Get More Out of AWS Config with Multi-Account, Multi-Region Advanced Queries

Archana Sridhar
Sr. Product Manager, AWS Config

May 18, 2020

aws

What you will learn

- How to simplify inventory management using AWS Config
- How to use a Config aggregator
- How to use AWS Config advanced queries across accounts and AWS Regions
- Demos
- Q&A

Inventory management

- What resources currently exist in my account?
- What is the latest configuration state of my resources?
- What relationships exist between my resources?
- What configuration changes occurred within a specific time period?
- Which resources in my account have encryption disabled?

aws

Configuration Compliance Management

- Are my resources configured based on best practices?
- Do my resources comply with regulatory requirements?
- How do I ensure continuous compliance?
- How can I get notified in real-time if certain resources go out of compliance?

aws

Traditionally supported by a
CMDB: Configuration Management Database

Managing cloud resources: How is it different?

- Resources are dynamic in the cloud
- Real time discovery and notification of resources is critical
- Configuration changes need to be recorded instantly
- Real time evaluation of configuration compliance is necessary
- APIs are needed to integrate with other systems

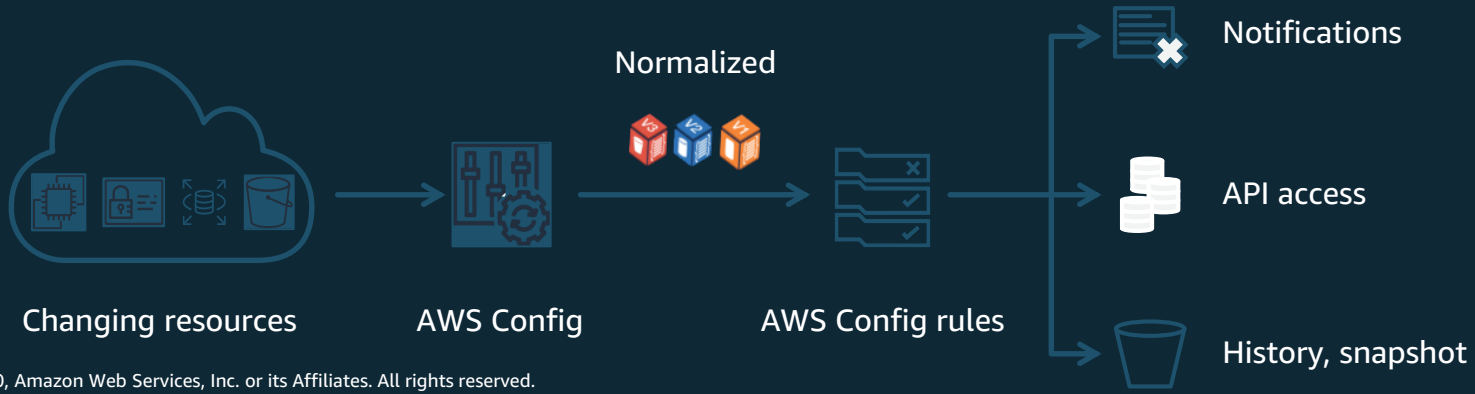
You need a
Cloud-aware CMDB

aws

AWS Config

- ✓ Native, agent-less AWS capability to discover resources in your account
- ✓ Tracks configuration changes and maintains a history (up to 7 years)
- ✓ Evaluates configuration changes against compliance policies (using AWS Config rules)
- ✓ Provides aggregated view of resource configuration and compliance status across accounts and regions
- ✓ Integrates with your own CMDBs (such as ServiceNow)

AWS Config = Continuous Configuration Auditor



Common use cases

Audit & compliance

Maintain a history of all configuration changes for audits

Verify configuration changes do not violate policies

Operational governance

DevOps compliance (e.g. evaluate CI/CD pipeline configuration)

Cost optimization (e.g. terminate unused resources)

Security intelligence

Security incident/breach analysis

Identifying unencrypted resources

Integration with ITSM/CMDB

Integration with asset/inventory management systems

Change management, incident management

aws

AWS Config - Features

Automatic Remediation with Config Rules

Enables you to automatically remediate noncompliant resources

Conformance Packs

Simplifies at-scale deployment of Config rules and associated remediation actions

Custom Configuration Items

Enables you to move non-AWS configuration data in AWS Config

Multi-Account, Multi-Region Data Aggregation

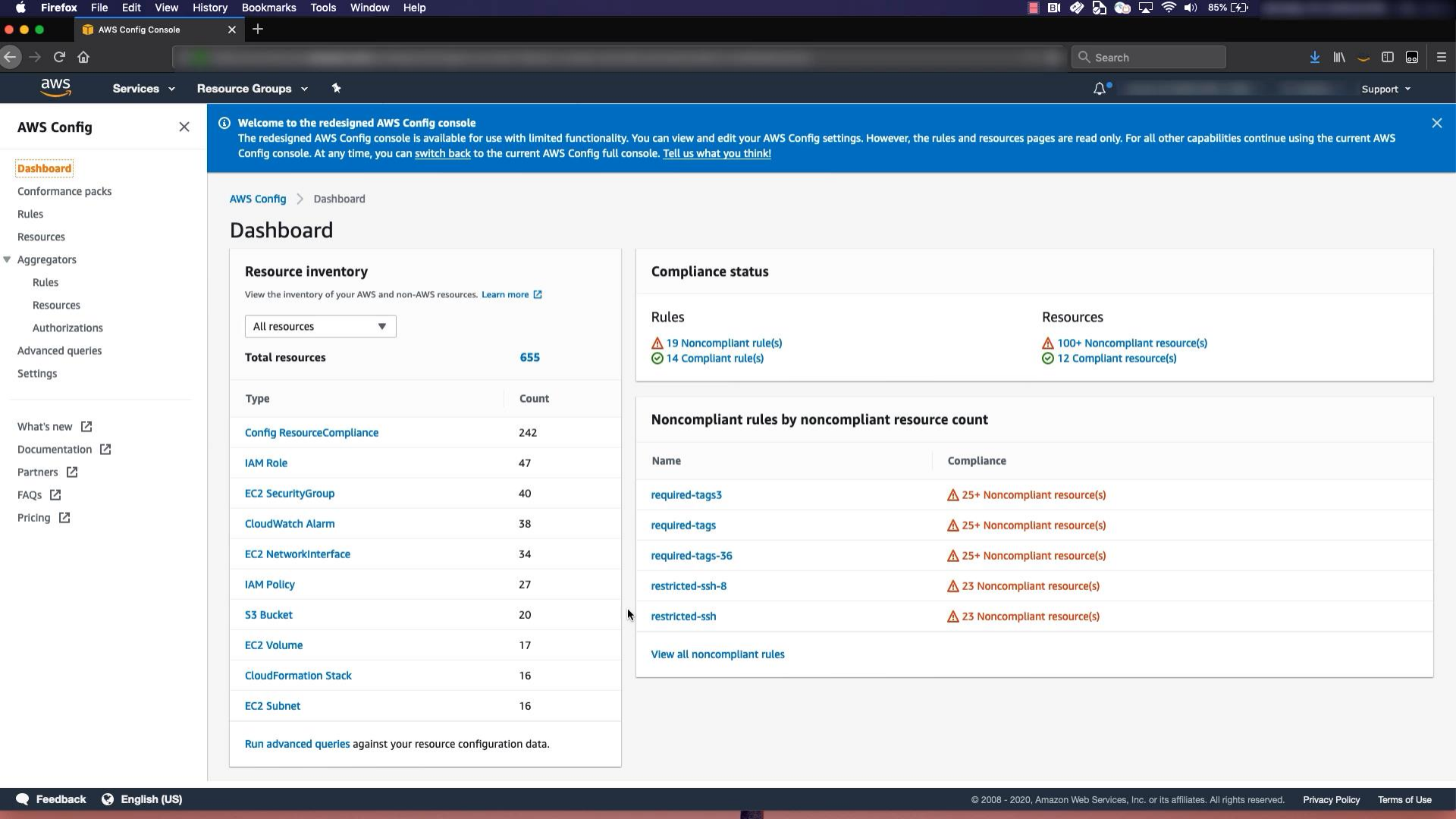
Accounts and regions
Select the source accounts and regions from where you want to to collect AWS Config data

AWS Config data
Collection of AWS Config data from multiple source accounts and regions.

Aggregator
Contains the resource configuration information and the compliance data recorded in AWS Config.

Aggregated View
View all compliant and non-compliant rules and resources for each aggregator.

Demo
Setting up AWS Config Aggregator


Firefox File Edit View History Bookmarks Tools Window Help
AWS Config Console
Search
aws
Services
Resource Groups
Support
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Rules
Resources
Authorizations
Advanced queries
Settings
What's new
Documentation
Partners
FAQs
Pricing
Welcome to the redesigned AWS Config console
The redesigned AWS Config console is available for use with limited functionality. You can view and edit your AWS Config settings. However, the rules and resources pages are read only. For all other capabilities continue using the current AWS Config console. At any time, you can switch back to the current AWS Config full console. Tell us what you think!
AWS Config > Dashboard
Dashboard
Resource inventory
View the inventory of your AWS and non-AWS resources. Learn more
All resources
Total resources 655
Type Count
Config ResourceCompliance 242
IAM Role 47
EC2 SecurityGroup 40
CloudWatch Alarm 38
EC2 NetworkInterface 34
IAM Policy 27
S3 Bucket 20
EC2 Volume 17
CloudFormation Stack 16
EC2 Subnet 16
Run advanced queries against your resource configuration data.
Compliance status
Rules
19 Noncompliant rule(s)
14 Compliant rule(s)
Resources
100+ Noncompliant resource(s)
12 Compliant resource(s)
Noncompliant rules by noncompliant resource count
Name Compliance
required-tags3 25+ Noncompliant resource(s)
required-tags 25+ Noncompliant resource(s)
required-tags-36 25+ Noncompliant resource(s)
restricted-ssh-8 23 Noncompliant resource(s)
restricted-ssh 23 Noncompliant resource(s)
View all noncompliant rules
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

AWS Config Advanced Queries

- Configuration attribute based queries against current state metadata.
- Single endpoint to query metadata across AWS services
- Uses a subset of SQL syntax
- Sample queries available out of the box
- Ability to extend the query across multiple accounts and multiple regions
- Available at no additional cost

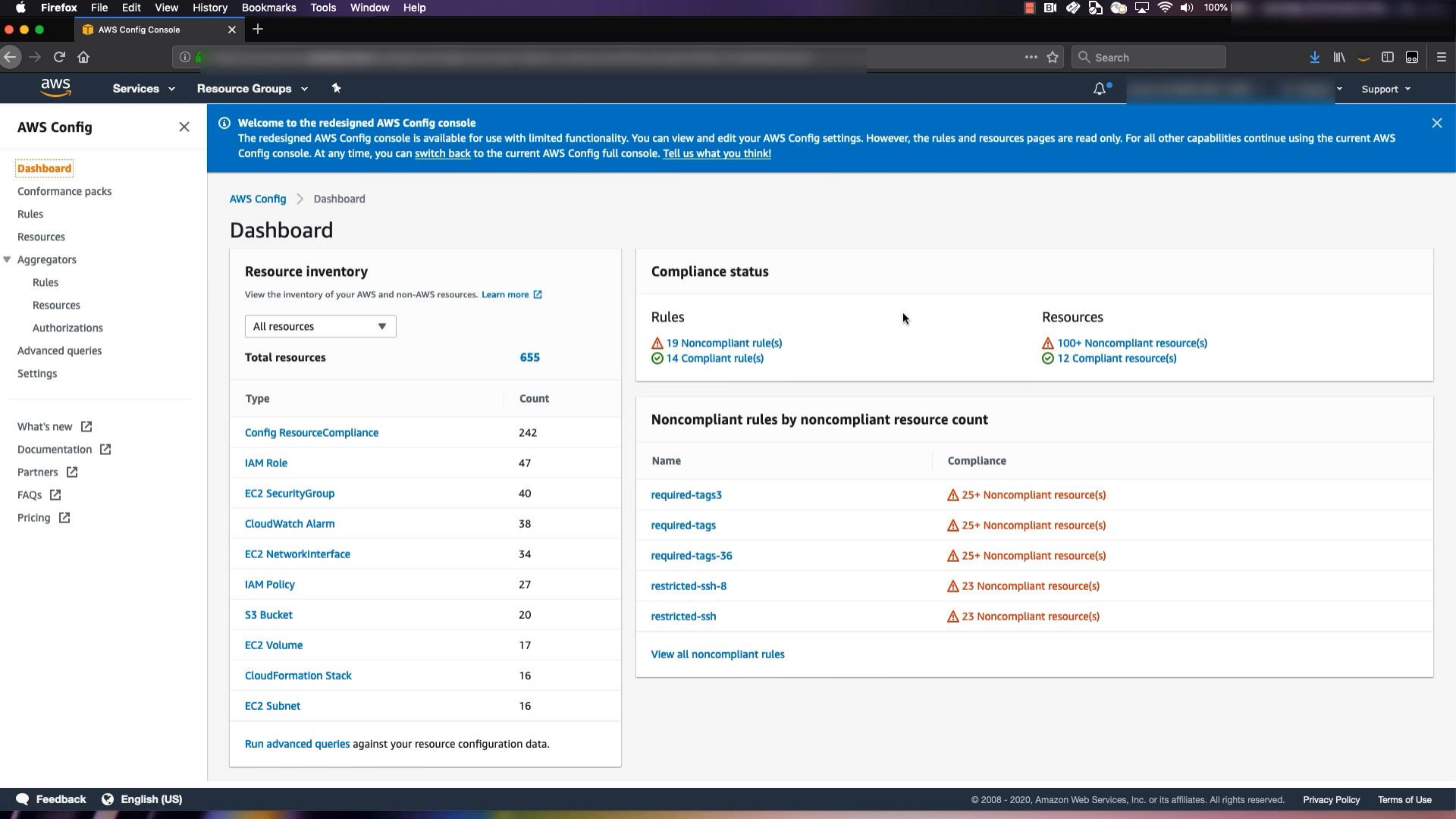
aws

Advanced Query: Use cases

Inventory Management	Identify resources that meet a specific criteria (e.g. EC2 instances of size “xlarge”, MySQL databases running an old version)
Cost Management	Identify unused resources (e.g. EBS volumes that are not in use)
Change Management	Understand impact of a change (e.g. view resources related to a security group)
Security Management	Identify resources that may be vulnerable (e.g. view all RDS instances that are publicly accessible)

aws

Demo
Using AWS Config Advanced Queries


Firefox File Edit View History Bookmarks Tools Window Help
AWS Config Console
Search
aws
Services
Resource Groups
Support
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Rules
Resources
Authorizations
Advanced queries
Settings
What's new
Documentation
Partners
FAQs
Pricing
Welcome to the redesigned AWS Config console
The redesigned AWS Config console is available for use with limited functionality. You can view and edit your AWS Config settings. However, the rules and resources pages are read only. For all other capabilities continue using the current AWS Config console. At any time, you can switch back to the current AWS Config full console. Tell us what you think!
AWS Config > Dashboard
Dashboard
Resource inventory
View the inventory of your AWS and non-AWS resources. Learn more
All resources
Total resources 655
Type Count
Config ResourceCompliance 242
IAM Role 47
EC2 SecurityGroup 40
CloudWatch Alarm 38
EC2 NetworkInterface 34
IAM Policy 27
S3 Bucket 20
EC2 Volume 17
CloudFormation Stack 16
EC2 Subnet 16
Run advanced queries against your resource configuration data.
Compliance status
Rules
19 Noncompliant rule(s)
14 Compliant rule(s)
Resources
100+ Noncompliant resource(s)
12 Compliant resource(s)
Noncompliant rules by noncompliant resource count
Name Compliance
required-tags3 25+ Noncompliant resource(s)
required-tags 25+ Noncompliant resource(s)
required-tags-36 25+ Noncompliant resource(s)
restricted-ssh-8 23 Noncompliant resource(s)
restricted-ssh 23 Noncompliant resource(s)
View all noncompliant rules
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Additional resources

- AWS Config tech docs
- AWS Config Resource schema in GitHub
- AWS Config pricing
- Blogposts
  - AWS Config best practices
  - Manage custom AWS Config rules with remediations using Conformance packs
  - AWS Control Tower Detective Guardrails as an AWS Config Conformance Pack
  - Introducing AWS Config multi account multi Region Advanced Queries

aws

Summary

- Advanced queries enable centralized inventory and compliance management across accounts and regions
- Integrated with AWS Organizations
- Available at no additional cost

Thank you!