
AWS
re:Invent

SEC211

BBC: Driving security best practices in a decentralized organization

Andrew Carlson
Sr. Software Engineer
BBC

Apurv Awasthi
Sr. Product Manager
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Introductions

BBC’s secrets management landscape

BBC’s adoption journey for AWS Secrets Manager

How did the BBC benefit from Secrets Manager?

Collecting and implementing feedback



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are secrets?

- AWS credentials
- Encryption keys
- SSH keys
- Certificates
- Database credentials
- Application credentials
- OAuth tokens
- Application Programming Interface (API) keys



AWS Identity and Access Management (IAM) roles

AWS Key Management Service

Amazon EC2 Instance Connect

AWS Certificate Manager

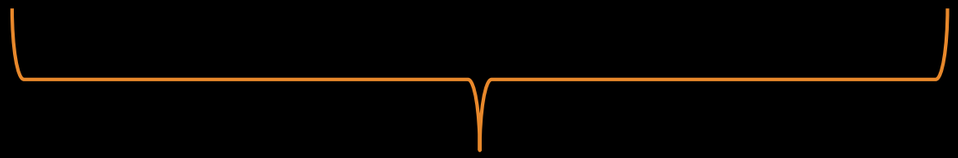
AWS Secrets Manager

What is secrets management?

Secrets management ≠ store and encrypt

Instead

Secrets management = {Store and encrypt, control access,
rotate, audit, monitor}



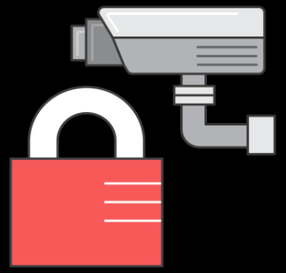
Lifecycle management

What is secrets management?

- I don’t want to email secrets
- I want fresh secrets to limit the risk of compromise
- I want to prevent developers from viewing or sharing secrets
- I want to stop “secret sprawl”
- I want to be able to see who used which secret, when
- I want to enable teams to operate quickly, without waiting on the security team to create and provision secrets
- I want to roll out secrets safely
- I want to rotate secrets without system downtime

Introduction to AWS Secrets Manager

AWS Secrets Manager enables customers to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle



Secure centrally



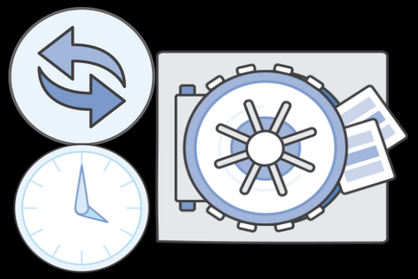
Scalable



Fine-grained access control



Monitor and audit



Rotate secrets safely

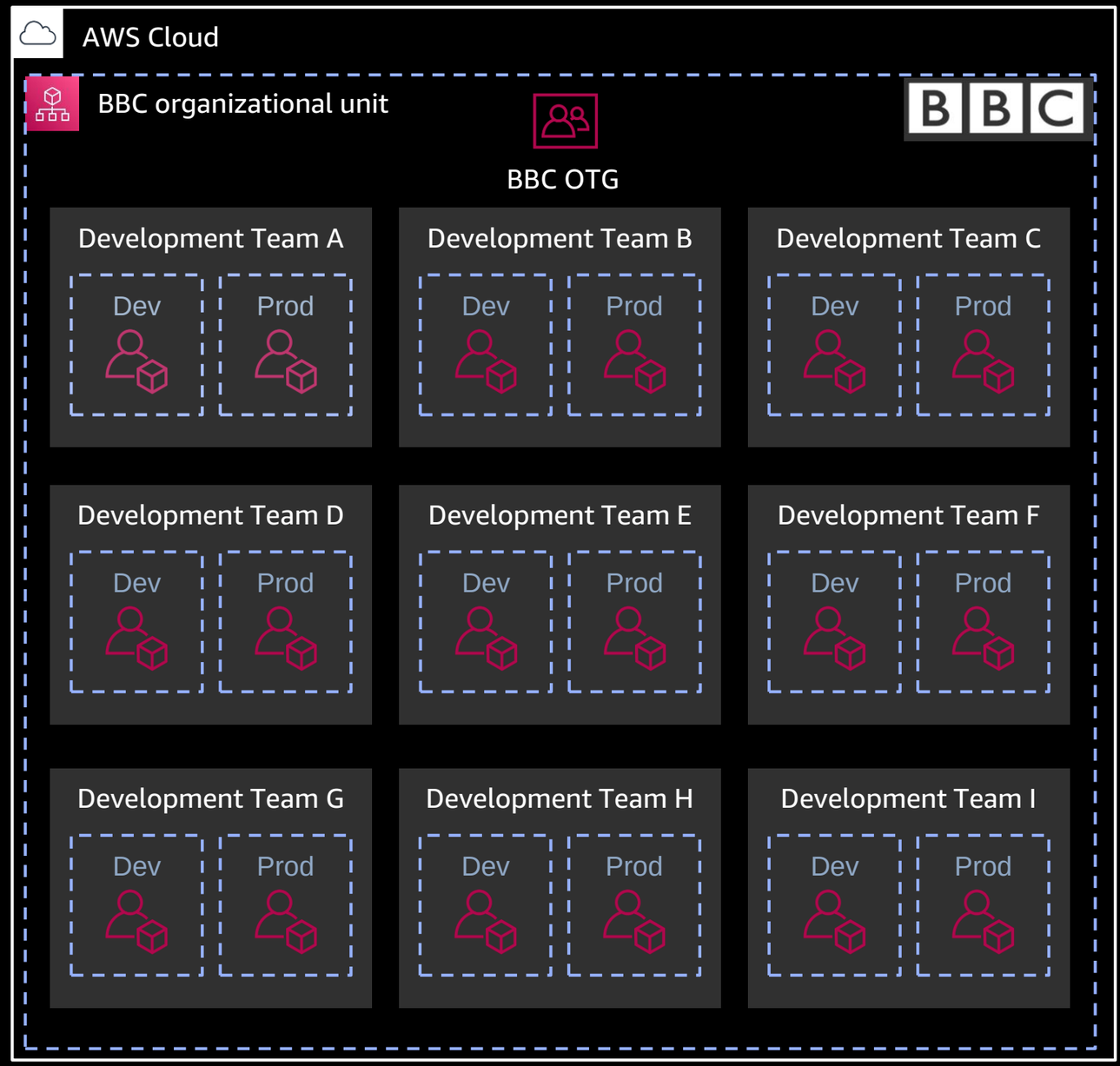


Compliance

Lifecycle management

The BBC organization

- Decentralized with lots of teams and accounts (516 as of 10/2020)
- Each team uses multiple accounts
- All accounts are administered and monitored by a central organization team
- Manages a variety of credentials: Database users, Git / application credentials, NPM tokens, API keys



Partner platform

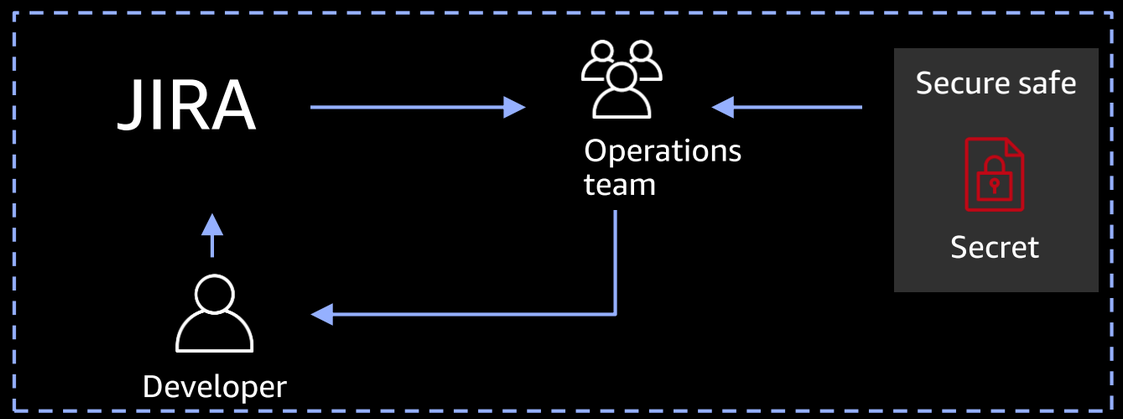
Deliver an authentication and authorization solution across the BBC



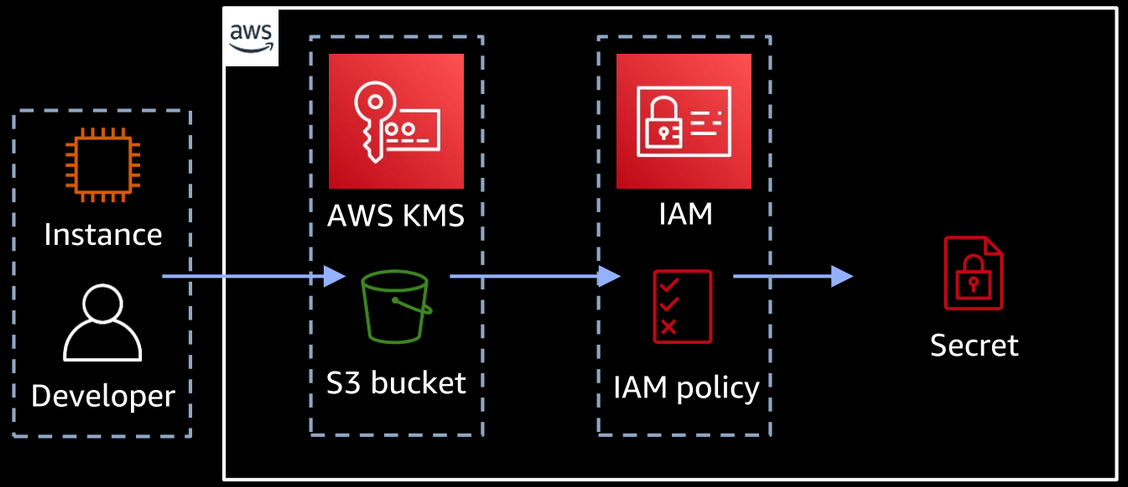
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The BBC's management of secrets before adopting Secrets Manager



Store secrets in USB keys that were stored in a secure safe



Secrets stored in KMS encrypted S3 buckets (with access restricted via IAM roles)

Pain points

- Secrets stored in one of 3 sites
- Paper-based audit trails
- Insufficient granularity for the visibility of secret use
- Lack of process consistency – Different teams doing different things
- Lack of automated secret rotation

The BBC's secrets management needs



- Needed a managed service for the use and maintenance of secrets
  Why? To ensure process consistency in managing secrets across the BBC
- Needed to audit and monitor the use of secrets
  Why? To have visibility into and tractability of the use of secrets
- Needed a way to automatically rotate secrets
  Why? To reduce the risk of exfiltration and out-of-band use of secrets

The BBC's Secrets Manager adoption journey



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The BBC's Secrets Manager adoption journey



Exploration and evaluation



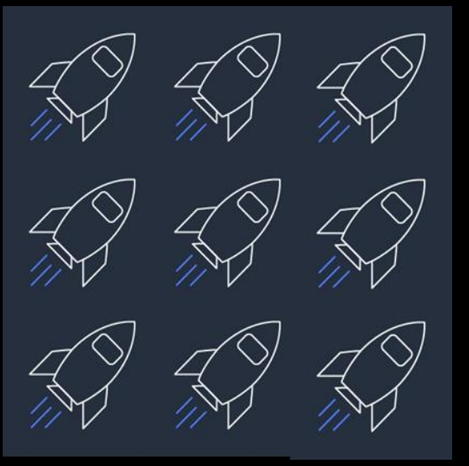
Proof of concept



Customization



Production rollout

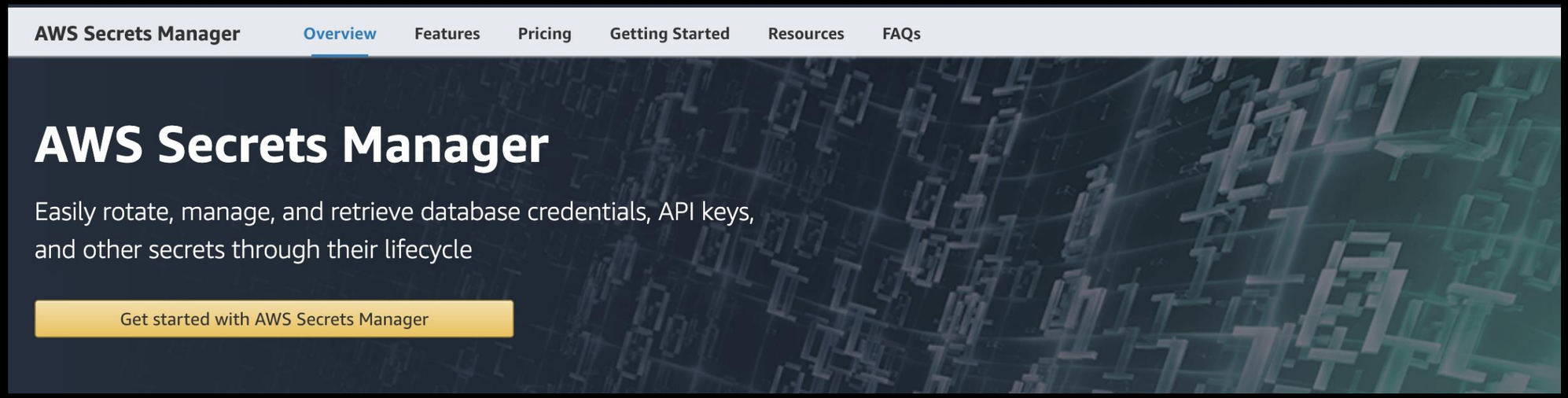


Adoption

Exploration and evaluation



Initially used the Secrets Manager console and reference documentation to explore and understand the service and what benefits / features it offered



- Secret rotation
- Fine-grained access controls
- Auditing
- Security / AWS KMS integration
- Compliance coverage

Exploration and evaluation



Storing and retrieving x509 server SSL certificates

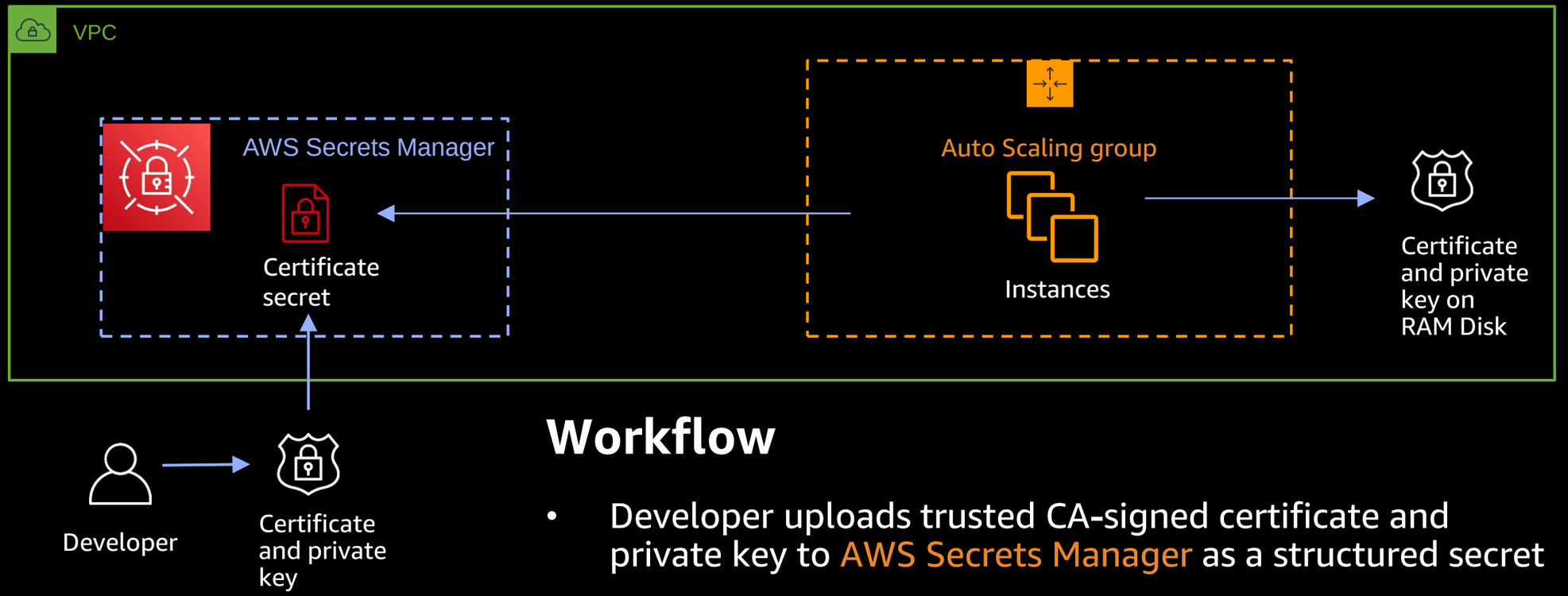
- BBC uses certificates from a trusted CA to secure SSL traffic on services
- Certificates and private keys were previously stored in off-site safes; these needed to be moved to the cloud
- Certificates must only be available to an instance via a RAM disk, not written to physical storage

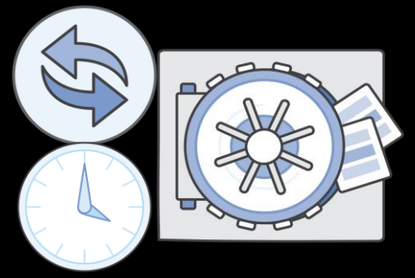
Automatic secret rotation

- Initial focus on AWS managed secrets (Relational Database Service (RDS) master credentials), which were consumed by low-volume services

Storing and retrieving x509 certificates







Workflow

- Developer uploads trusted CA-signed certificate and private key to AWS Secrets Manager as a structured secret
- Amazon EC2 Instances fetch secret at service startup and write certificate and private key to a RAM disk
- Application service has access to certificate and private key, but these are not written to physical storage / Amazon Elastic Block Store (EBS) volume

Proof of concept



Start small

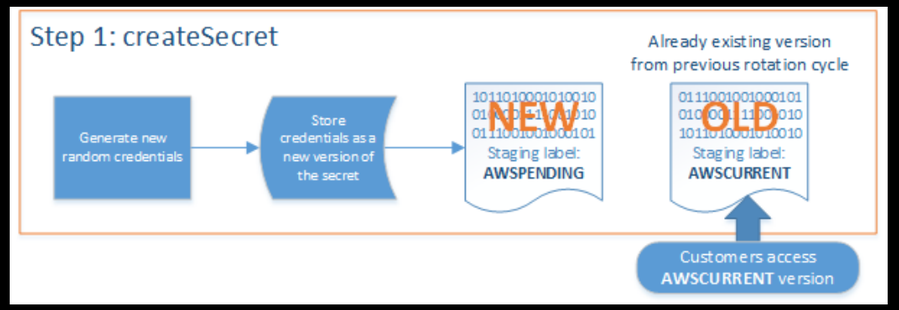
We began by testing secret rotation functionality with an initial focus on AWS-managed secrets, such as RDS master credentials consumed by low-volume services

Architectural considerations

- What secrets do we have to migrate?
- How will the secrets be stored?
- How will the secrets be retrieved?
- How will the secrets be rotated?
- How will these secrets be monitored and audited?

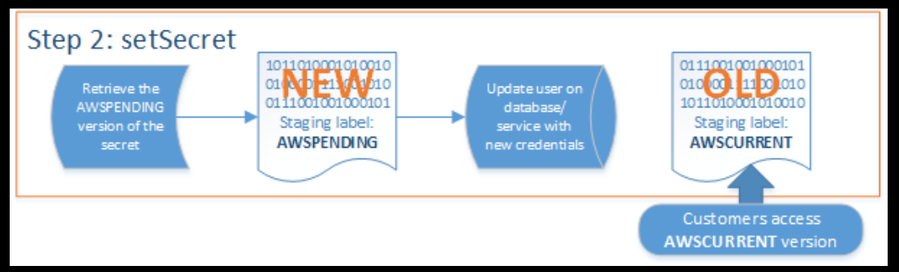
Secret rotation

ROTATION LAMBDA: 4 STEP PROCESS



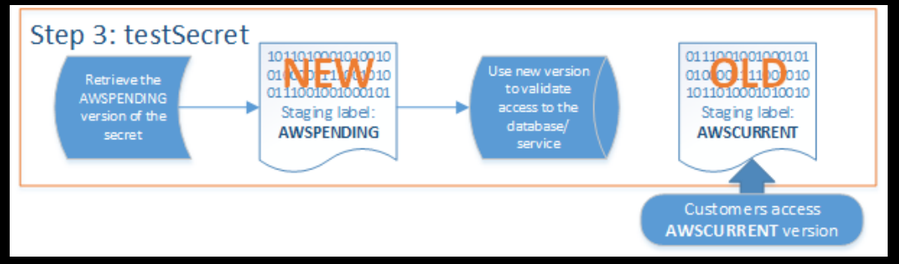
Create secret

Generate new credentials and store in Secrets Manager with the **AWSPENDING** label



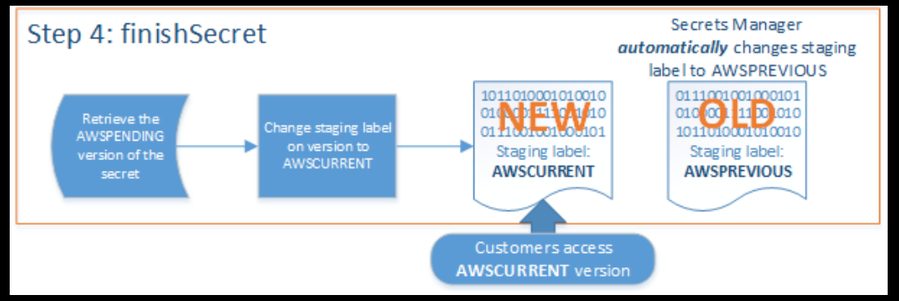
Set secret

Retrieve secret with **AWSPENDING** label, and update the user in DB / service



Test secret

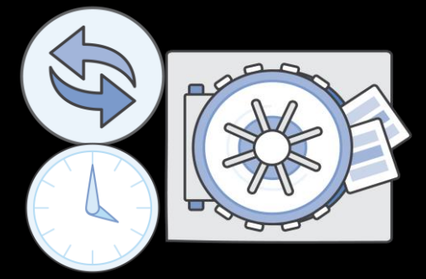
Validate the access credentials of the secret with the **AWSPENDING** label



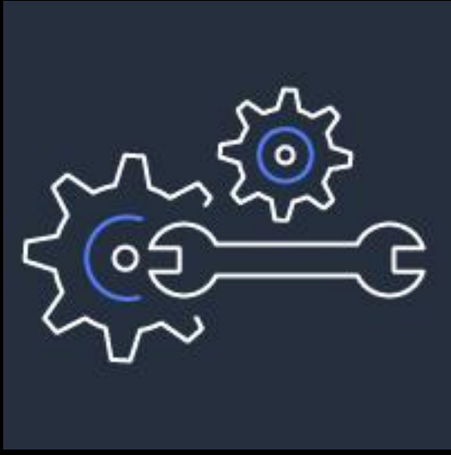
Finish secret

Retrieve secret with **AWSPENDING** label and change to **AWSCURRENT**





Customization



- We had a requirement to rotate secrets associated with database backups (and apply labels for when this occurred)
- Client-side caching libraries
  - Libraries for Java, Python, Go, .NET
  - We needed to ensure that applications retrieved the refreshed credentials each time a secret was rotated

✓ Leveraged extensibility of Secrets Manager and implemented a custom AWS Lambda-backed solution

Customization

WHAT DID WE CREATE?



2 Custom Lambdas



Secret rotation Lambda

- Triggered by Amazon CloudWatch schedule
- Rotates RDS credentials and permissions



AWS Auto Scaling replacement Lambda

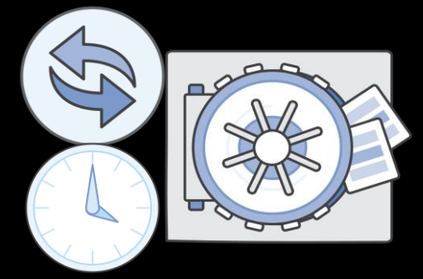
- Triggered by **FinishSecret** step
- Replaces EC2 Instances in Auto Scaling group

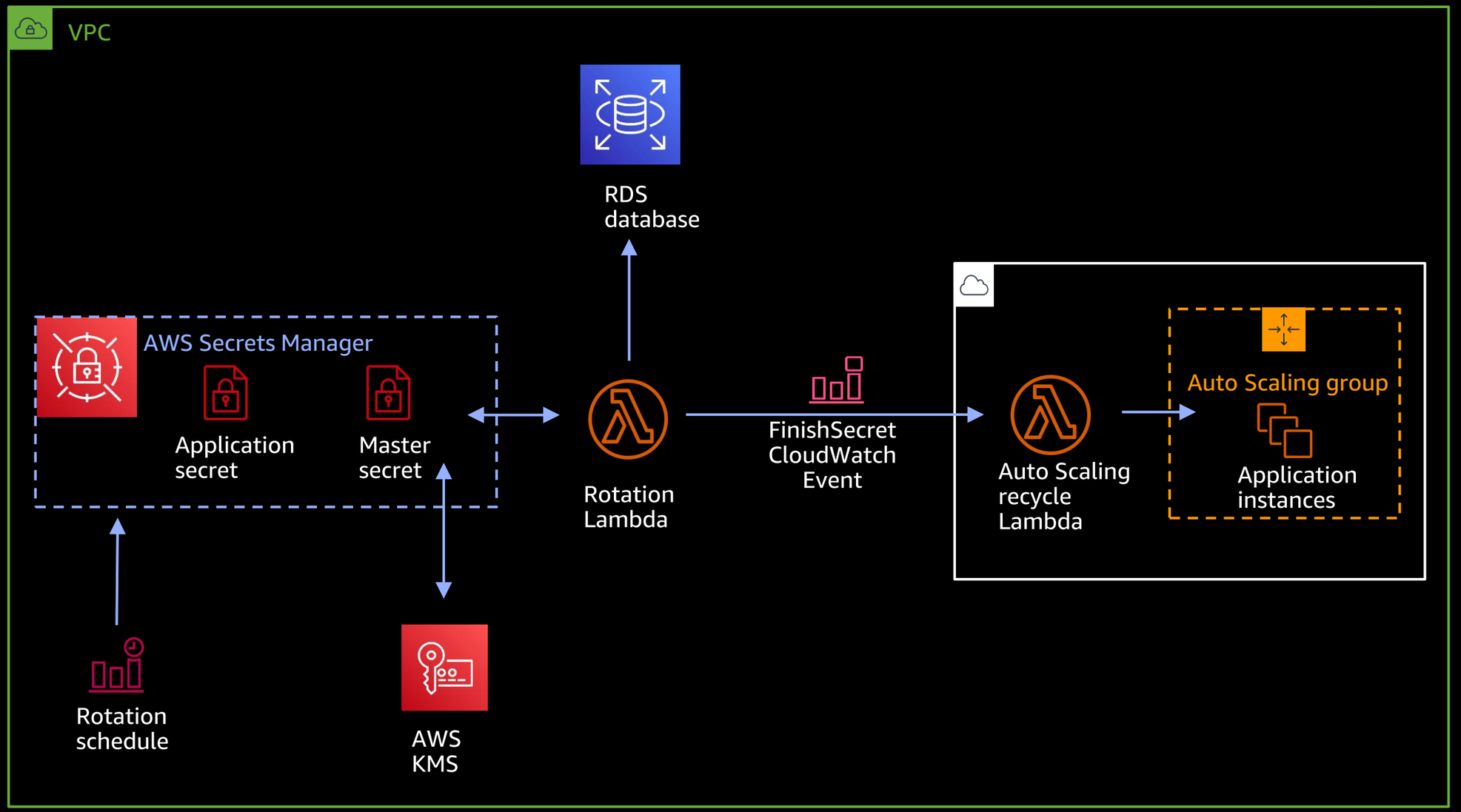
Secret rotation

PRODUCTION ROLLOUT: 2019

2019







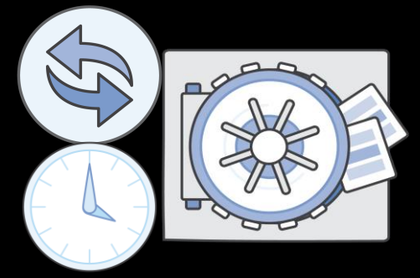
Secret rotation

PRODUCTION UPDATE: 2020



2020 – New AWS functionality





With the release of Instance Refresh for EC2 Auto Scaling, we were able to remove our custom Auto Scaling refresh Lambda

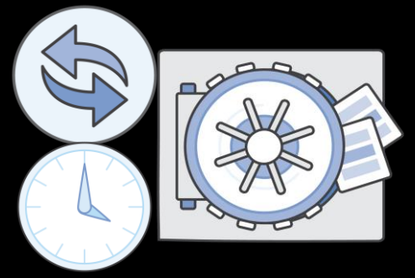
Instead, we use an AWS API call to start recycling instances for them to pick up the new version of the secret / credentials

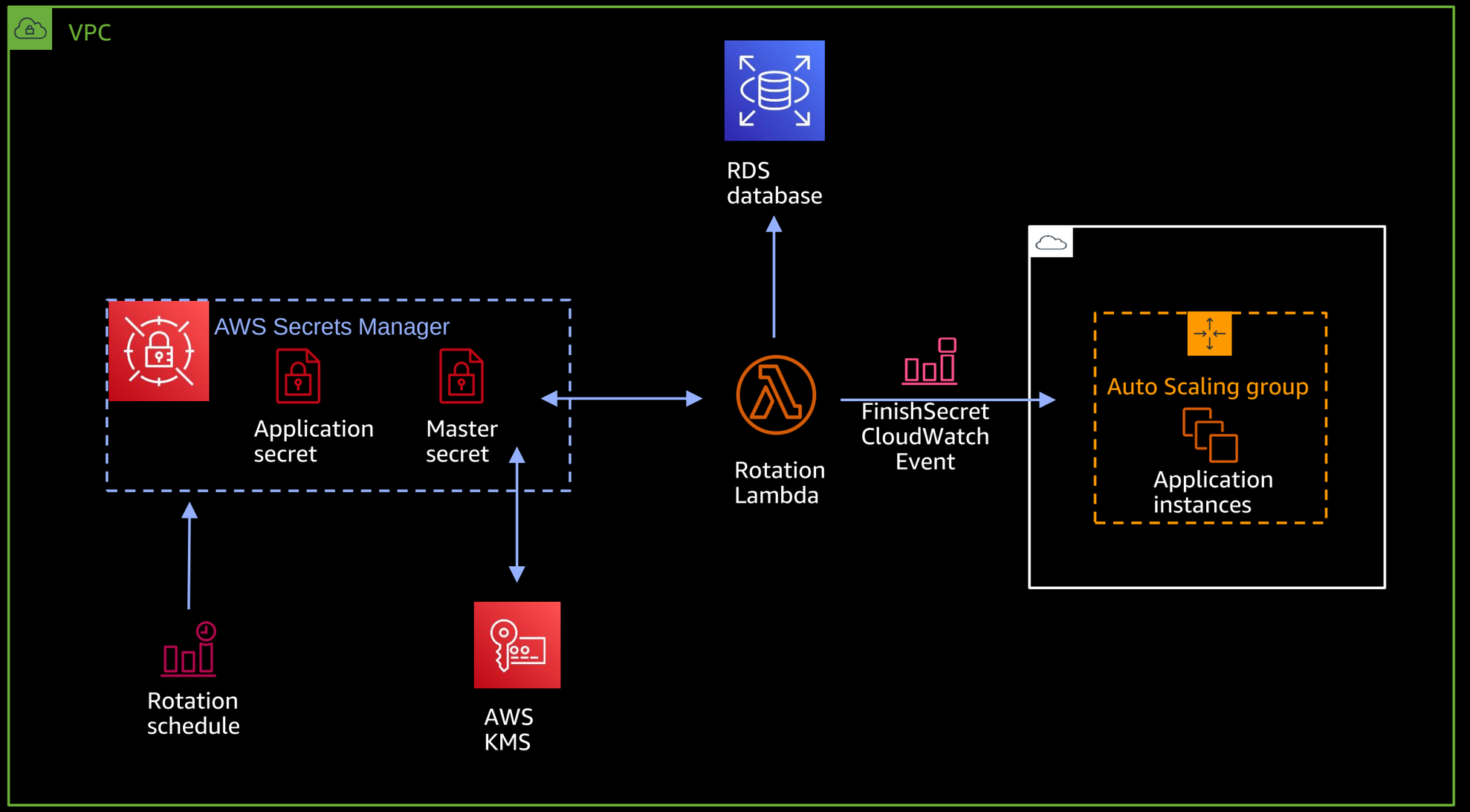
Secret rotation

PRODUCTION UPDATE: 2020

2020







Auditing and monitoring



Our central organization team uses Secrets Manager's integration with CloudTrail / CloudWatch to audit and monitor the use of secrets



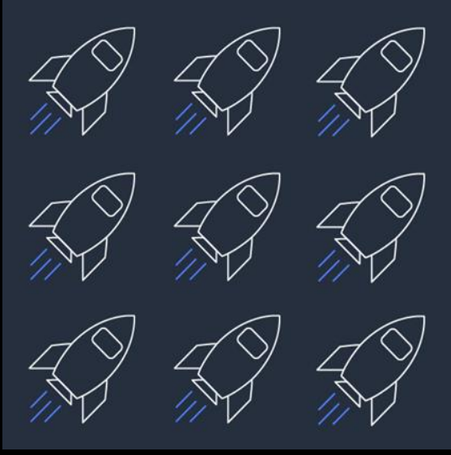
- Auditing and monitoring provide visibility into the use of secrets and help prevent abuse

Examples

- Alerts on rotation events
- Alerts on secret decryption and retrieval

Adoption

How do we drive engagement within the organization?



InfoSec reviews an approach with Development Team on the proposed use of Secrets Manager

Secrets Manager identified as approved service by the BBC InfoSec for managing secrets

More teams evaluate the use of Secrets Manager as part of their service's threat model

More services progress to a production rollout with Secrets Manager

Create awareness

- ✓ Conduct knowledge shares / show and tell
- ✓ Discuss with design and engineering advocacy groups
- ✓ Internal AWS / development Slack channels

Adoption



	2019	2020
AWS accounts	410	516
Accounts using Secrets Manager	92	157
Penetration rate	22%	30%

Data accurate as of 10/31/2020

The number of AWS accounts within the organization has continued to grow since 2019, with new teams and products under development

Penetration rate grew by **~8%** in total but **70%** from 2019!

More teams are using AWS Secrets Manager within their services

How did the BBC benefit from Secrets Manager?



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How did the BBC benefit from Secrets Manager?

The organization has confidence in what AWS Secrets Manager offers (security, secret lifecycle management) – We are now building new solutions with Secrets Manager embedded from the start

- E.g., AWS Fargate (Amazon Elastic Container Service (ECS)) and Amazon Elastic Kubernetes Service (EKS) managed solutions

We moved away from ad hoc solutions to utilize a managed service to centrally and securely store and manage the lifecycle of secrets

We eliminated the overhead associated with rotating secrets manually by implementing AWS Secrets Manager's automatic rotation functionality

How did the BBC benefit from Secrets Manager?

We leveraged the extensibility of AWS Secrets Manager to build a custom solution to ensure Node JS applications retrieved the latest version of rotated secrets

We made it possible to centrally monitor the use of secrets across the BBC while various teams quickly scale the use of AWS Secrets Manager in their own development workflow

Continuous feedback loop



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Continuous feedback loop



Recurring engagement with the Secrets Manager service team to provide feedback and feature requests

Custom defined rotation windows to specify a time window for rotation to occur, in addition to specifying the number of days

- Use case – Control the time window when rotation occurs

Client-side caching libraries for Node JS to have a way to propagate secrets to serverless / EC2 and RDS instances

- Use case – Easily cache secrets locally for Node JS applications

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.