AWS re:Invent

WPS308

Continuous monitoring techniques in AWS GovCloud (US)

Randy Domingo
Consultant
Amazon Web Services

Brian Landry
Consultant
Amazon Web Services

AWS re:Invent

aws

Objectives

NIST 800-137: “Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

Demonstrate, discuss, and whiteboard reusable solutions we’ve implemented across our DoD engagements in AWS GovCloud (US)

Q&A (Gather more use cases!)

Solutions available (with how-to videos) at

https://github.com/aws-samples/aws-govcloud-continuous-monitoring/

Agenda

Multi-account automation documents

AWS Config managed rules

Identifying unmanaged configuration changes

Create Jira issues upon creation of unencrypted Amazon Elastic Block Store (Amazon EBS) volumes

Auto-tag resources

Alert on protected actions

Alert on manual tag modifications

Amazon Virtual Private Cloud (Amazon VPC) flow log visualization

Pseudo parameters

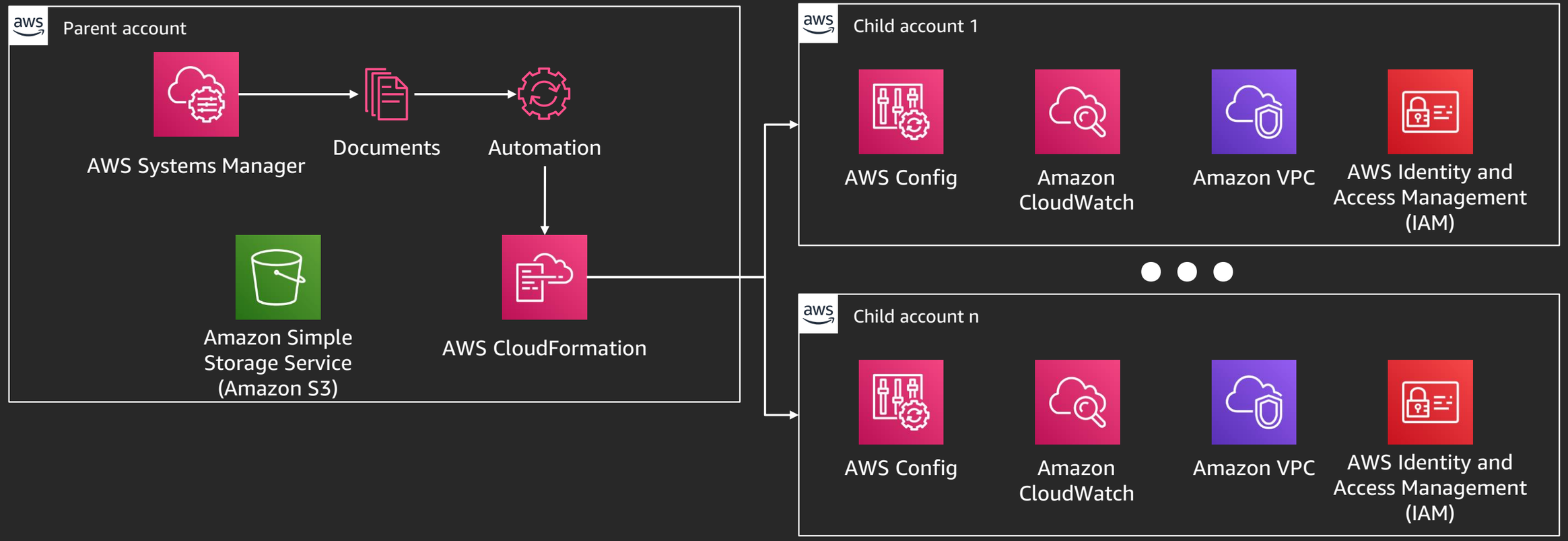
AWS::Partition

AWS::Region

Reference: “Pseudo Parameters Reference”

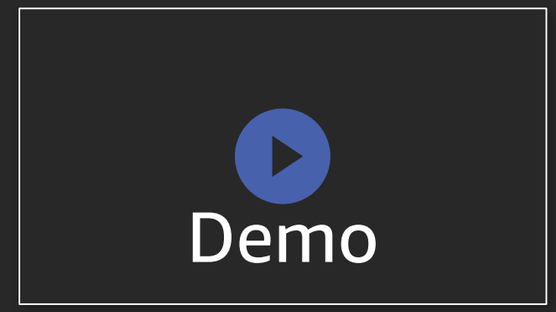
Multi-account automation documents

Demo



Reference: “Managing AWS resources across multiple accounts and Regions using AWS Systems Manager Automation”

AWS Config managed rules



Required tags

Running Amazon Elastic Compute Cloud (Amazon EC2) instances use specified AMIs

Amazon EC2 instances are managed by Systems Manager

Attached Amazon EBS volumes are encrypted

Amazon Relational Database Service (Amazon RDS) DB instances have backups enabled

AWS CloudTrail is enabled

Amazon VPC flow logs are enabled

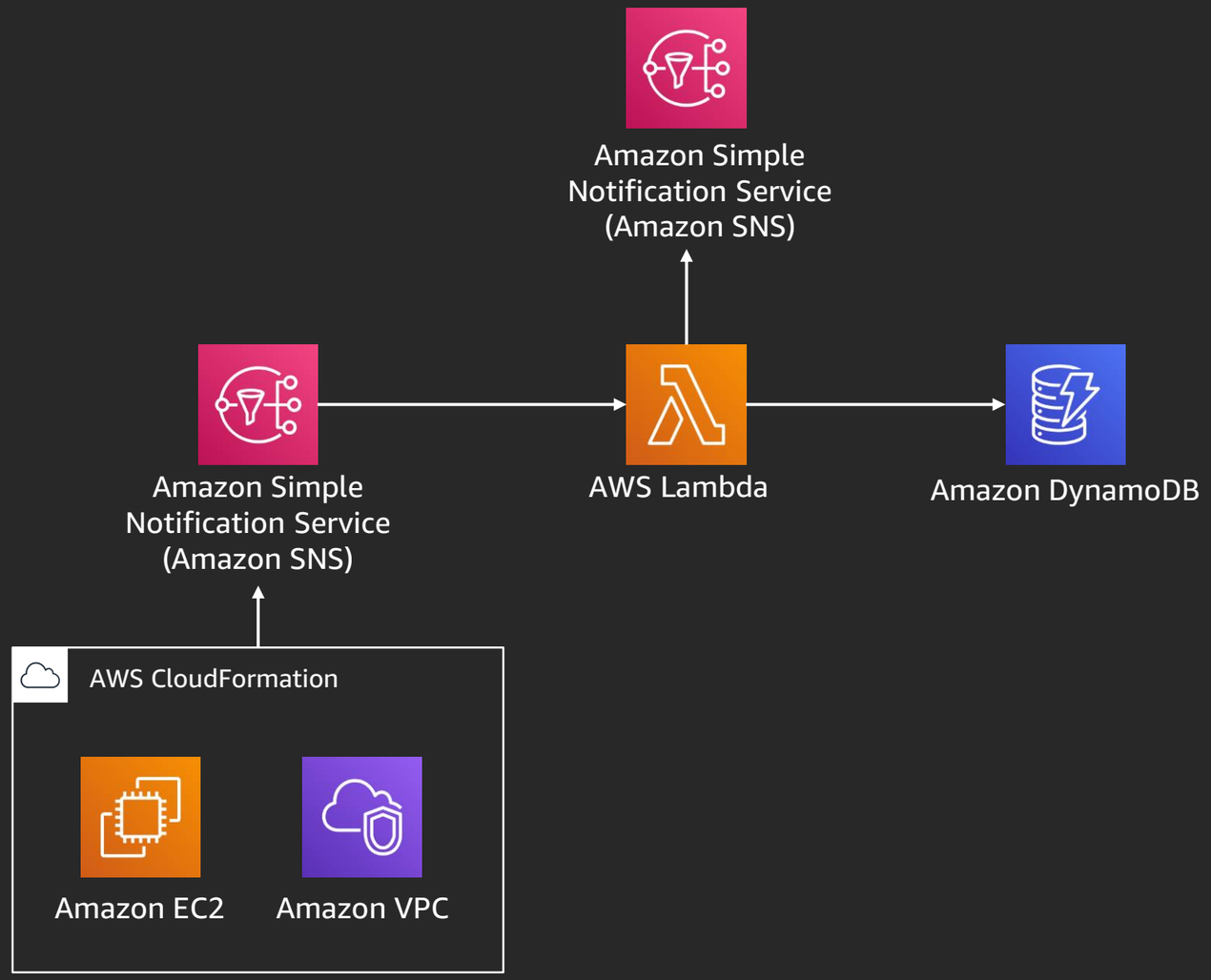
Amazon S3 buckets do not allow public read/write access

And more …

Reference: “List of AWS Config Managed Rules”

Identifying unmanaged configuration changes

Demo



Create Jira issues upon creation of unencrypted Amazon EBS volumes

Demo

Auto-tag resources

Demo


```
"EventPattern": {
  "source": ["aws.ec2","aws.s3","aws.rds"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["ec2.amazonaws.com","s3.amazonaws.com","rds.amazonaws.com"],
    "eventName": ["RunInstances","CreateBucket","CreateDBInstance"]
  }
}
```

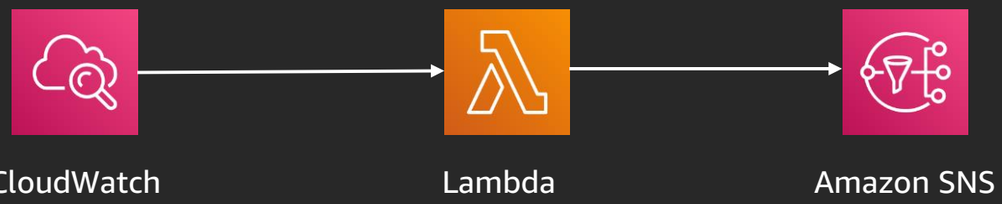
Alert on protected actions

Demo


```
"EventPattern": {
  "detail": {
    "eventName": ["StopLogging”, “CreateRoute”, “AttachInternetGateway”, “AttachVpnGateway”, “CreateVpcPeeringConnection”, “CreateUser”, “CreateSAMLProvider”, “DeleteBucketPolicy"]
  }
}
```

Alert on manual tag modifications

Demo




```
for t in tag_list:
  if (event['detail']['userAgent'] !='cloudformation.amazonaws.com')
    and
    (t['key'] in protected_tags):
```

VPC flow log visualization

Demo

Reference: “How to Visualize and Refine Your Network’s Security by Adding Security Group IDs to Your Amazon VPC Flow Logs”

Demonstration/whiteboard/Q&A

Agenda

Multi-account automation documents

AWS Config managed rules

Identifying unmanaged configuration changes

Create Jira issues upon creation of unencrypted Amazon EBS volumes

Auto-tag resources

Alert on protected actions

Alert on manual tag modifications

Amazon VPC flow log visualization

Thank you!

Randy Domingo
domrandy@amazon.com

Brian Landry
landrybr@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.