# 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 professional services
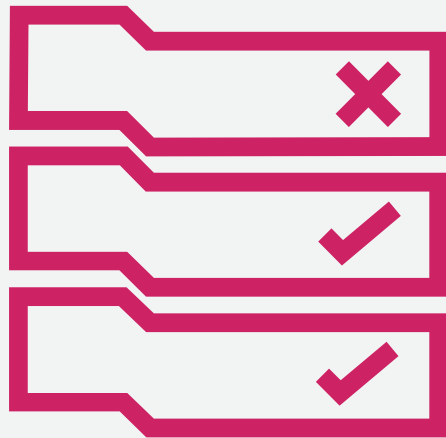
AWS Config Rules
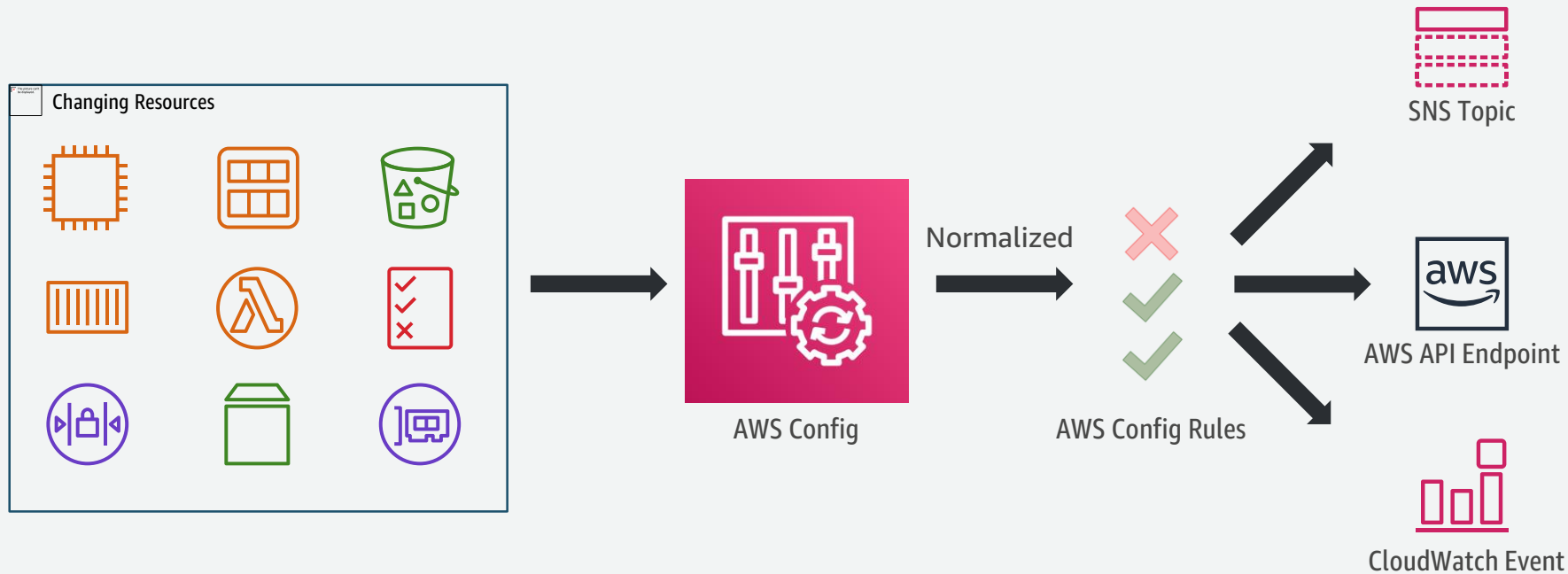
AWS Config Rules

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
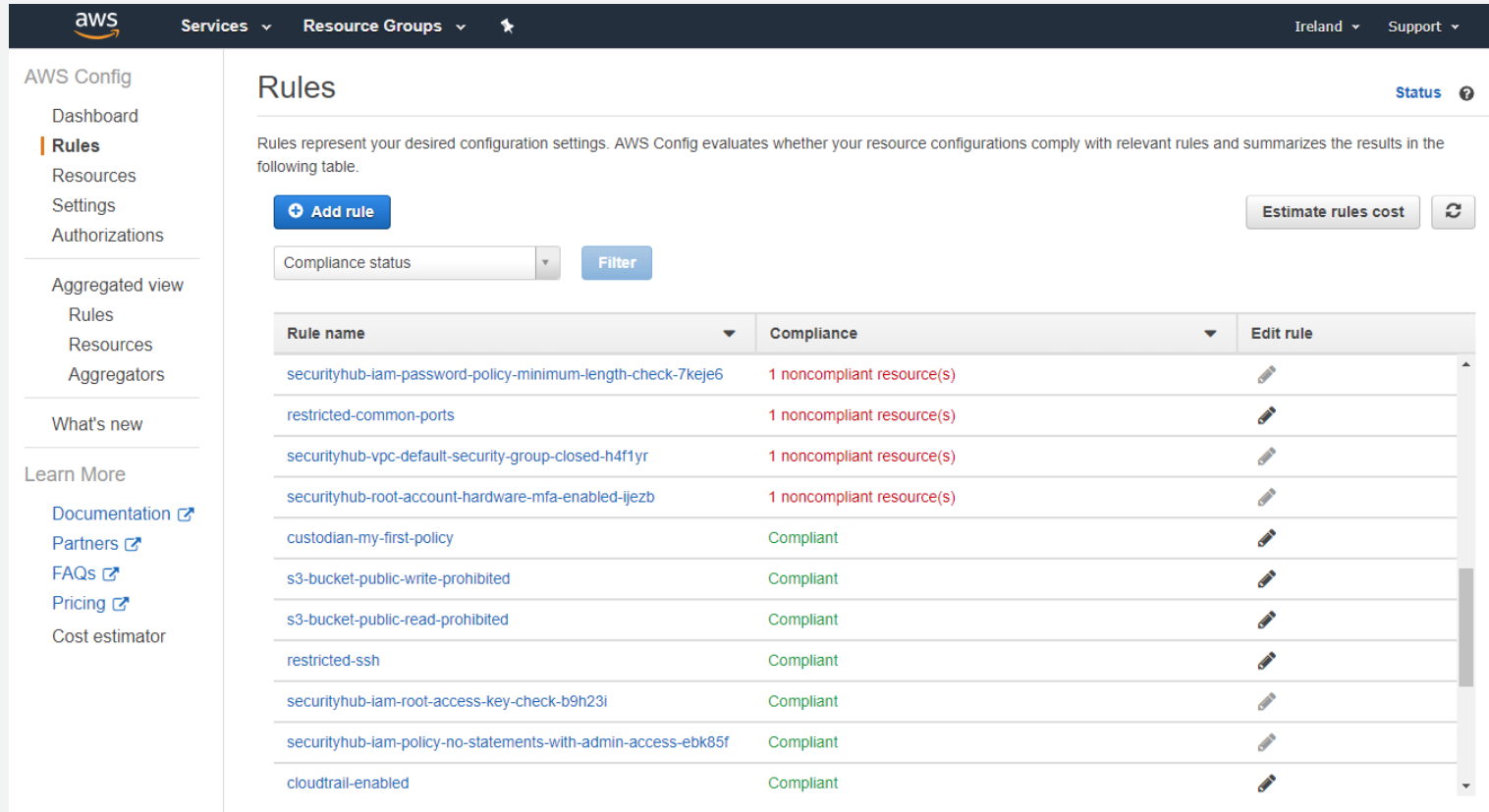 - You maintain the rule

aws professional services

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 professional services

AWS Config Rules – Review Compliance

AWS Config Rules – Review Compliance

AWS Config Rules – Review Compliance (Aggregated)

AWS Config Rules - Examples

AWS Cloud

Availability Zone 1

VPC

VPC CIDR: 10.0.0.0/16

Public subnet

Private subnet

Sensitive subnet

Security Groups must not allow unrestricted SSH access

IAM policies must not include *:* permissions

IAM credentials must be rotated every 90 days

Instances must be created from an approved AMI

WEB   APP   DB   Forensic

WEB

10.0.32.0/20   10.0.0.0/19

aws professional services
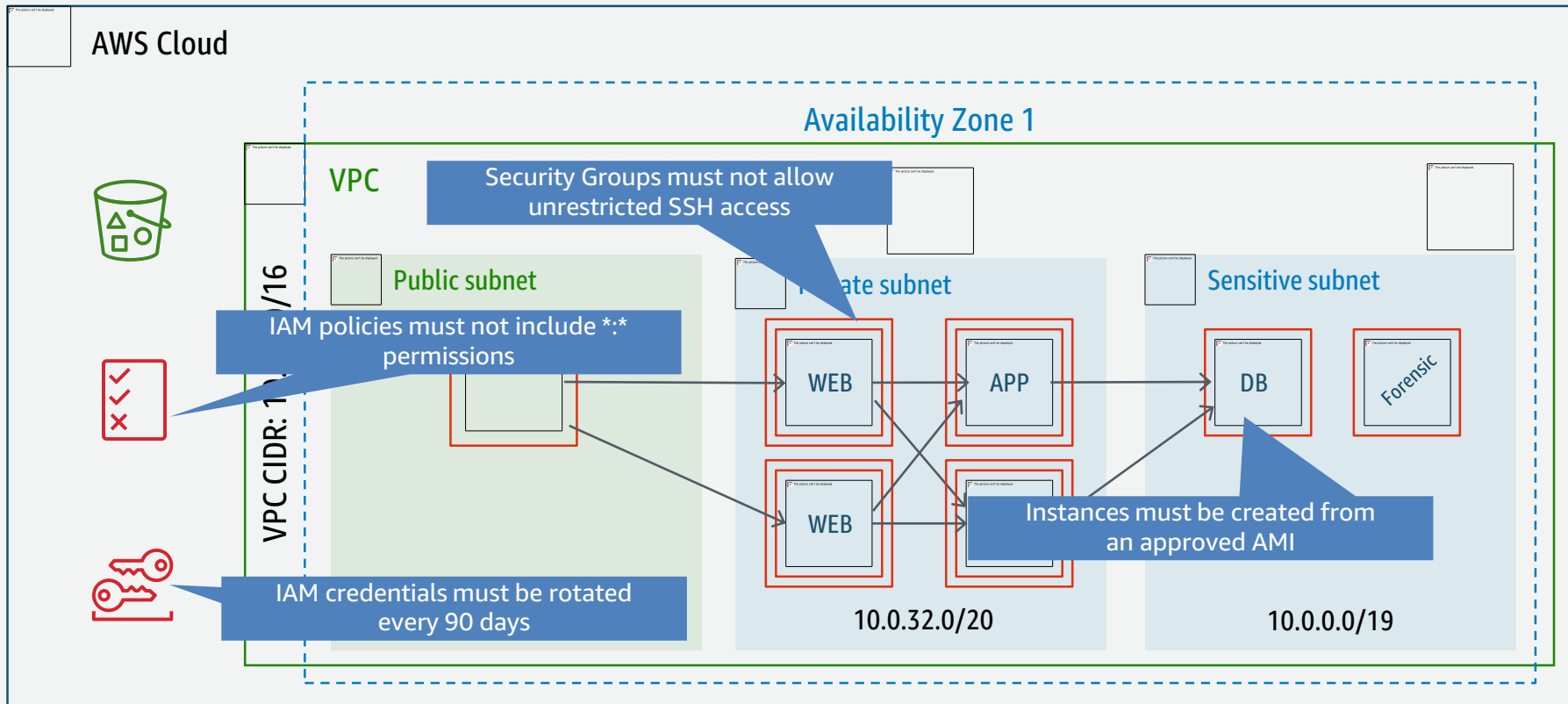
AWS Config Rules – Custom Config Rules

- 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 professional services

AWS Config Rules – Evaluating Compliance

```javascript
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 professional services

AWS Config Rules – Recording Compliance State

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

aws professional services

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

AWS Config Partners

- 2nd Watch

- CloudCheckr

- CloudNexa

- CloudHealth

- Evident.IO

- Red Hat Cloud Forms

- RedSeal Networks

- Splunk

- Alertlogic – Cloud Insight

- Allgress
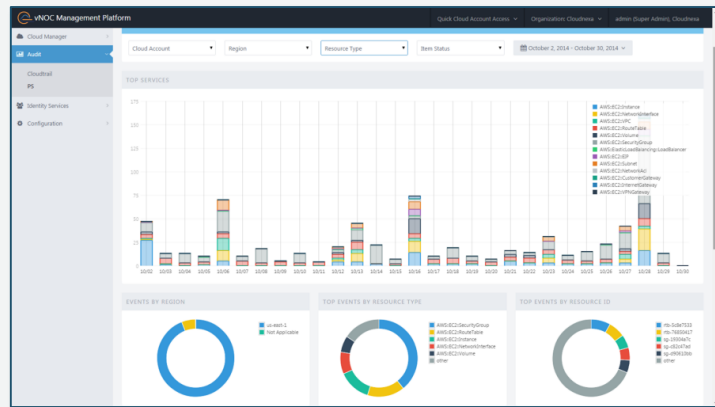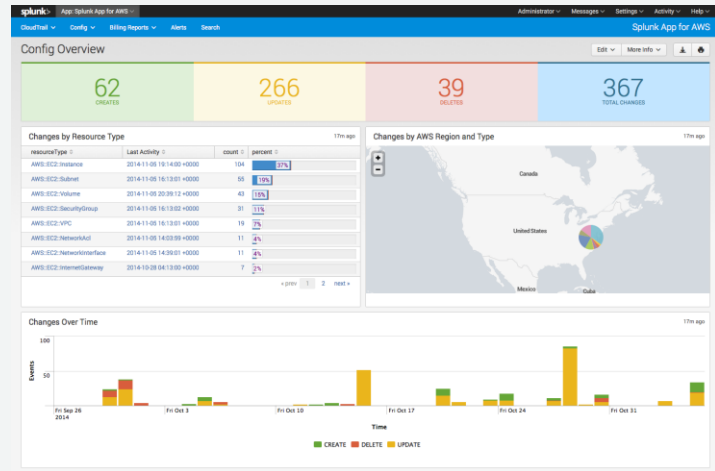
AWS Config Rules Partners

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

aws professional services
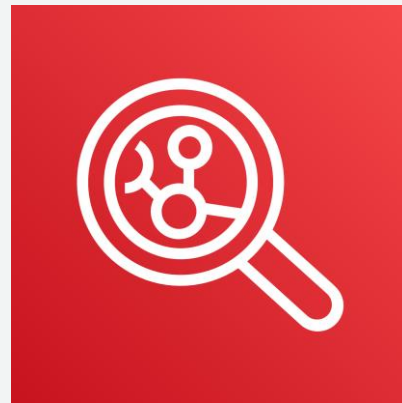
Amazon Inspector – Assessments and results

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 professional services
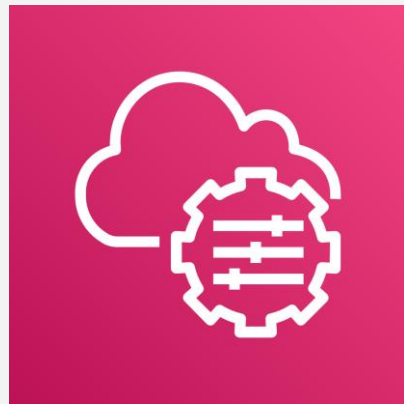
AWS Systems Manager – Capabilities
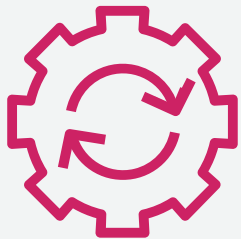
Automation

Documents
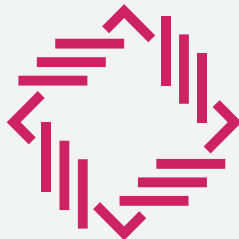
Patch Manager

Parameter Store
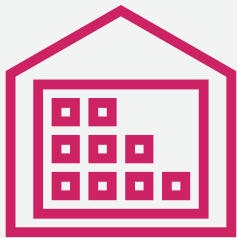
Inventory
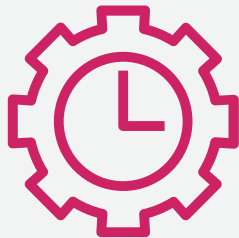
Maintenance
Windows

State Manager

Run Command

aws professional services
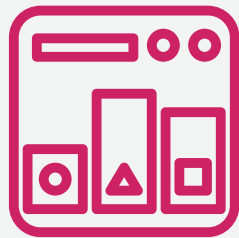
AWS Systems Manager – Compliance with Patch Manager

AWS Cloud

EC2 Instances
Patch Group = WebServers

EC2 Instances
Ungrouped Instances

Patch Baseline: WebServers

Patch Baseline: EnterpriseApp

Patch Baseline: Default

Maintenance Window

Compliance

Alerts

AWS Systems Manager
Patch Manager

Corporate data center

Traditional Servers
Patch Group = EnterpriseApp

aws professional services

AWS Systems Manager – Run Command

AWS Cloud

VPC

EC2 Instances

AWS Systems Manager
Run Command

AWS CloudWatch
Events

AWS Systems Manager
Documents

AWS CloudTrail

AWS Identity and
Access Management

Corporate data center

Traditional Servers

Users

AWS Systems Manager – Inventory

AWS Cloud

VPC

EC2 Instances

AWS Systems Manager Inventory

AWS Config

Amazon S3

Third Party BI Tooling

Amazon Quicksight

Corporate data center

Traditional Servers

aws professional services

AWS Systems Manager – Session Manager

EC2 Instances

VPC

AWS Cloud

AWS Systems Manager
Session Manager

AWS Identity and
Access Management

Users

AWS CloudWatch Logs

Amazon S3

AWS CloudTrail

aws professional services

AWS Systems Manager – State Manager

- 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 Cloud

VPC

EC2 Instances

AWS Systems Manager
State Manager

AWS Systems Manager
Documents

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

aws professional services

AWS Systems Manager – Parameter Store
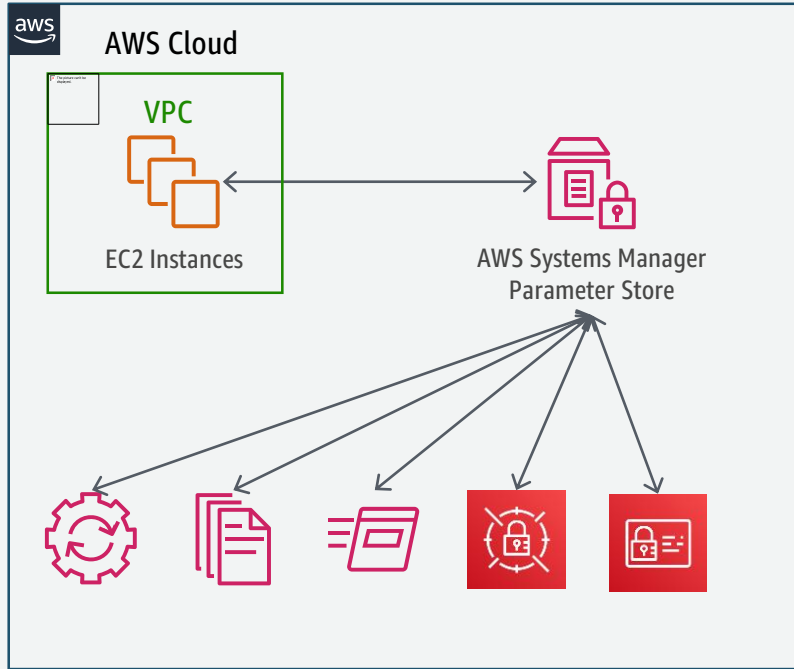
- Raise your security profile by managing configuration data separately from code

- 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 professional services

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 professional services

AWS Secrets Manager: IAM Roles

Your Code

Access controlled by policy attached to role

AWS Resources

AWS credentials auto discovered and used

Operating System

AWS credentials auto delivered and rotated

EC2 Instance
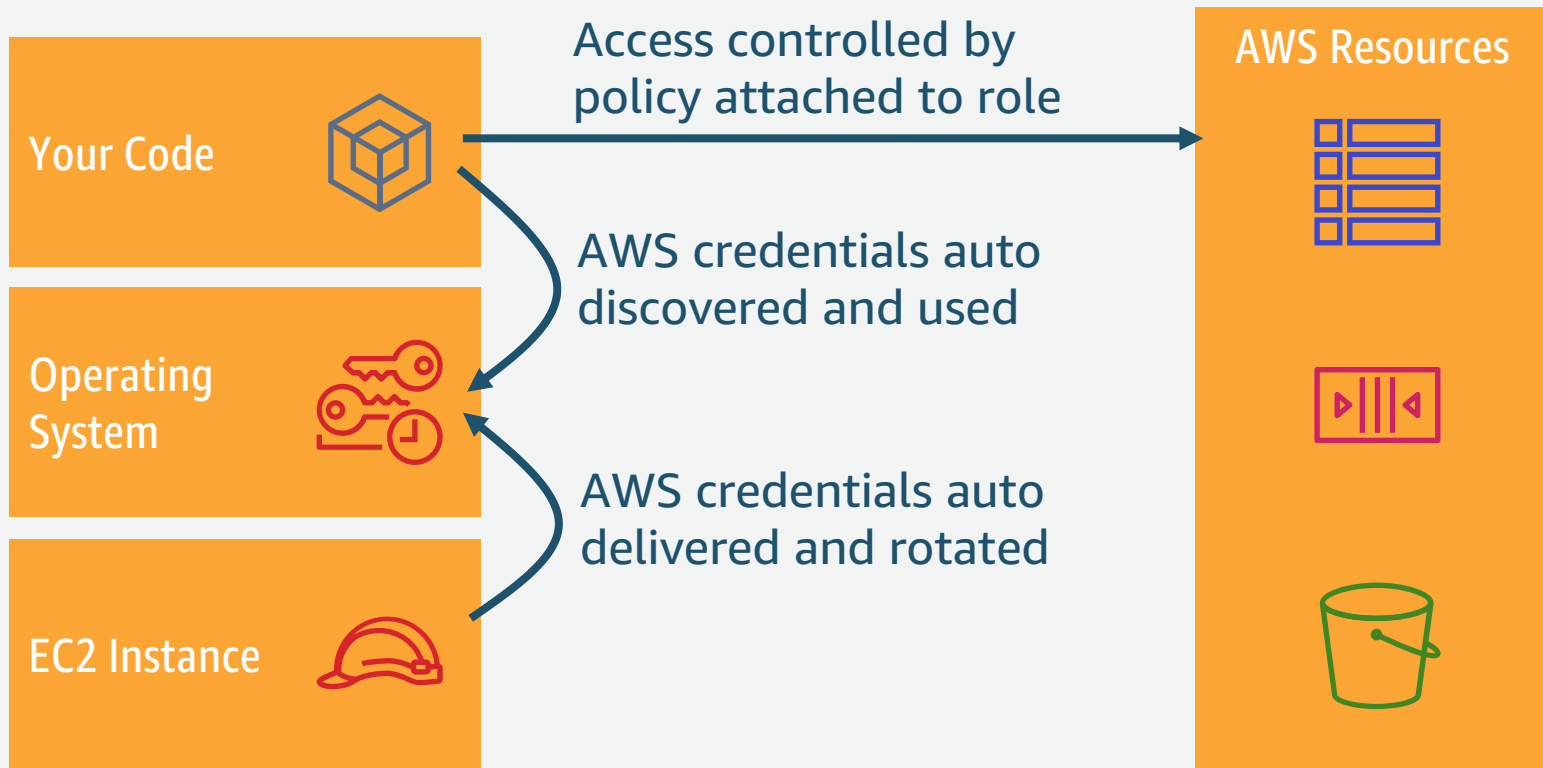
Also works with AWS Lambda & Amazon ECS

aws professional services

AWS Secrets Manager: Retrieve Secret

Your Code

Operating System

EC2 Instance

AWS Resources

Authorized call to Secrets Manager

DB creds returned

connection established

Other Resources

Safe rotation

aws professional services
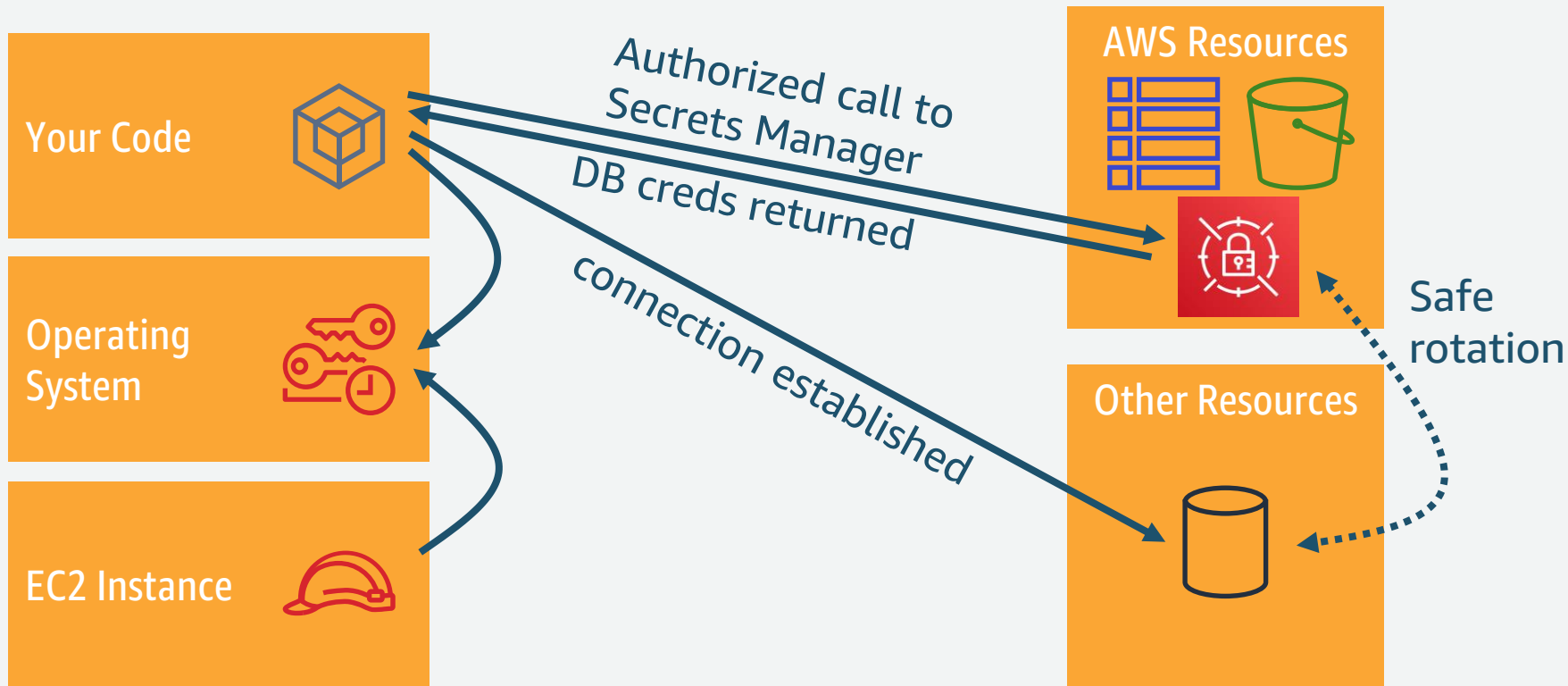
AWS Secrets Manager: Rotate Secret (Integrated)

AWS Secrets Manager

Your Code

Integrated Backend Resource

1) Rotation event

2) New credential creation initiated

3) New credential creation completed

4) New credential promoted to active

5) Secret retrieval gets new version

6) Connection using new credential

aws professional services

Rotate Secret (Custom)

1) Rotation event

AWS Secrets Manager

2) Multi-step rotation (create, set, test, finish)

Custom Lambda Rotator

(You write)

3) Operations per rotation strategy supported by backend

Custom Backend Resource (e.g. 3rd party API key)

4) New cred promoted to active

5) Secret retrieval

Your Code

6) Connection using new credential

aws professional services

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.

aws professional services

Questions?

aws professional services