
AWS
re:Invent

SEC320

Use AWS Firewall Manager to audit overpermissive security groups

Adhish Bhobe

Senior Product Manager
AWS

AWS re:Invent

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

Agenda

AWS Firewall Manager: An introduction

Current challenges

Deep dive: Audit Amazon VPC security groups using Firewall Manager

Demo

Getting started



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

Service overview



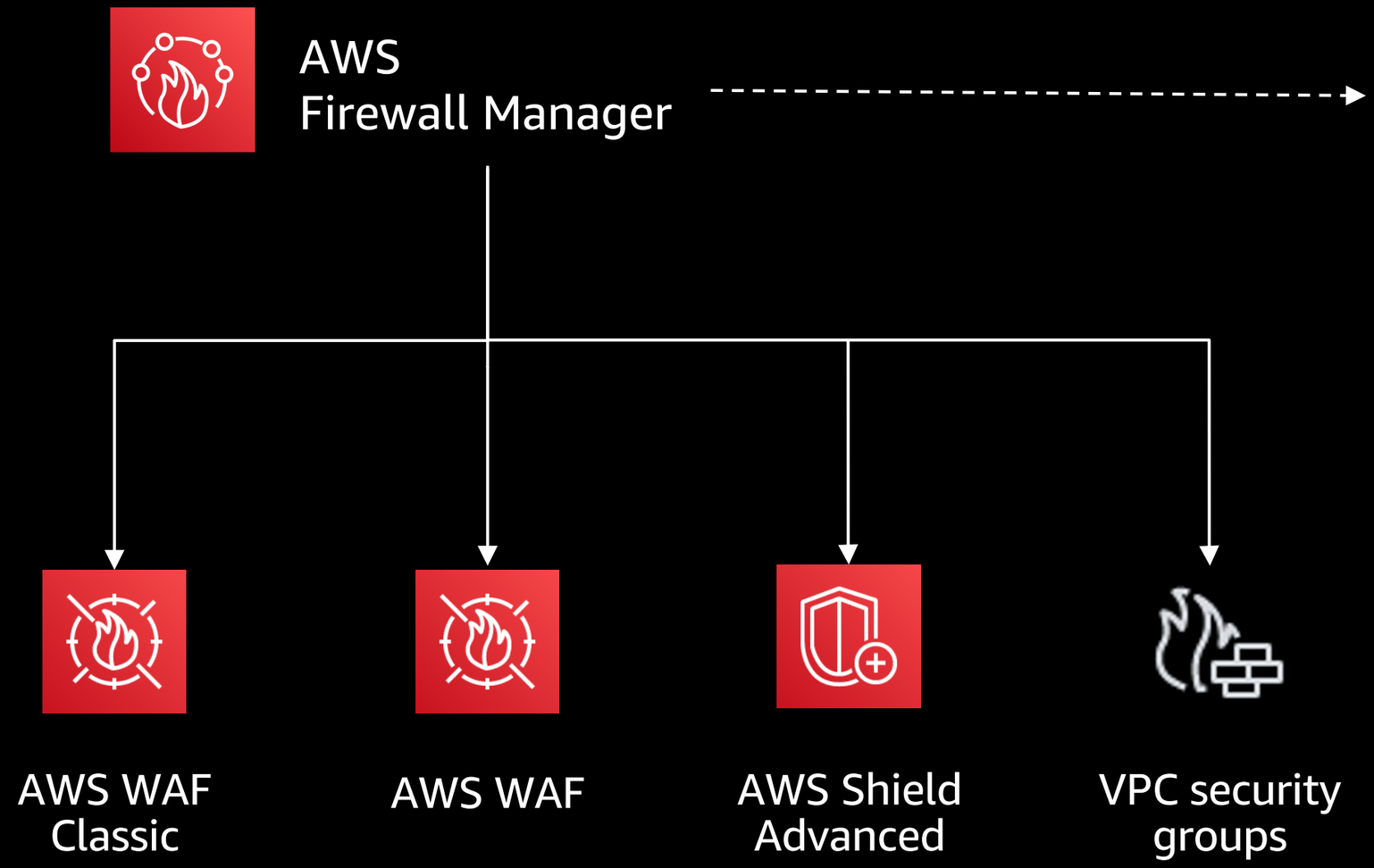
Central security teams
and multiple accounts



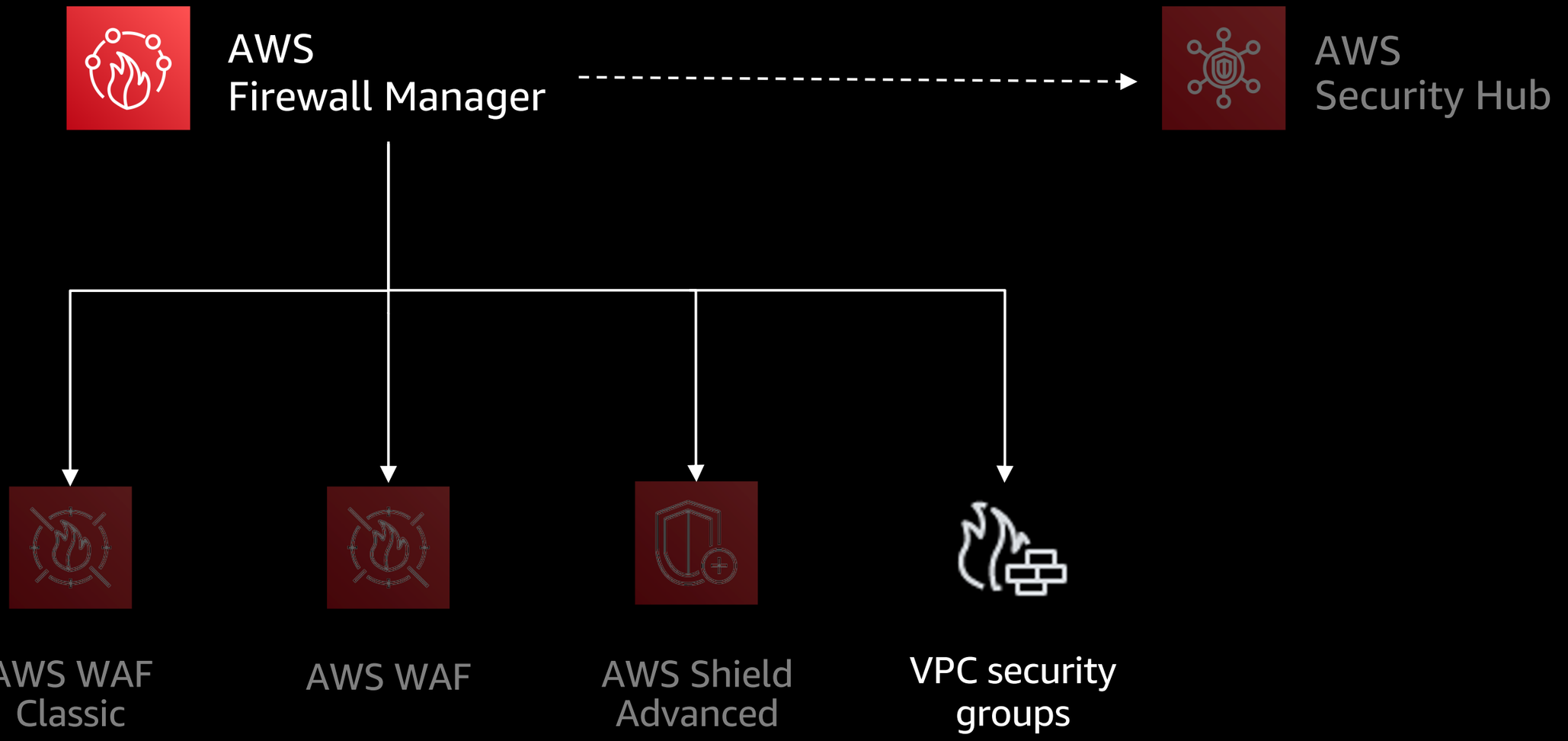
Scale firewall rules
organization wide

AWS Firewall Manager is a security management service to centrally configure and manage your firewall policies across your accounts and applications in your organization

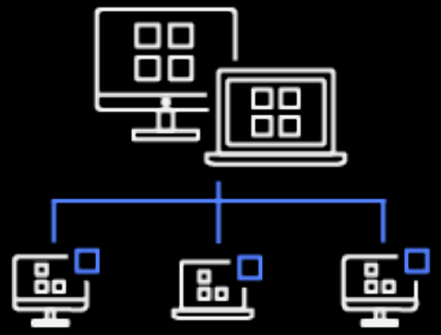
Firewall Manager supports AWS WAF, AWS Shield Advanced, and VPC security groups



Firewall Manager supports AWS WAF, AWS Shield Advanced, and VPC security groups



Challenge: Monitoring for over-permissive VPC security groups



Distributed ownership of security groups



Constant changes to resources and security group rules



Central visibility into violations and non-compliant events

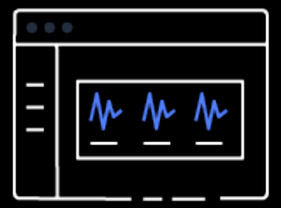
Audit VPC security groups using Firewall Manager



Centrally monitor VPC security groups



Managed policies to remediate over-permissive rules

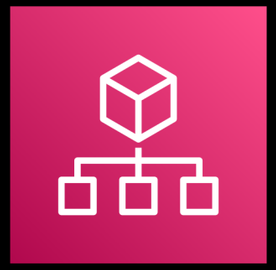


Continuous audit of new and existing resources

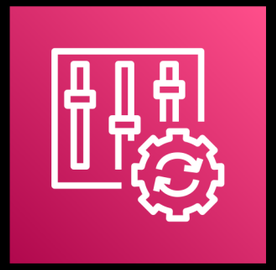


Central reporting dashboard

Firewall Manager prerequisites



Enable AWS Organizations full feature

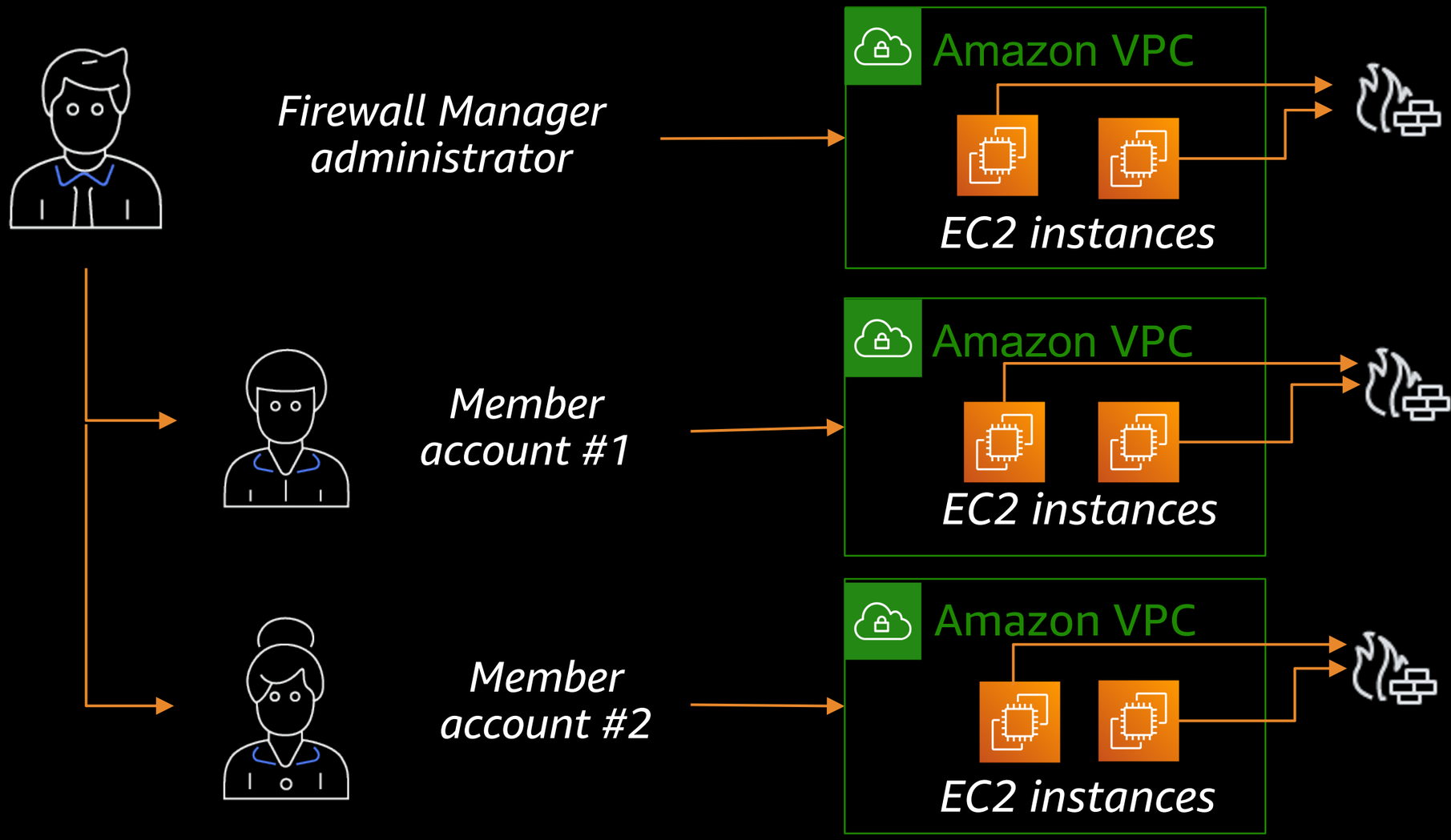


Enable AWS Config on all accounts

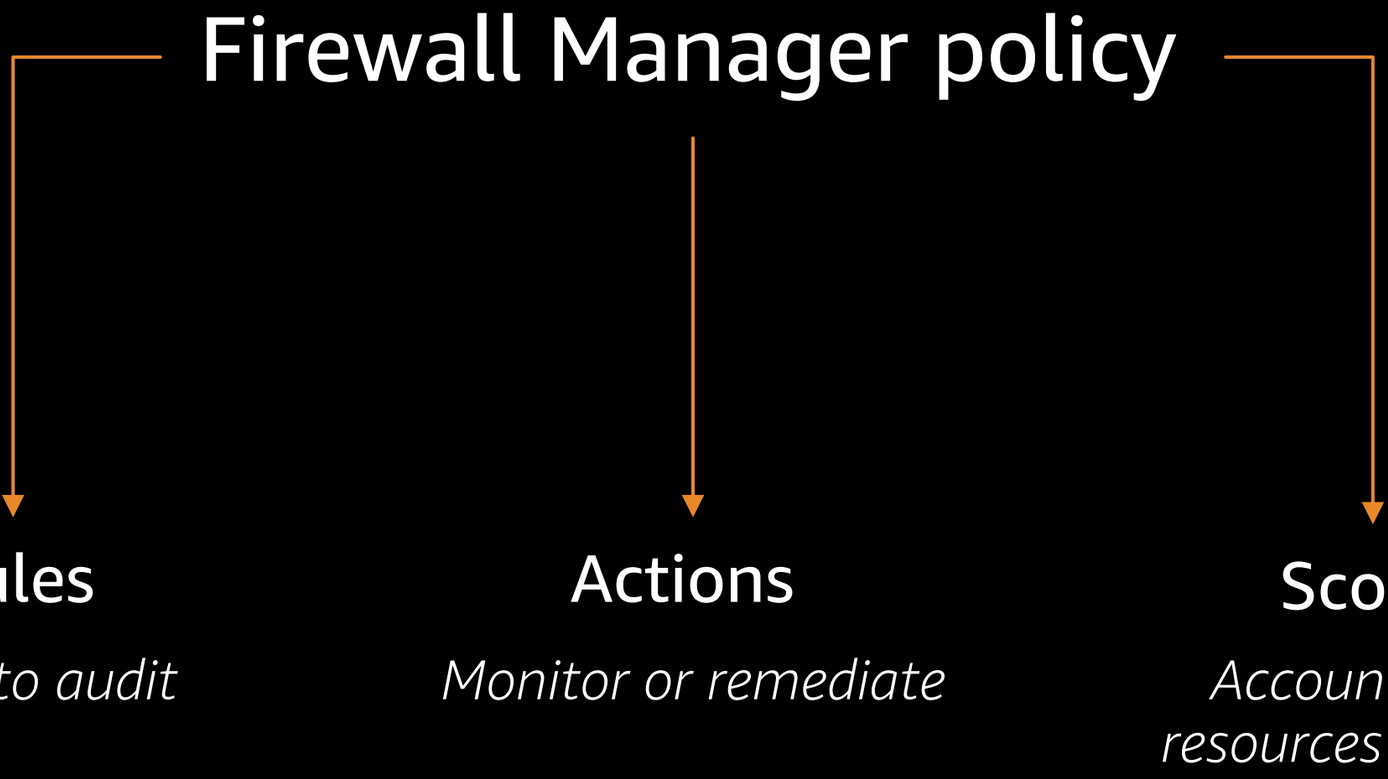


Designate Firewall Manager administrator

Demo setup


Firewall Manager administrator
Amazon VPC
EC2 instances
Member account #1
Amazon VPC
EC2 instances
Member account #2
Amazon VPC
EC2 instances

Demo : Firewall Manager basics



Demo #1

Use case

- Audit security groups rules with overly permissive CIDR ranges
- Detect violating security groups across your organization
- Remediate violating rules

New EC2 Experience
Tell us what you think

EC2 Dashboard New
Events New
Tags
Limits

Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Scheduled Instances
Capacity Reservations

Images
AMIs

Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

Network & Security

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Running instances	0	Dedicated Hosts	0
Elastic IPs	0	Instances (all states)	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2
Snapshots	0	Volumes	0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the US East (N. Virginia) Region

Scheduled events

Account attributes

Supported platforms
- VPC

Default VPC
vpc-b9bdd7c3

Settings

EBS encryption
Zones
Default credit specification
Console experiments

Explore AWS

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads.
Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in

Demo #2

Use case

- Audit for high-risk applications such as RDP and SSH open to the internet
- Identify accounts and security groups that expose these applications
- Remediate security group rules

New EC2 Experience
Tell us what you think

EC2 Dashboard New
Events New
Tags
Limits

Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Scheduled Instances
Capacity Reservations

Images
AMIs

Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

Network & Security

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Running instances	0	Dedicated Hosts	0
Elastic IPs	0	Instances (all states)	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2
Snapshots	0	Volumes	0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the US East (N. Virginia) Region

Scheduled events

Account attributes

Supported platforms
- VPC

Default VPC
vpc-c9d41bb4

Settings

EBS encryption
Zones
Default credit specification
Console experiments

Explore AWS

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads.
Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in

What have we learned so far?

- Challenges with monitoring overpermissive security group rules
- Enable quick-start audit rules to monitor VPC security groups
- Analyze violations with central dashboard
- Remediate non-compliant events across your organization

Getting started



- AWS solution - **AWS Centralized WAF and VPC security group management**
- Reference solution to automate the setup for Firewall Manager service
- AWS managed rules to audit VPC security groups

Visit aws.amazon.com/firewall-manager

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.