uses AWS key management service to generate data keys, allowing customers to control their customer managed keys by setting permissions per key and specifying key rotation schedules. With DSSE-KMS, customers can now query and analyze their dual encrypted data with AWS services such as Amazon Athena, Amazon SageMaker, and more. So check that one out. And Amazon EFS now supports up to 10 gigabytes of provision throughput. So this is an increase to the maximum by three times. With this launch, you now have a cost-effective way to drive up to 10 gigabits of a read throughput and three gigabits of write throughput for workloads, including machine learning, data processing analytics, and transcoding that demand consistent and high levels of throughput performance. So there we go. A magical mystery tour through 84 different updates, and I think we did it in a reasonable time. And a reminder that there is always the link to all the items in the show notes. So if you want to dive deep on some of those headlines, you can. Hon what was your favorite thing and how do people get in touch with you?

Hawn Nguyen-Loughren (32:48):

I think my favorite thing is the, don't have to [inaudible 00:32:52] host into your EC2s anymore, and also all of the developer tools and the security tools that we have, especially with Inspector and Security. So you can reach out to me at my Twitter, @hansolo_1.

Simon Elisha (33:05):

Nice. And Jillian, same questions.

Jillian Forde (33:08):

The same as what Han said. So the Amazon Inspector with code scans for Lambda functions. I love recommending Lambda when it applies to my startups. And then anything security is always a win, so it's just a double win-win.

Simon Elisha (33:22):

And how do people find you?

Jillian Forde (33:24):

And on Twitter, you can find me at @missjillforde. So Sammy, what about you? What was your favorite?

Simon Elisha (33:30):

Yeah, so mine was the dual layer, server side encryption for S3. I just think that's just so cool, because it adds so much more security with very little effort. In fact, I had a play with it the other day and I was like, "Yeah, this is... I'm a fan."

Hawn Nguyen-Loughren (33:44):

All the things storage.

Simon Elisha (33:45):

Yeah, we love that. And if you want to reach out to me, awspodcast@amazon.com is the old school way that I like to operate. And of course, until next time, keep on building.

PART 4 OF 4 ENDS [00:33:58]