

Security Automation

AWS Security Workshop



Agenda

- AWS Config
- AWS Config Rules
- Amazon Inspector
- AWS Systems Manager
- AWS Secrets Manager

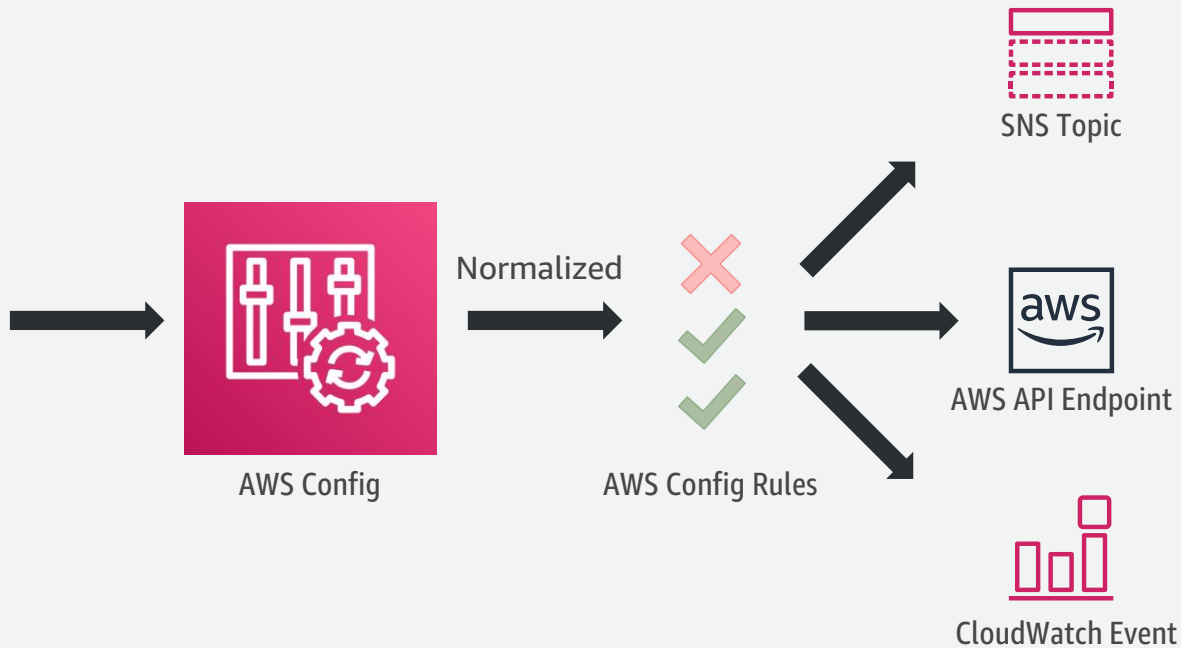
Goals

- Learn how to monitor the security of your AWS environment
- Discover options to remedy environments that fall out of compliance
- Understand tools used to automate your AWS estate

AWS Config Rules



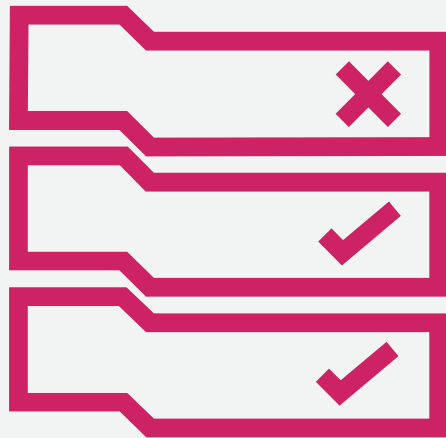
AWS Config Rules



AWS Config Rules

Continuous and automated compliance validation against the specified configuration

- AWS managed rules
 - Defined by AWS
 - Require minimal (or no) configuration
 - Rules are maintained by AWS
- Customer managed rules
 - Authored by you using AWS Lambda
 - Rules execute in your account
 - You maintain the rule



AWS Config Rules - Triggers

Two types of Triggers:

- Triggered by **resource change**: rules are invoked when a specified resource type has changed
 - Scope:
 - Tag key/value
 - Supported resource types
 - Specific resource ID
- Triggered **periodically**: rules are invoked on a specified schedule
 - Useful for checking long-running resources and resources that are not natively supported by AWS Config

AWS Config Rules – Review Compliance

aws

Services ▾

Resource Groups ▾

★

Ireland ▾

Support ▾

AWS Config

Dashboard

Rules

Resources

Settings

Authorizations

Aggregated view

Rules

Resources

Aggregators

What's new

Learn More

Documentation ↗

Partners ↗

FAQs ↗

Pricing ↗

Cost estimator

Rules

Status ⓘ

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

➕ Add rule

Estimate rules cost

↺

Compliance status ▾

Filter

Rule name ▾	Compliance ▾	Edit rule
securityhub-iam-password-policy-minimum-length-check-7keje6	1 noncompliant resource(s)	
restricted-common-ports	1 noncompliant resource(s)	
securityhub-vpc-default-security-group-closed-h4f1yr	1 noncompliant resource(s)	
securityhub-root-account-hardware-mfa-enabled-ljezb	1 noncompliant resource(s)	
custodian-my-first-policy	Compliant	
s3-bucket-public-write-prohibited	Compliant	
s3-bucket-public-read-prohibited	Compliant	
restricted-ssh	Compliant	
securityhub-iam-root-access-key-check-b9h23i	Compliant	
securityhub-iam-policy-no-statements-with-admin-access-ebk85f	Compliant	
cloudtrail-enabled	Compliant	

AWS Config Rules – Review Compliance

AWS Config > resources > bucketname > compliance

S3 Bucket bucketname

on October 17, 2018 6:57:15 PM Pacific Daylight Time (UTC-07:00)

[Manage resource](#) ⓘ

Configuration timeline Compliance timeline

17th October 2018 1:17:19 PM Compliant 2 Changes

17th October 2018 6:02:33 PM Noncompliant 3 Changes

17th October 2018 6:02:33 PM Noncompliant 2 Changes

17th October 2018 6:57:15 PM Noncompliant 2 Changes

17th October 2018 6:57:15 PM Compliant 3 Changes

Now

Calendar icon


▼ Configuration Details [View Details](#)

Amazon Resource Name	null	Target resource type	AWS::S3::Bucket
Resource type	AWS::Config::ResourceCompliance	Target resource ID	bucketname
Resource ID	AWS::S3::Bucket/bucketname	Compliance	NON_COMPLIANT
Resource name	null		
Availability zone	null		
Created on	Not available		
Tags (0)			

▼ Rules 1

Rule name	Compliance status	Amazon resource name
s3-bucket-public-read-prohibited	Noncompliant	arn:aws:config:Region:AccountID:config-rule/config-rule-id
s3-bucket-public-write-prohibited	Compliant	arn:aws:config:Region:AccountID:config-rule/config-rule-id

AWS Config Rules – Review Compliance (Aggregated)

 Services ▾ Resource Groups ▾ ★

AWS Config

Dashboard

Rules

Resources

Settings

Authorizations

Aggregated view

Rules

Resources

Aggregators

What's new

Learn More

[Documentation](#)

[Partners](#)

[FAQs](#)

[Pricing](#)

Cost estimator

Aggregated view

Note: Data displayed in the dashboard is received from multiple aggregation sources and is refreshed at different intervals. Data might be delayed by a few minutes.


Resources

Total resource count


368

Top 10 resource types


Total

 IAM Role


164

 IAM Policy


62

 S3 Bucket


23

 IAM User


14

 EC2 SecurityGroup


13

 EC2 NetworkInterface


12

 EC2 Subnet


8

 Lambda Function

7

 RDS DBSnapshot

5

 EC2 Volume

5

[View all 368 resources](#)

Config rule compliance status

22 noncompliant rule(s)

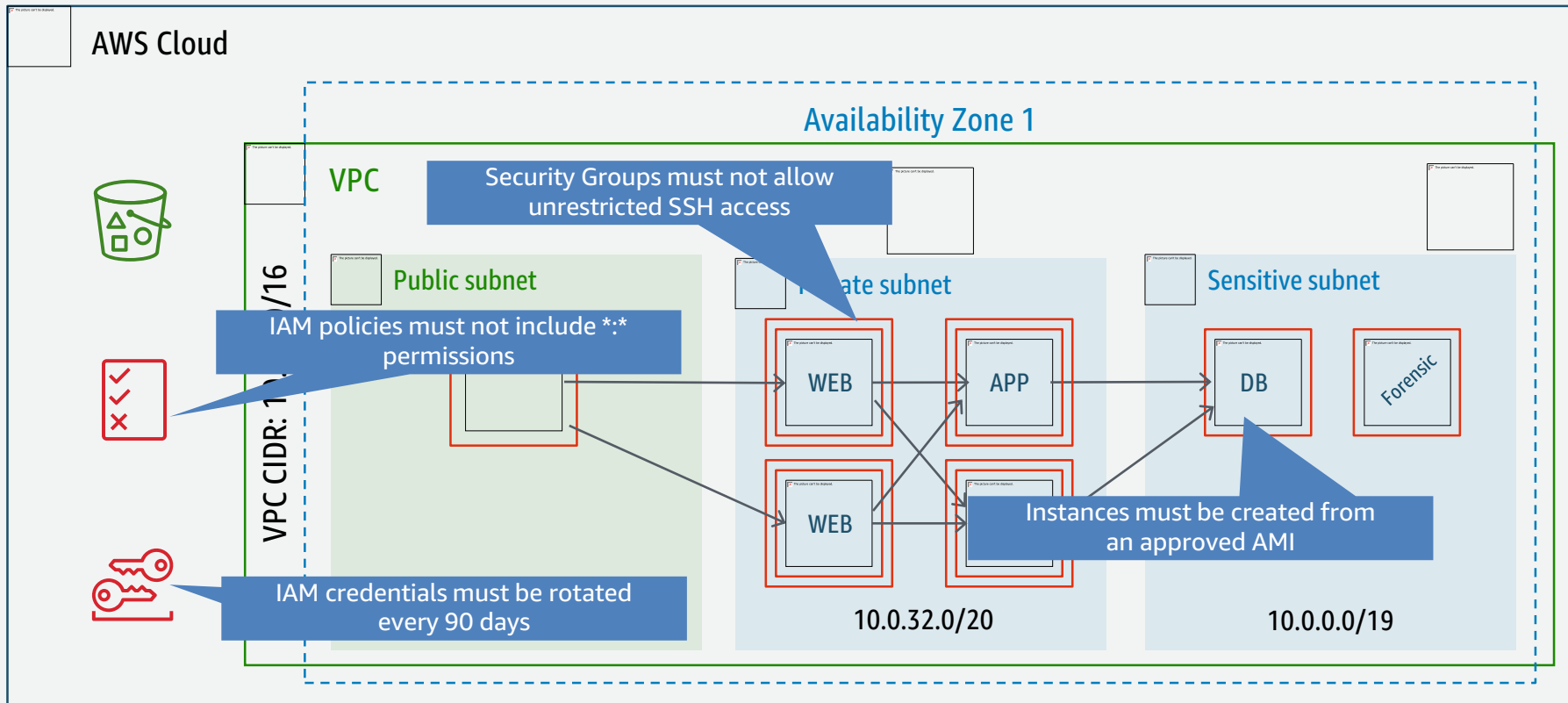
20 compliant rule(s)

Top 5 noncompliant rules

Rule name	Region	Account	Compliance
required-tags	eu-west-1	[REDACTED]	56 noncompliant resource(s)
securityhub-s3-bucket-logging-en...	eu-west-1	[REDACTED]	12 noncompliant resource(s)
securityhub-access-keys-rotated-...	eu-west-1	[REDACTED]	5 noncompliant resource(s)
securityhub-iam-user-no-policies-...	eu-west-1	[REDACTED]	5 noncompliant resource(s)
securityhub-iam-user-unused-cre...	eu-west-1	[REDACTED]	4 noncompliant resource(s)

[View all noncompliant rules](#)

AWS Config Rules - Examples



AWS Config Rules – Custom Config Rules

- Codify and automate your own security controls
- Get started with the AWS Rule Development Kit (RDK)
- Get started with samples in AWS Lambda
- Implement guidelines for security best practices and compliance
- Use rules from various AWS Partners
- View compliance in one dashboard across your AWS accounts and regions

AWS Community repository of custom Config rules

<https://github.com/awslabs/aws-config-rules>

Contains Node and Python samples for Custom Rules for AWS Config

AWS Config Rules – Evaluating Compliance

```
function hasExpectedSecurityGroup(expectedSecurityGroupId,  
securityGroups) {  
    for (var i = 0; i < securityGroups.length; i++) {  
        var securityGroup = securityGroups[i];  
        if (securityGroup.groupId ===  
expectedSecurityGroupId) {  
            return true;  
        }  
    }  
    return false;  
}
```

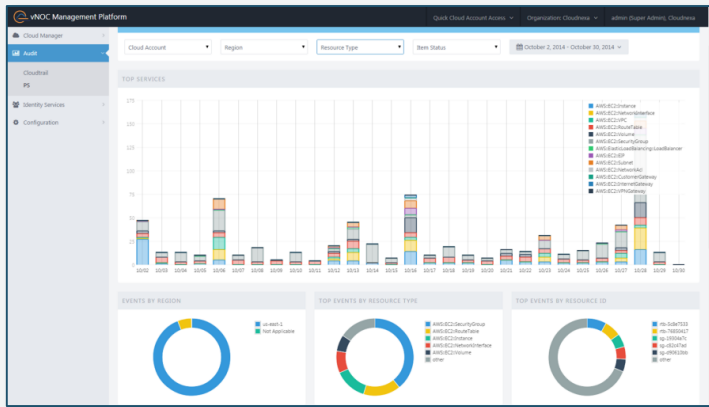
AWS Config Rules – Recording Compliance State

```
config.putEvaluations(putEvaluationsRequest, function  
(err, data) {  
    if (err) {  
        context.fail(err);  
    } else {  
        context.succeed(data);  
    }  
});
```

AWS Config Rules – Automatic Remediation

- Config Rules support automatic remediation
- YAML/JSON based AWS Systems Manager Automation Documents
- Pre-defined and custom documents can be used

- 2nd Watch
- CloudCheckr
- CloudNexa
- CloudHealth
- Evident.IO
- Red Hat Cloud Forms
- RedSeal Networks
- Splunk
- Alertlogic – Cloud Insight
- Allgress



AWS Config Rules Partners



Security Operations



Amazon Inspector

- Vulnerability Assessment Service
 - Built from the ground up to support DevSecOps
 - Automatable via APIs
 - Integrates with CI/CD tools
 - On-Demand Pricing model
 - Generates Findings
 - Multiple Static & Dynamic Rules Packages
 - Generate Finding based Action using CloudWatch Events integration



Amazon Inspector - Assessments and results

<div>CreateRunStopDeleteClone</div>					Last	
<div>Filter</div>			1 selected			
<input type="checkbox"/>		Name		Duration	Target name	
<input type="checkbox"/>	▶	TomsAssessment		15 Minutes	TomsAssessment	
<input type="checkbox"/>	▶	BestPractices		15 Minutes	TomsAssessment	
<input checked="" type="checkbox"/>	▶	ApplicationAlphaCVE		15 Minutes	ApplicationAlpha	

Amazon Inspector - Finding details

Finding Instance i-57dd8990 is using insecure protocol(s) smtp (port 25, Simple Mail Transfer).

Severity Informational ⓘ

Description This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

Recommendation We recommend you disable insecure protocols in your application and replace them with secure alternatives as listed below:

- Disable telnet, rsh, and rlogin and replace them with SSH. Where this is not possible, you should ensure that the insecure service is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups.
- Replace FTP with SCP or SFTP where possible. Where this is not possible, you should ensure that the FTP server is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups.
- Replace HTTP with HTTPS where possible. For more information specific to the web server in question see http://nginx.org/en/docs/http/configuring_https_servers.html and https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html.
- Disable IMAP, POP3, SMTP services if not required. If required, it's recommended these email protocols should be used with encrypted protocols such as TLS.
- Disable SNMP service if not required. If required, replace SNMP v1, v2 with more secure SNMP v3 which uses encrypted communication.

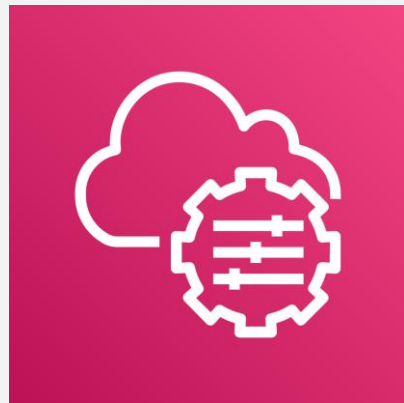
Amazon Inspector – Rules Packages

- Common Vulnerabilities & Exposures
- Center for Internet Security (CIS) Benchmarks
- Security Best Practices
- Runtime Behavior Analysis
- Network Reachability

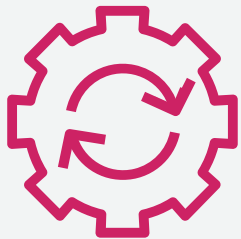


AWS Systems Manager

- Enable automated configuration
- Support ongoing management of systems at scale
- Work across all of your Windows and Linux workloads
- Run in Amazon EC2 or on-premises
- Carry no additional charge to use



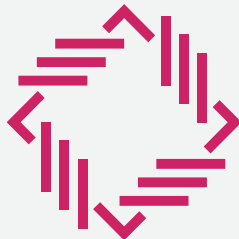
AWS Systems Manager - Capabilities



Automation



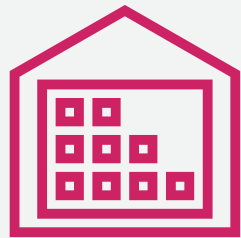
Documents



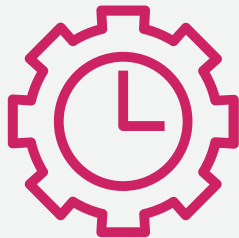
Patch Manager



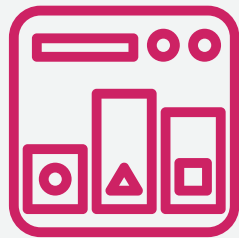
Parameter Store



Inventory



Maintenance
Windows

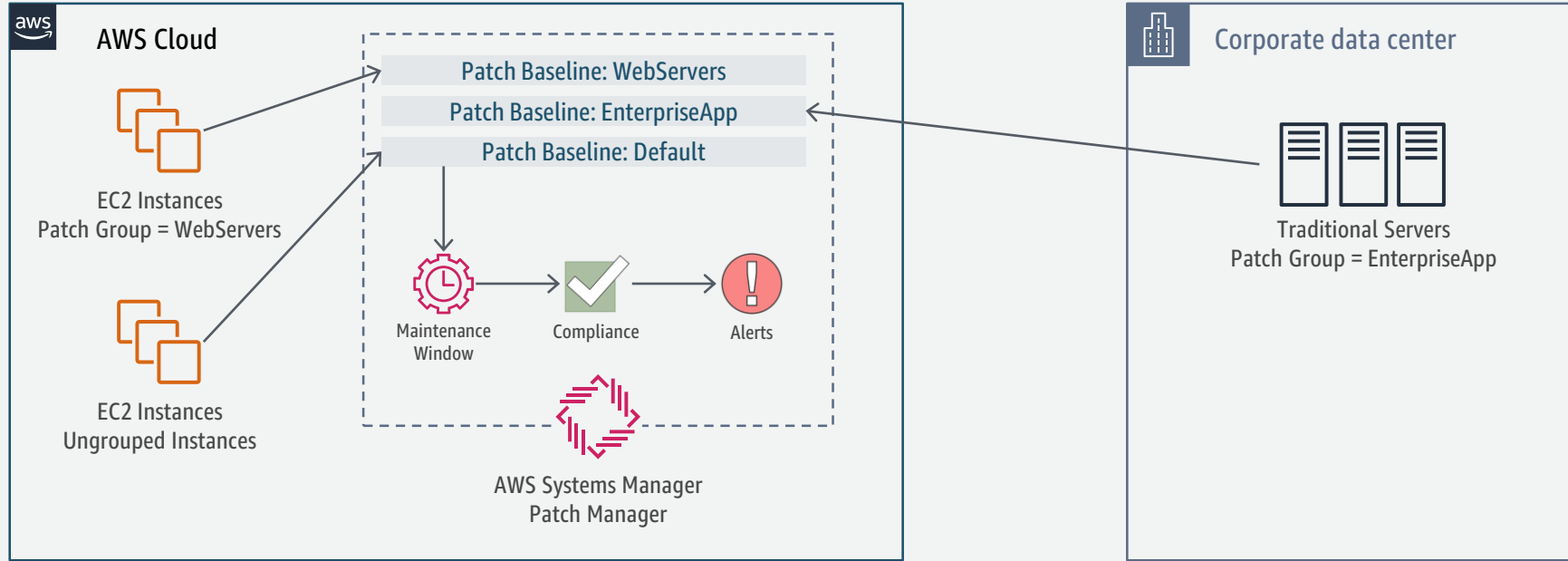


State Manager

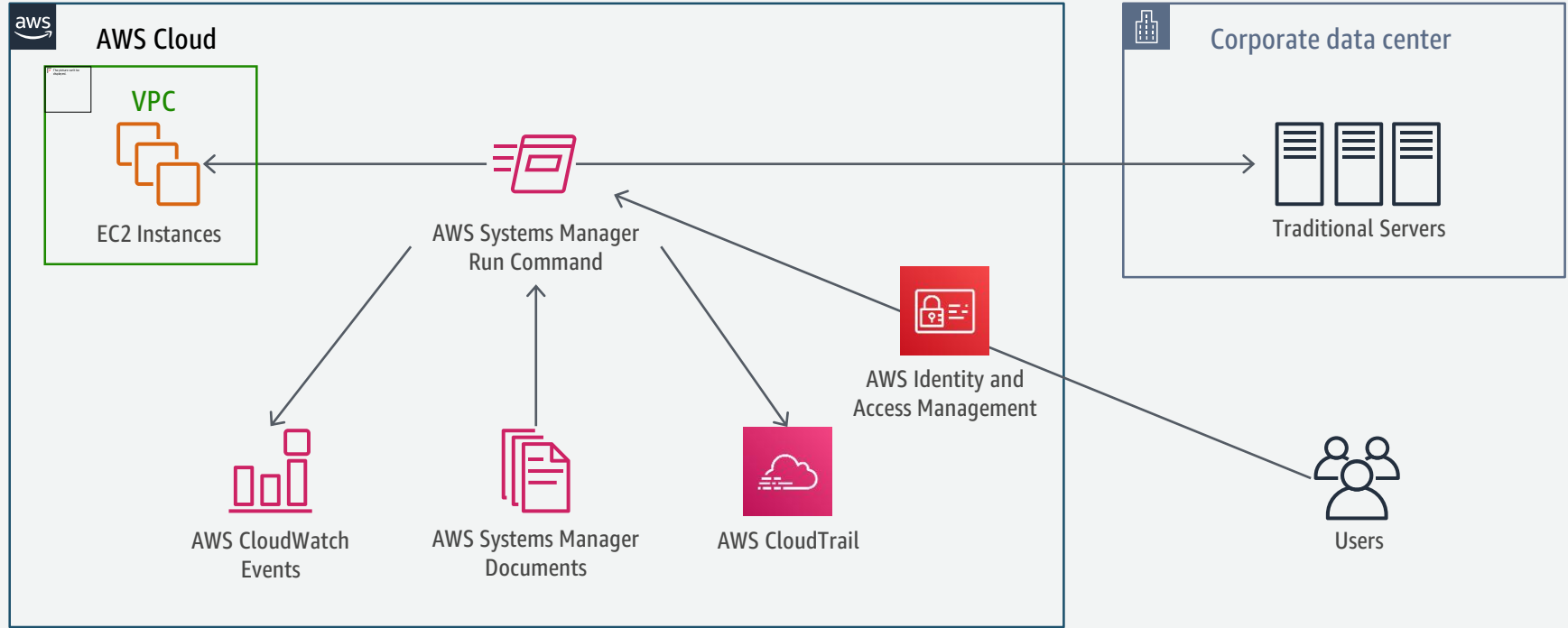


Run Command

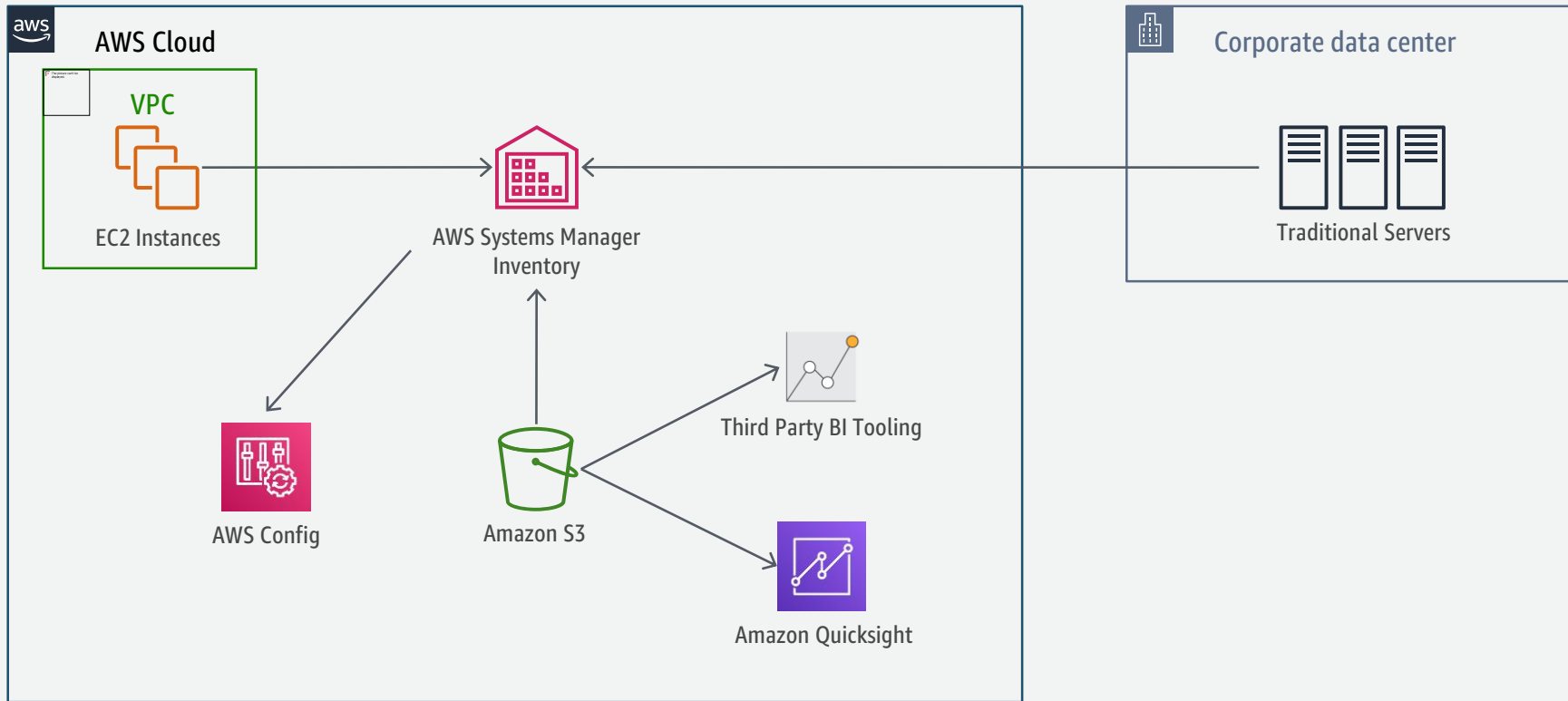
AWS Systems Manager – Compliance with Patch Manager



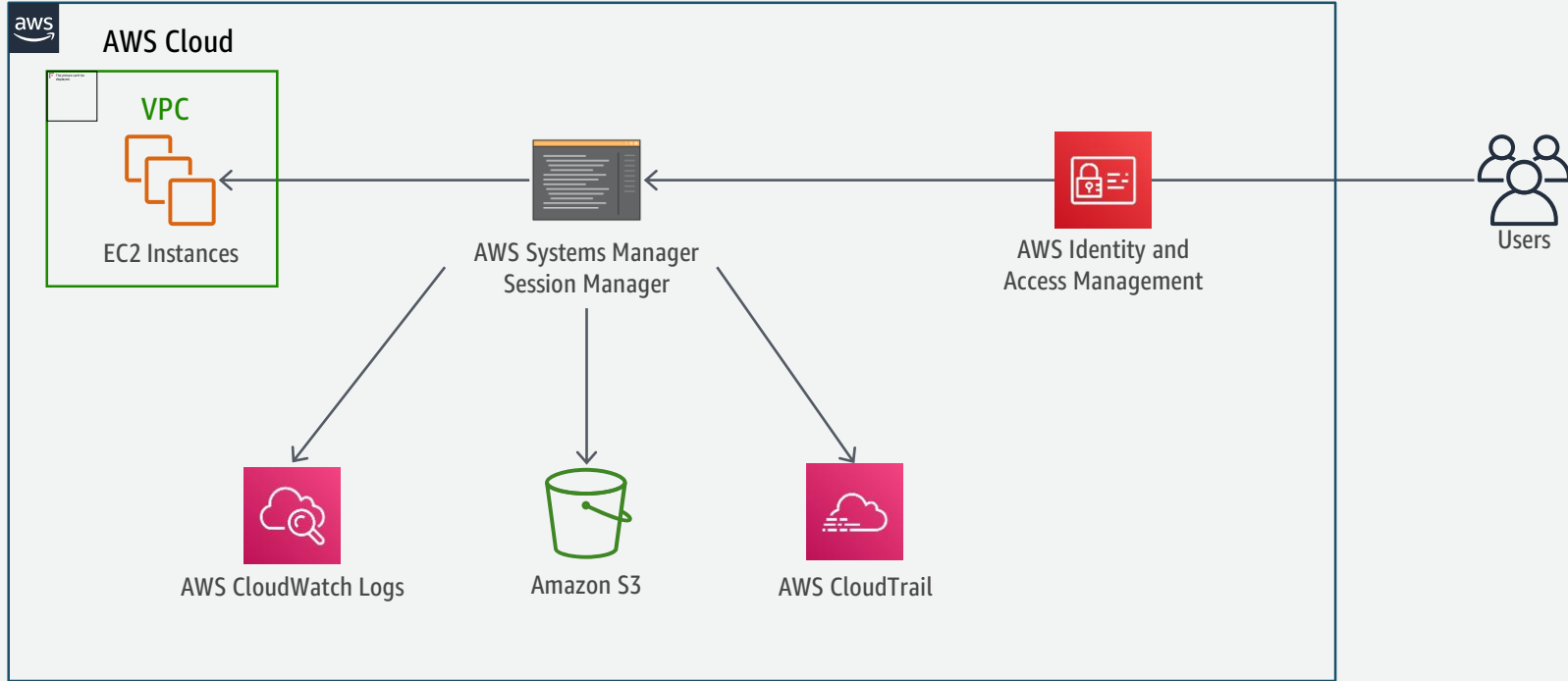
AWS Systems Manager – Run Command



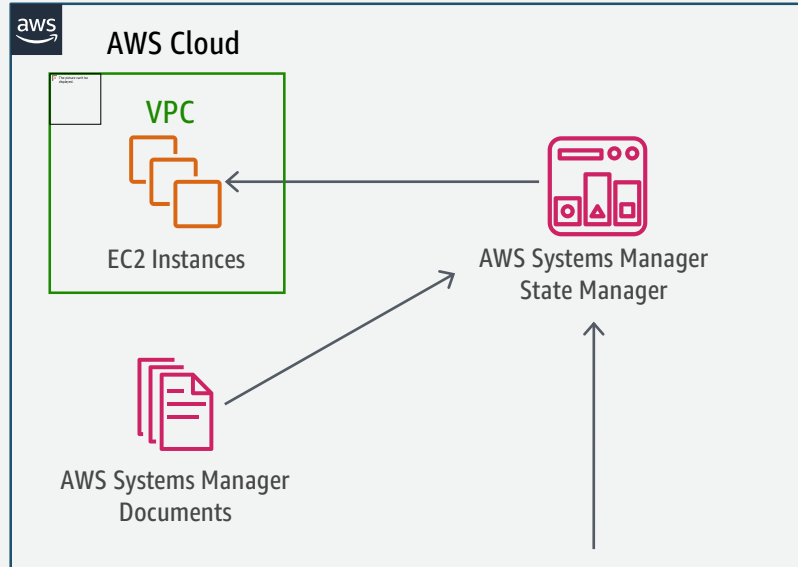
AWS Systems Manager – Inventory



AWS Systems Manager – Session Manager



AWS Systems Manager – State Manager



Schedule

To run an association automatically set a schedule defining when it will run.

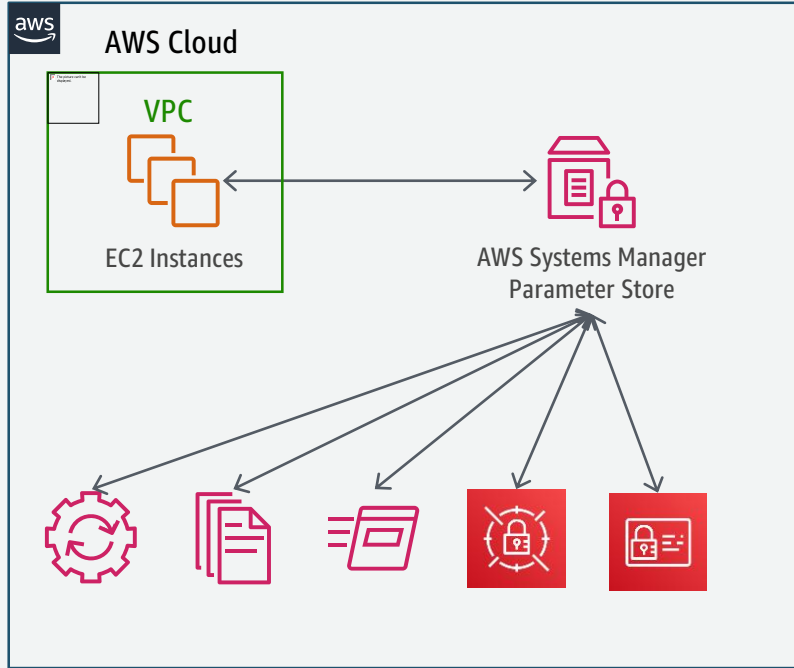
Schedule ☒ Every 30 Minutes

☐ Every 1 Hours

☐ Every Sunday at HH:mm UTC

- Control configuration details such as anti-virus settings, iptables, etc.
- Compare actual deployments against specified configuration policy
- Automatically re-apply policies if state drift is detected
 - OS changes
 - Local users and permissions

AWS Systems Manager – Parameter Store



- Raise your security profile by managing configuration data separately from code
- Store parameters in hierarchies, track versions and dynamically reference to them from APIs
- Granularly control and audit access at parameter, tag, and path levels
- Integrates with AWS Secrets Manager and the other AWS Systems Manager components

AWS Systems Manager

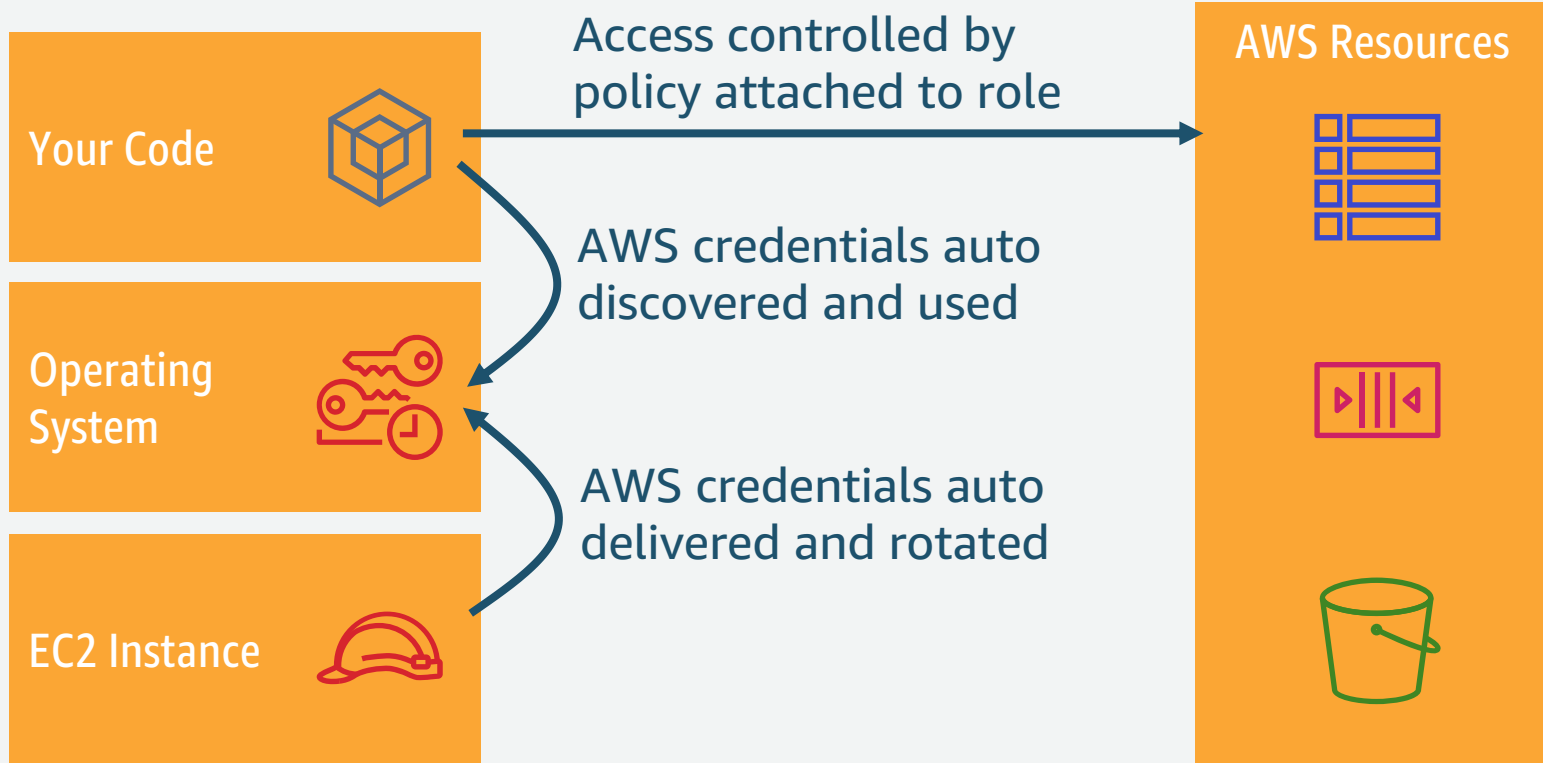
Run Command	allows for a simple way of automating common administrative tasks like remotely executing shell scripts or PowerShell commands, installing software updates, or making changes to the configuration of OS, software.
Inventory	an extensible framework to collect and query configuration and inventory information about your instances and the software installed on them.
Patch Manager	helps select and deploy operating system and software patches automatically across large groups of instances.
State Manager	helps define and maintain consistent OS configurations such as firewall settings and anti-malware definitions to comply with your policies.
Maintenance Window	defines a recurring window of time to run administrative and maintenance tasks across your instances.
Session Manager	lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.
Automation	simplifies common maintenance and deployment tasks, such as updating Amazon Machine Images (AMIs).
Parameter Store	a centralized location to store, provide access control, and easily reference your configuration data and secrets.
Documents	describe an instance configuration, which you can use to set up and run commands on your instances.

AWS Secrets Manager

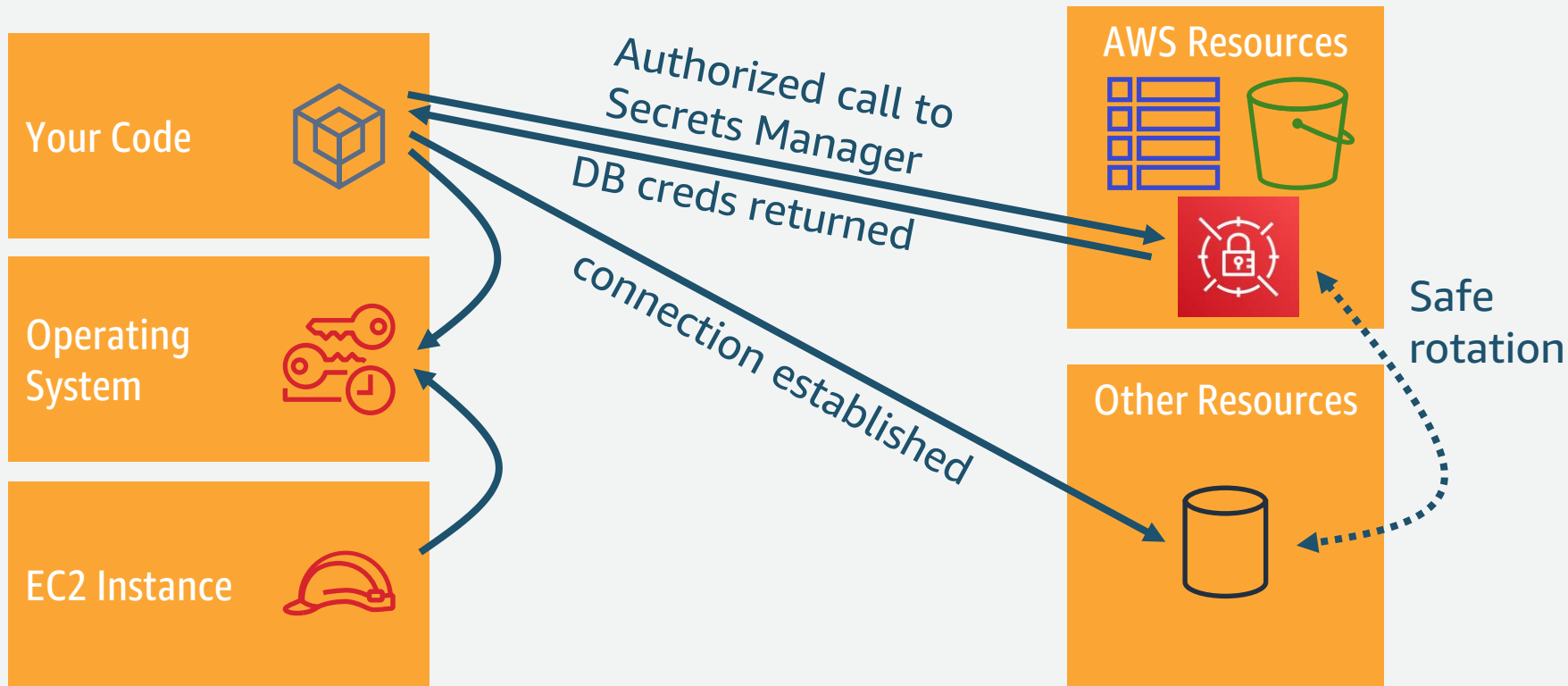
- Safe rotation of secrets
- Built-in integrations, extensible with Lambda
- On-demand or automatic rotation with versioning
- Fine-grained access policies
- Encrypted storage
- Logging and auditability



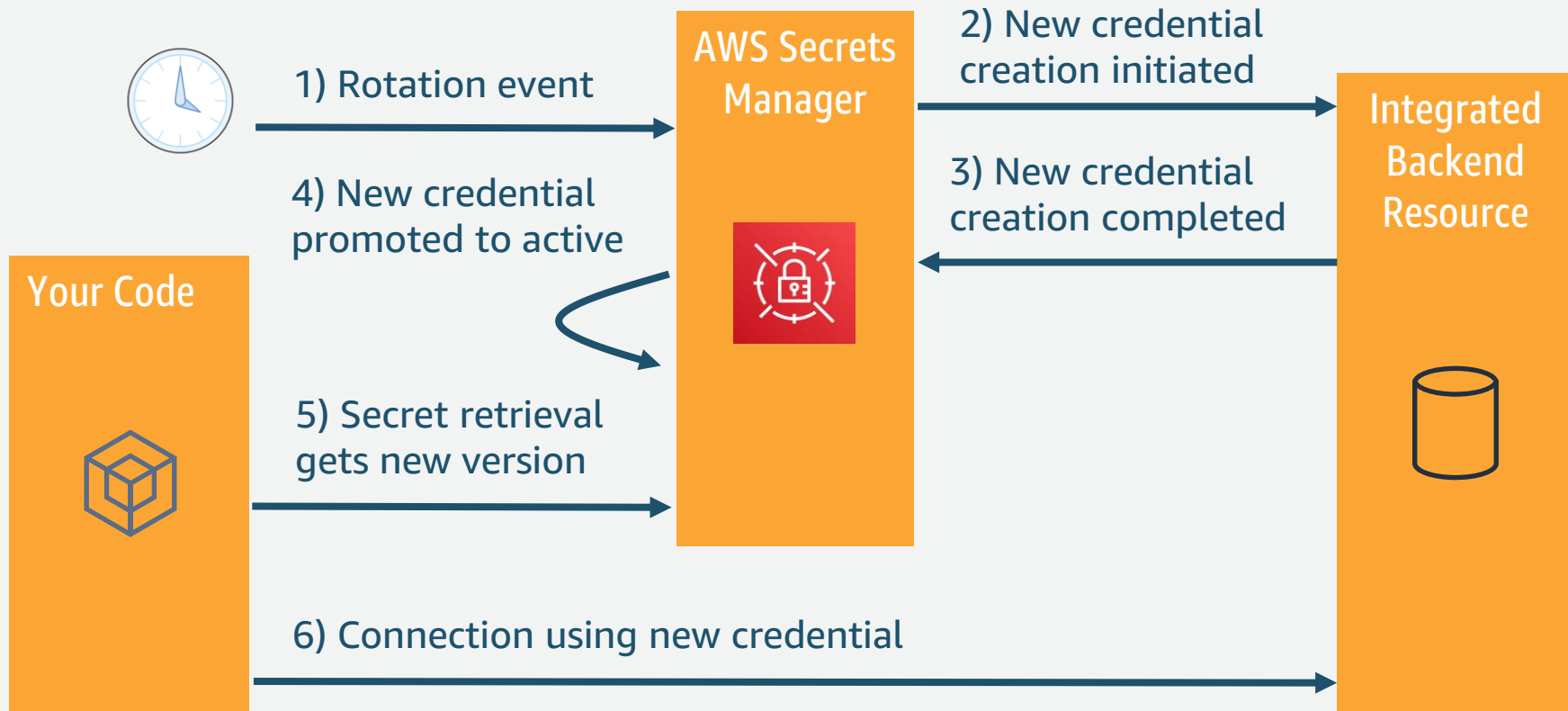
AWS Secrets Manager: IAM Roles



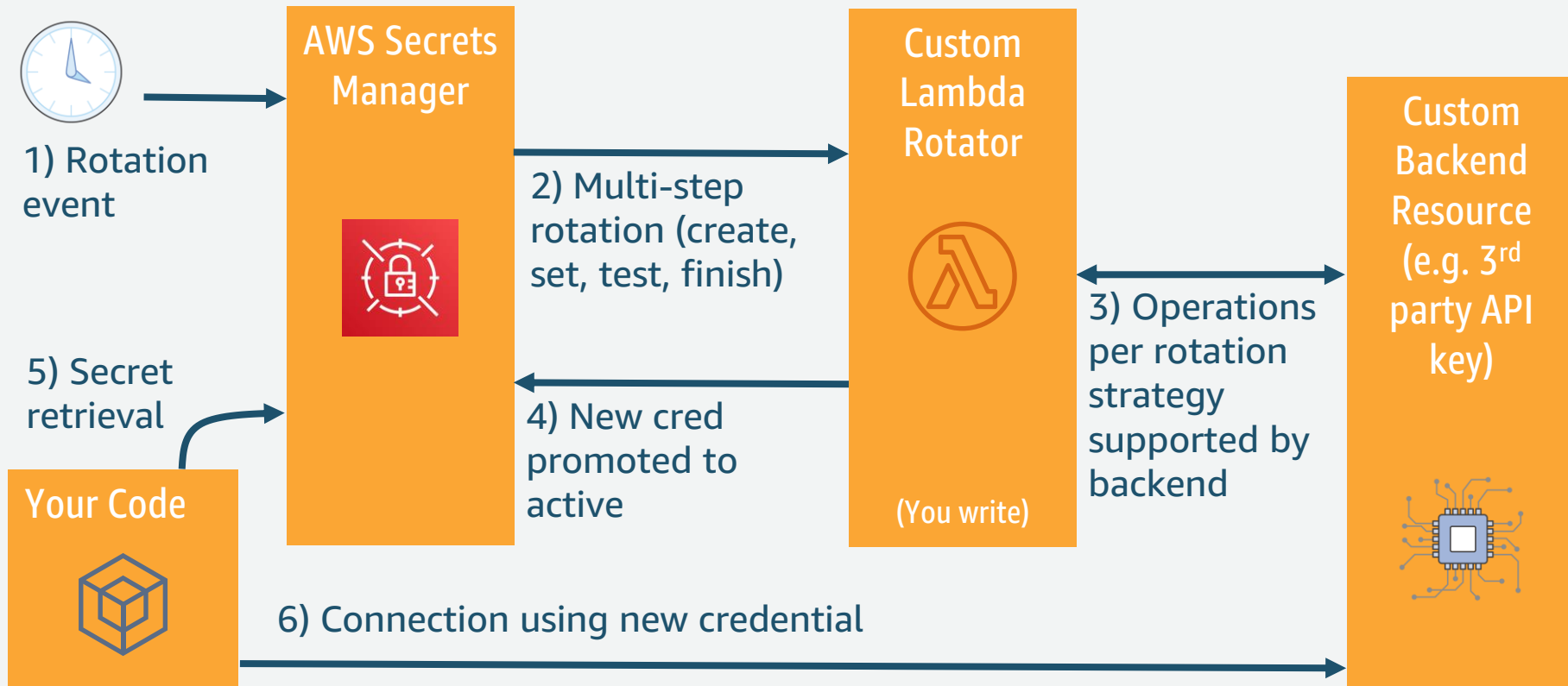
AWS Secrets Manager: Retrieve Secret



AWS Secrets Manager: Rotate Secret (Integrated)



Rotate Secret (Custom)



Encryption

All secrets protected at-rest and in-transit

At-rest

Secrets encrypted at rest using AWS Key Management Service (KMS).

Choose your desired Customer Master Key (CMK) or AWS managed default encryption key.

In-transit

Secrets encrypted in transit using Transport Layer Security (TLS).

All API calls authenticated by SigV4 verification.

Questions?