
AWS
re:Invent

MGT402

# Manage configuration and compliance in hybrid environments

Brian Terry

Sr Partner SA, CMT
AWS

AWS re:Invent

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



“Out of clutter, find simplicity. From discord, find harmony. In the middle of difficulty lies opportunity.”

Albert Einstein



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

# AWS management and governance services



**Enable**

- AWS Control Tower
- AWS Organizations
- AWS Budgets
- AWS License Manager
- AWS WA Tool



**Provision**

- AWS CloudFormation
- AWS Service Catalog
- AWS OpsWorks
- AWS Marketplace



**Operate**

- Amazon CloudWatch
- AWS CloudTrail
- AWS Systems Manager
- AWS Config
- AWS Trusted Advisor
- AWS Cost and Usage Report
- AWS Cost Explorer

Business agility + governance control

# Agenda

- Capturing resource inventory and configuration history
- Extend inventory and compliance management capabilities
- Demonstration
- Wrap it up





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

# Let’s talk about capturing resource inventory and configuration history!



AWS re:Invent

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

# Inventory and configuration management

- What is currently out there?
- What is the latest configuration state of my resources?
- What relationships exist between my resources?
- What configuration changes occurred in the past?
- Which resources have violated compliance policies?

# Governance and compliance management

- Are my resources properly configured?
- Do my resources comply with regulatory requirements
- How do I ensure continuous compliance?
- How can I get notified in near real-time if resource(s) go out of compliance?

# Benefits



Continuous monitoring



Continuous assessment



Change management

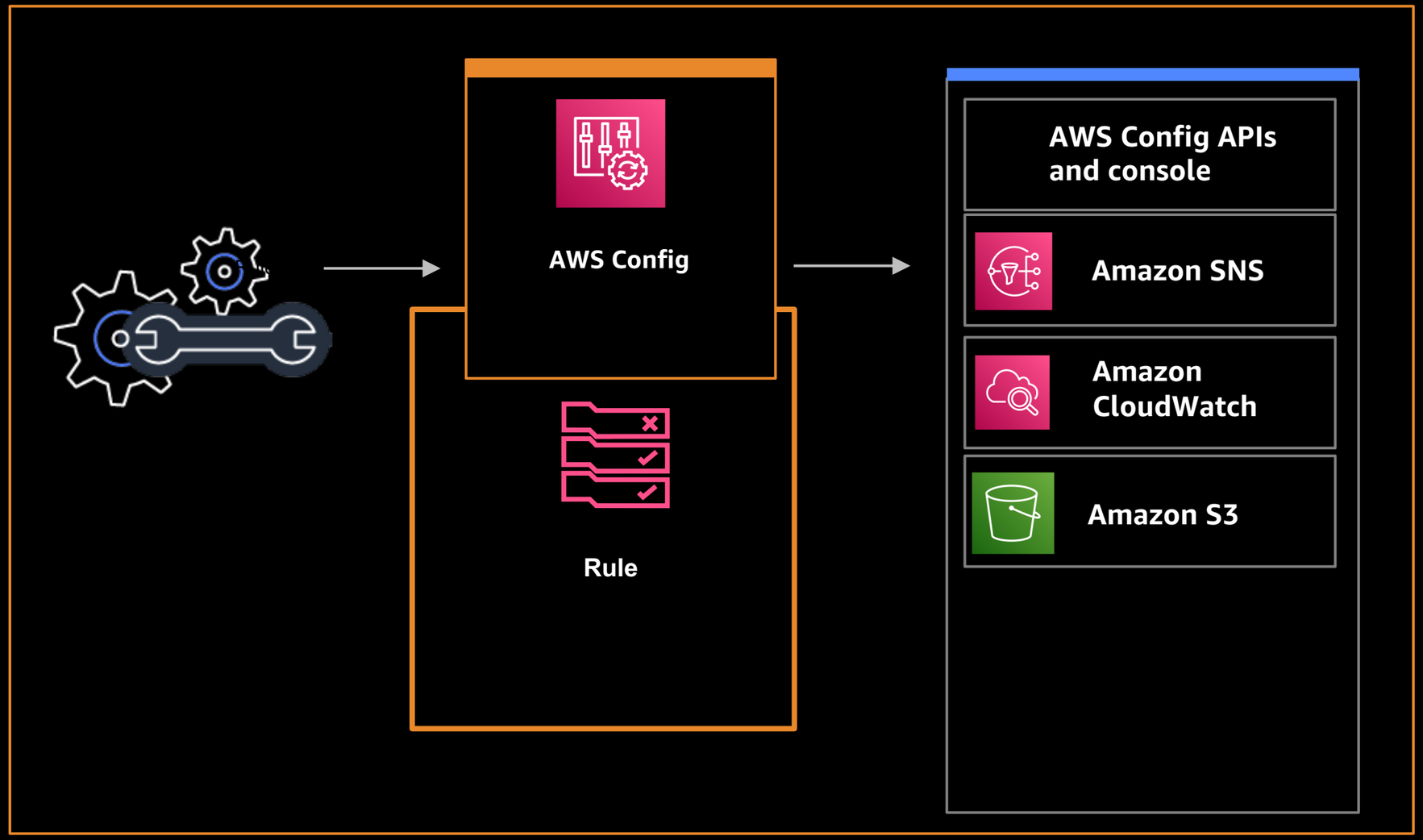


Operational troubleshooting



Enterprise-wide compliance monitoring including third-party resources

# How it works


AWS Config
Rule
AWS Config APIs and console
Amazon SNS
Amazon CloudWatch
Amazon S3

# AWS Config features



## Configuration history of AWS resources

- Records details of changes to your AWS resources to provide you with a configuration history timeline
- Obtain details of what a resource's configuration looked like at any point in the past

## Configuration history of software (requires SSM agent)

- Records software configuration changes within your Amazon EC2 instances and servers running on-premises or other cloud providers
- Provides a history of OS and system-level configuration changes alongside infrastructure configuration changes recorded for EC2 instances

## Configuration snapshots

Provides a point-in-time capture of all your resources and their configurations

## Configurable and customizable rules

- Assess your resource configurations and resource changes for compliance against built-in or custom rules and automate remediation of non-compliant resources
- Customize pre-built rules or create your own custom rules in AWS Lambda that define your internal best practices and guidelines for resource configurations

# AWS Config features



## Resource relationship tracking

- Discovers, maps, and tracks AWS resource relationships in your account
- For example, if a new Amazon EC2 security group is associated with an Amazon EC2 instance, Config records the updated configurations of both the Amazon EC2 security group and the Amazon EC2 instance

## Conformance packs

Packages a collection of AWS Config rules and remediation actions into a single entity and deploy it in a single account or across an entire organization

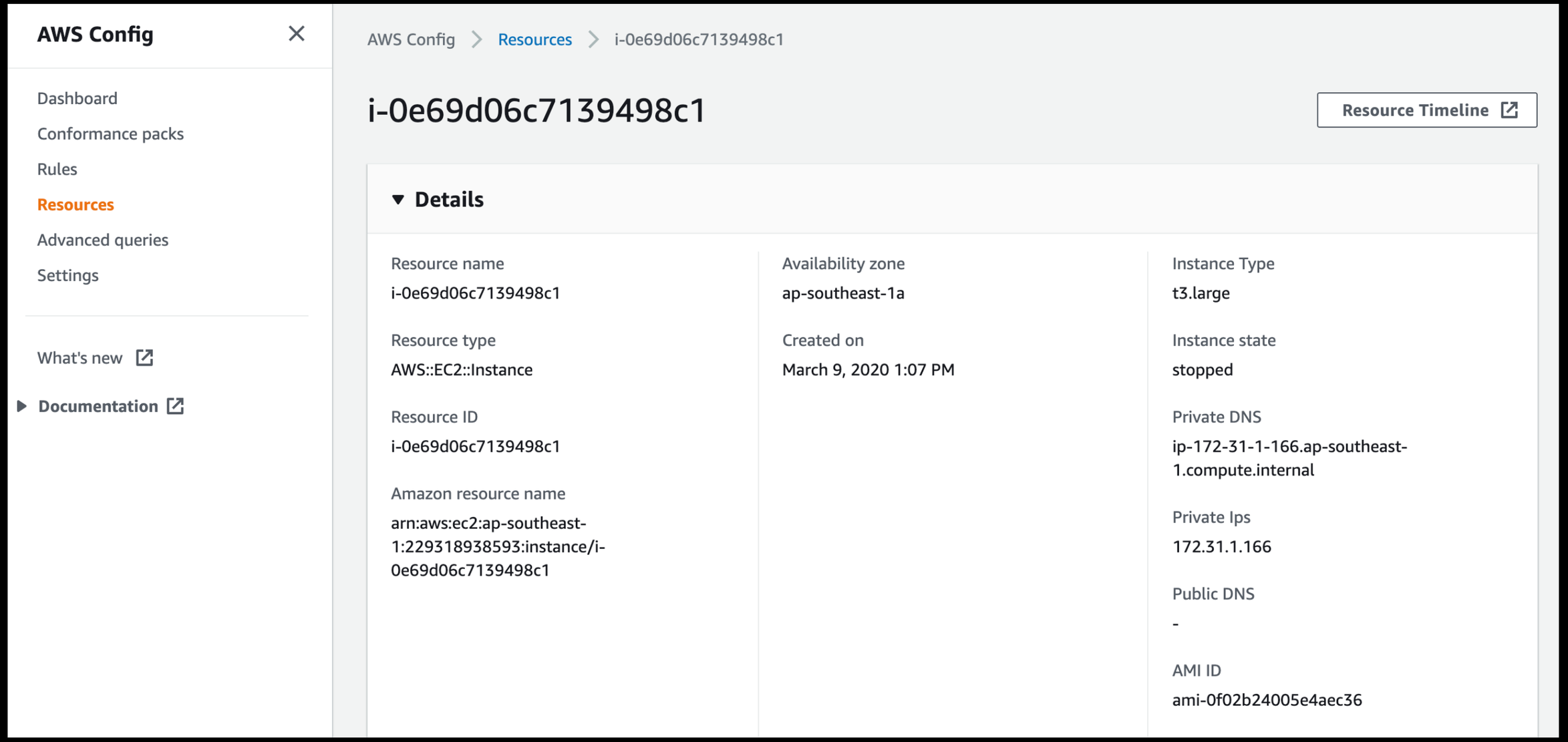
## Multi-account, multi-region data aggregation

Enables centralized auditing and governance by providing an enterprise-wide view of your resources and Config rule compliance status

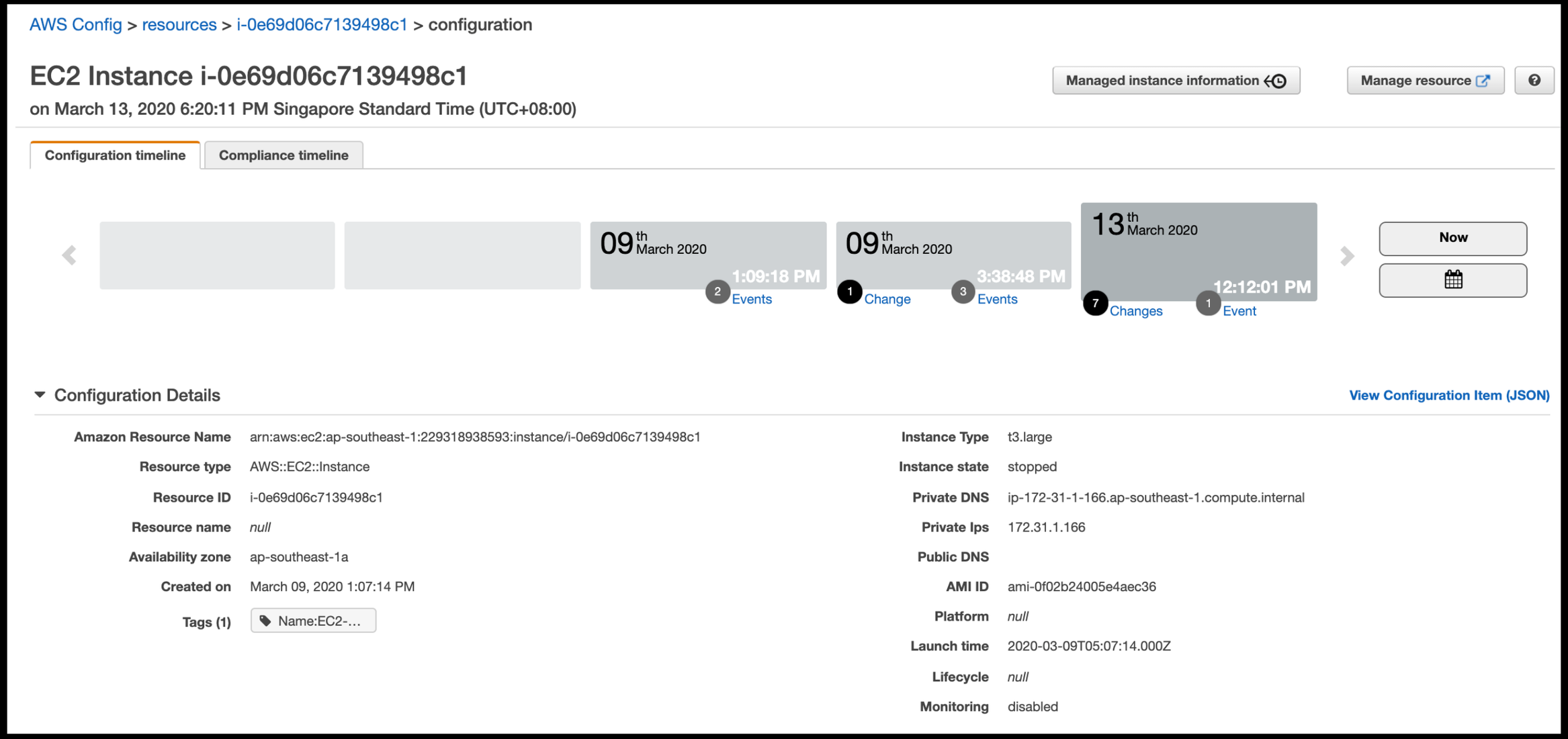
## Cloud governance dashboard

Provides a visual dashboard to help you quickly spot non-compliant resources and take appropriate action

# AWS resource



# Resource timeline



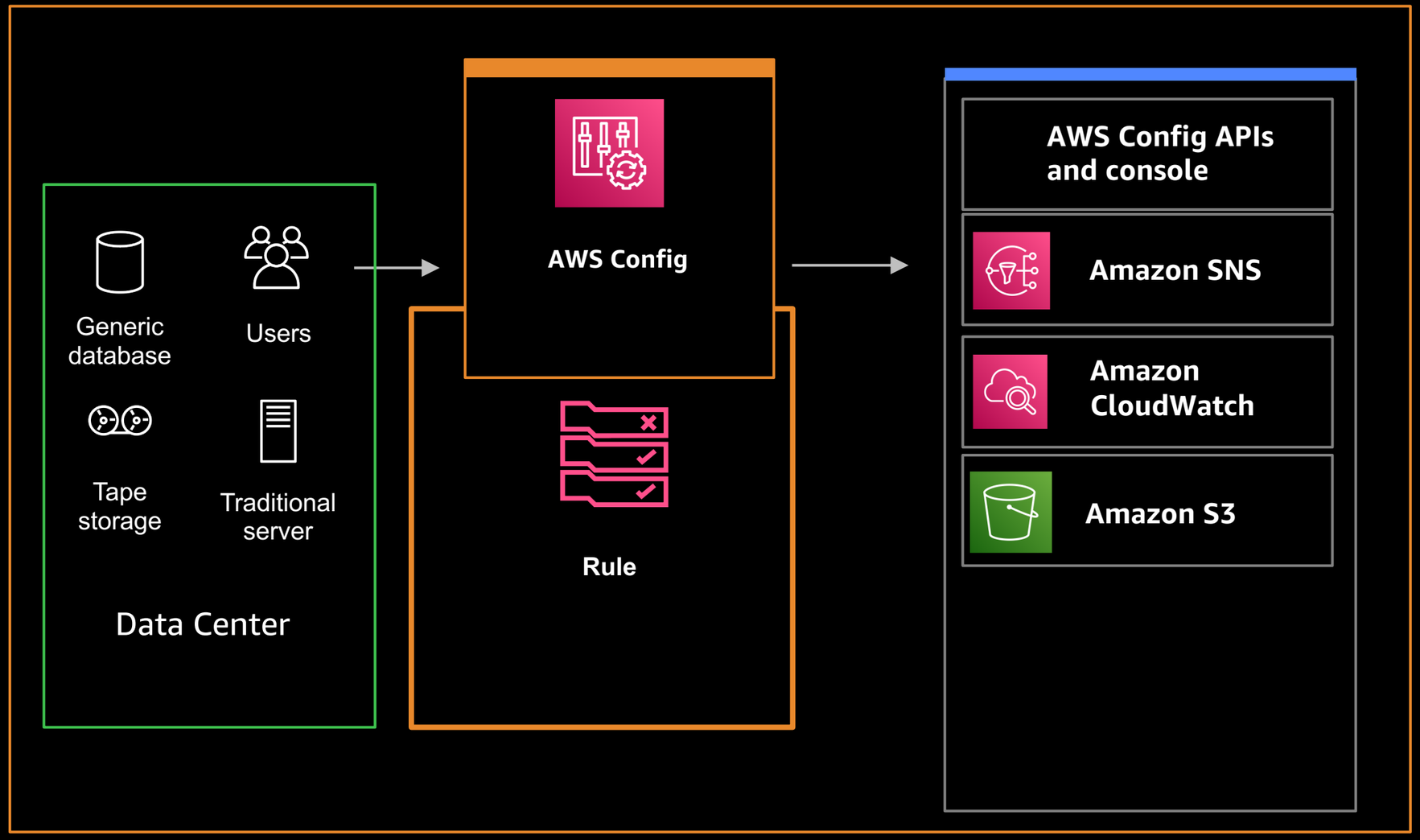
# Extend inventory and compliance management capabilities



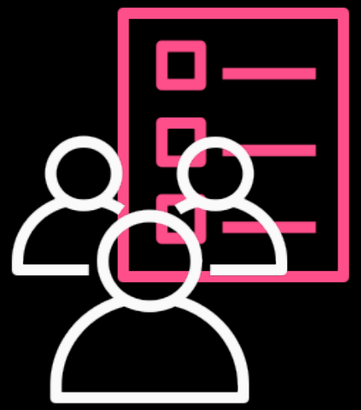
AWS re:Invent

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

# Extend inventory



# Development process



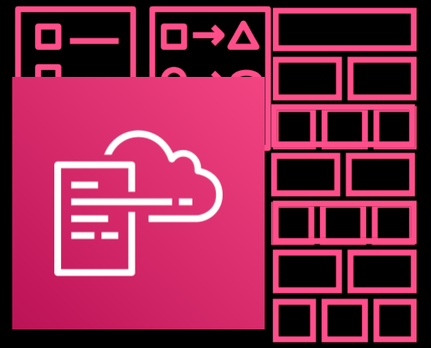
Code

- Generate project
- Edit schema



Submit

- Submit



Deploy

- Deploy your resource

# Unicorns!

MAJESTIC ANIMALS



# Unicorn CI

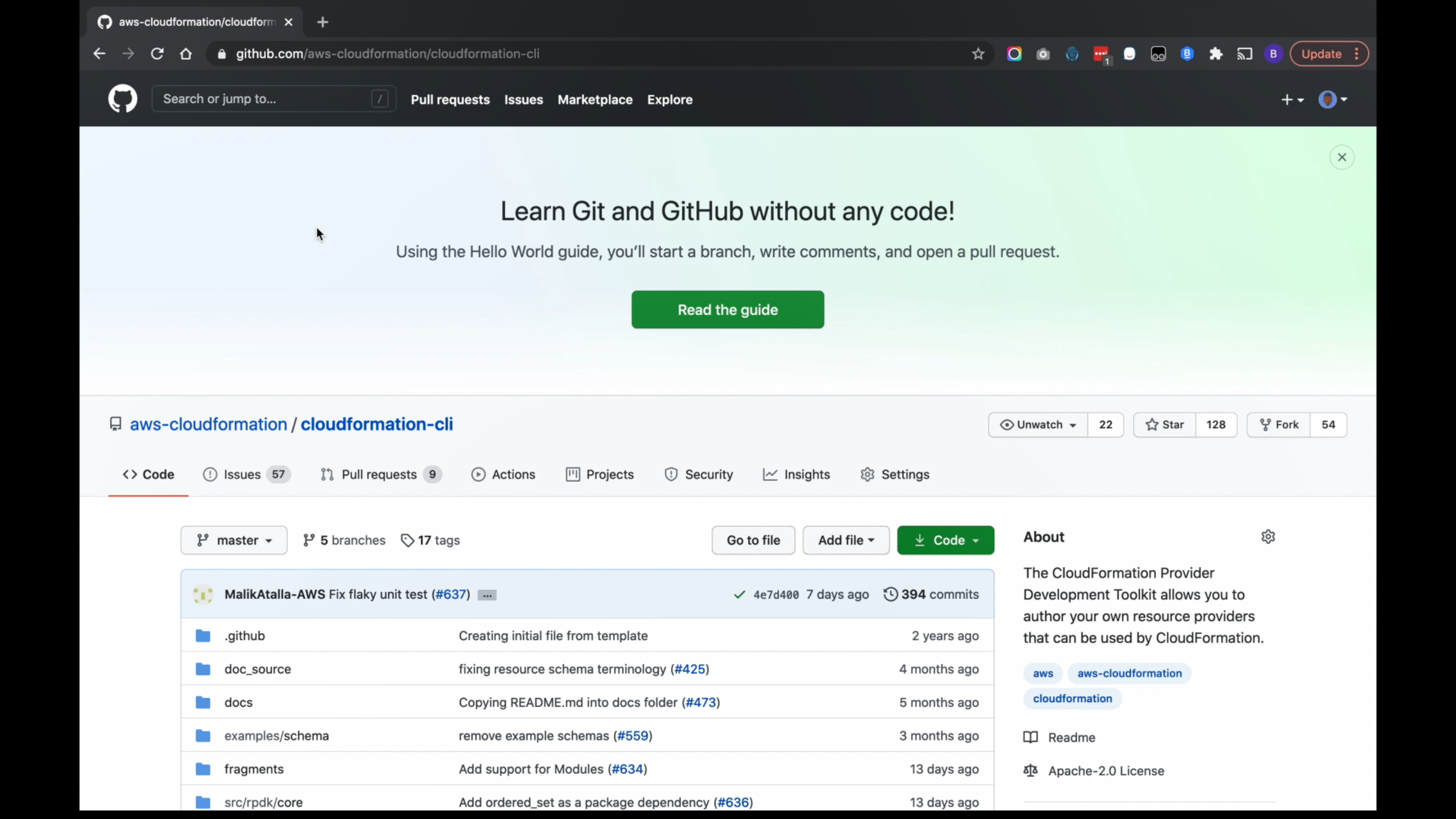


Brianterry::Majestic::Animal

# Unicorn schema



```
{
    "typeName": "Brianterry::Majestic::Animal",
    "description": "A resource that creates unicorns.",
    "sourceUrl": "https://github.com/aws-cloudformation/aws-cloudformation-rpdk.git",
    "properties": {
        "UID": {
            "description": "The ID of the majestic animal",
            "type": "string"
        },
        "Name": {
            "description": "The name of the majestic animal",
            "type": "string",
            "minLength": 3,
            "maxLength": 250
        },
        "Color": {
            "description": "The Color of the majestic animal",
            "type": "string",
            "minLength": 3,
            "maxLength": 250
        }
```


aws-cloudformation/cloudform
github.com/aws-cloudformation/cloudformation-cli
Update
Search or jump to...
Pull requests
Issues
Marketplace
Explore
Learn Git and GitHub without any code!
Using the Hello World guide, you'll start a branch, write comments, and open a pull request.
Read the guide
aws-cloudformation / cloudformation-cli
Unwatch 22
Star 128
Fork 54
Code
Issues 57
Pull requests 9
Actions
Projects
Security
Insights
Settings
master
5 branches
17 tags
Go to file
Add file
Code
MalikAtalla-AWS Fix flaky unit test (#637)
4e7d400 7 days ago
394 commits
.github Creating initial file from template 2 years ago
doc_source fixing resource schema terminology (#425) 4 months ago
docs Copying README.md into docs folder (#473) 5 months ago
examples/schema remove example schemas (#559) 3 months ago
fragments Add support for Modules (#634) 13 days ago
src/rpdk/core Add ordered_set as a package dependency (#636) 13 days ago
About
The CloudFormation Provider Development Toolkit allows you to author your own resource providers that can be used by CloudFormation.
aws
aws-cloudformation
cloudformation
Readme
Apache-2.0 License

# 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.