

The background features a dark blue gradient with large, overlapping, semi-transparent shapes in shades of purple and magenta. Two thin, light blue lines intersect diagonally across the upper right portion of the image.

AWS re:Invent

DECEMBER 2 - 6, 2024 | LAS VEGAS, NV

COP378

New governance capabilities for multi-account environments

Tim Honychurch

(he/him)

Principal Specialist, Cloud Governance
AWS

Naveen Ravisanker

(he/him)

Sr. Product Manager, AWS Organizations
AWS



Speakers



Tim Honychurch

He/him
Principal Specialist, Cloud Governance
AWS



Naveen Ravisankar

He/him
Sr. Product Manager, AWS Organizations
AWS



Agenda

- 01 Cloud Governance defined
- 02 What's new in Control Policies
- 03 Observability and governance

What is cloud governance?



AWS cloud governance helps you align your AWS cloud use with your business objectives.

AWS Cloud Governance Mission

Move fast toward business objectives

Security & Compliance

Efficient operations



Why is governance challenging?



Balance: innovation & controls



Keep pace with regulations



Stay agile



Cost consciousness



Operational efficiency

Customer success story

CLEARWATER
ANALYTICS.



Priorities

Rapid growth
Scale
Automation
Efficiency – lean team



AWS Organizations



AWS Control Tower



Policies



Outcomes

+200% management capacity
Independent developers
Safety net



What's new in governance



AWS Organizations & AWS Control Tower

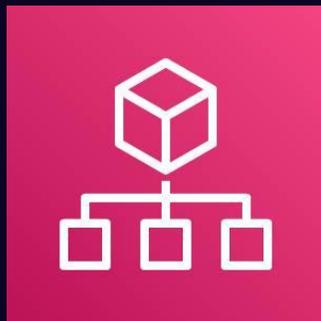
AWS Control Tower



Offers an **easy way to setup and govern** a secure, multi-account AWS environment

500+ preconfigured, managed controls

AWS Organizations



Helps you **centrally govern** a multi-account AWS environment using policies

AWS Organization Policies

Authorization Policies

Manage **access for principals and resources**

- Service Control Policies
- Resource Control Policies (Nov, 2024)

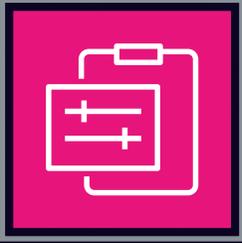
Management Policies

Manage **configuration of AWS services**

- Backup Policies
- Tag Policies
- AI-Optout Policies
- Chatbot Policies (October 2024)
- Declarative Policies for Amazon EC2

re:Invent
2024

Customer need



Enforce uniform configuration



Peace of mind



Apply configuration at scale

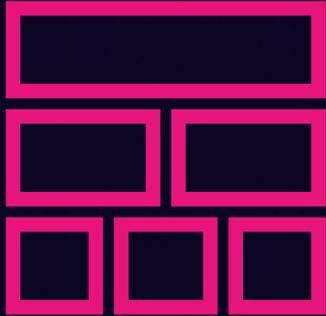
Example Configuration

I'm an enterprise admin

**I have an AWS organization with
500 accounts**

I want to block public access of VPCs

Service Configuration – Customer Challenges



Enforcing at scale

Running campaigns

Understanding current configurations

Service Configuration – Customer Challenges



Navigate complexity

VPCs

Internet Gateways

NAT Gateway

Subnets

Route tables

Security Groups

Service Configuration – Customer Challenges

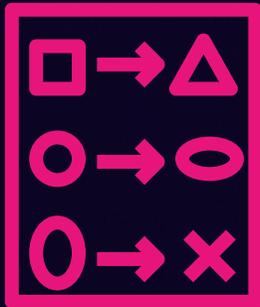


Navigate
complexity

Protect these configurations using an SCP

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

Service Configuration – Customer Challenges



Continuously monitor
& update policies

Monitor every new feature, resource, principal, action and account

Update the policy to ensure the intent is maintained

Service Configuration – Customer Challenges



End user
challenge

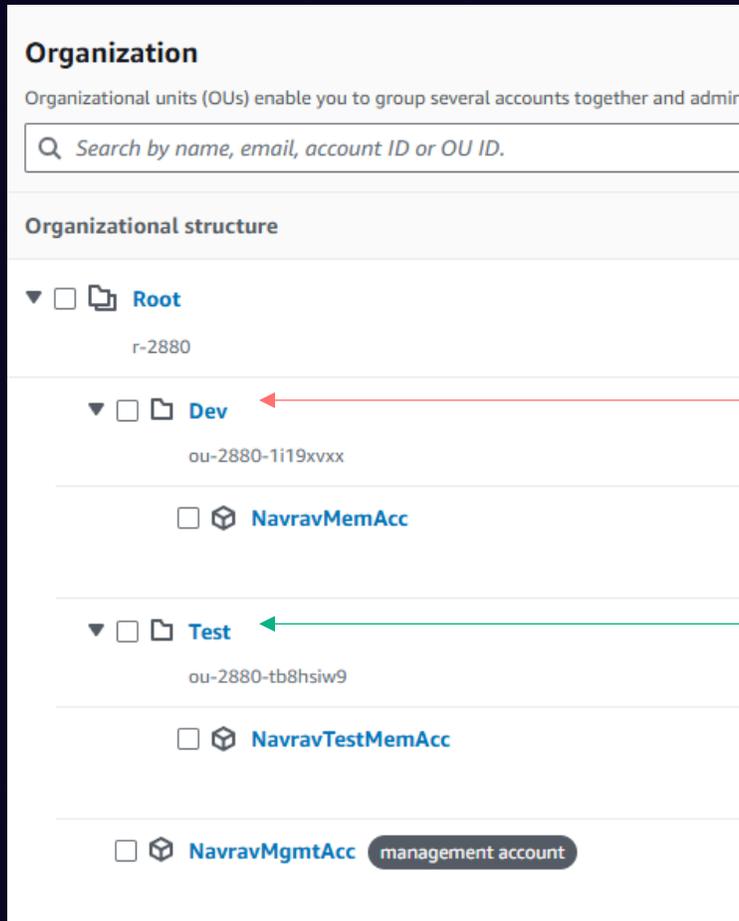
Decoding errors can be challenging

Declarative Policies

Declare and enforce desired configuration for a given AWS service at scale across your organization

Declarative Policies - DEMO Set Up

Objective: Block public access to VPCs in a specific OU



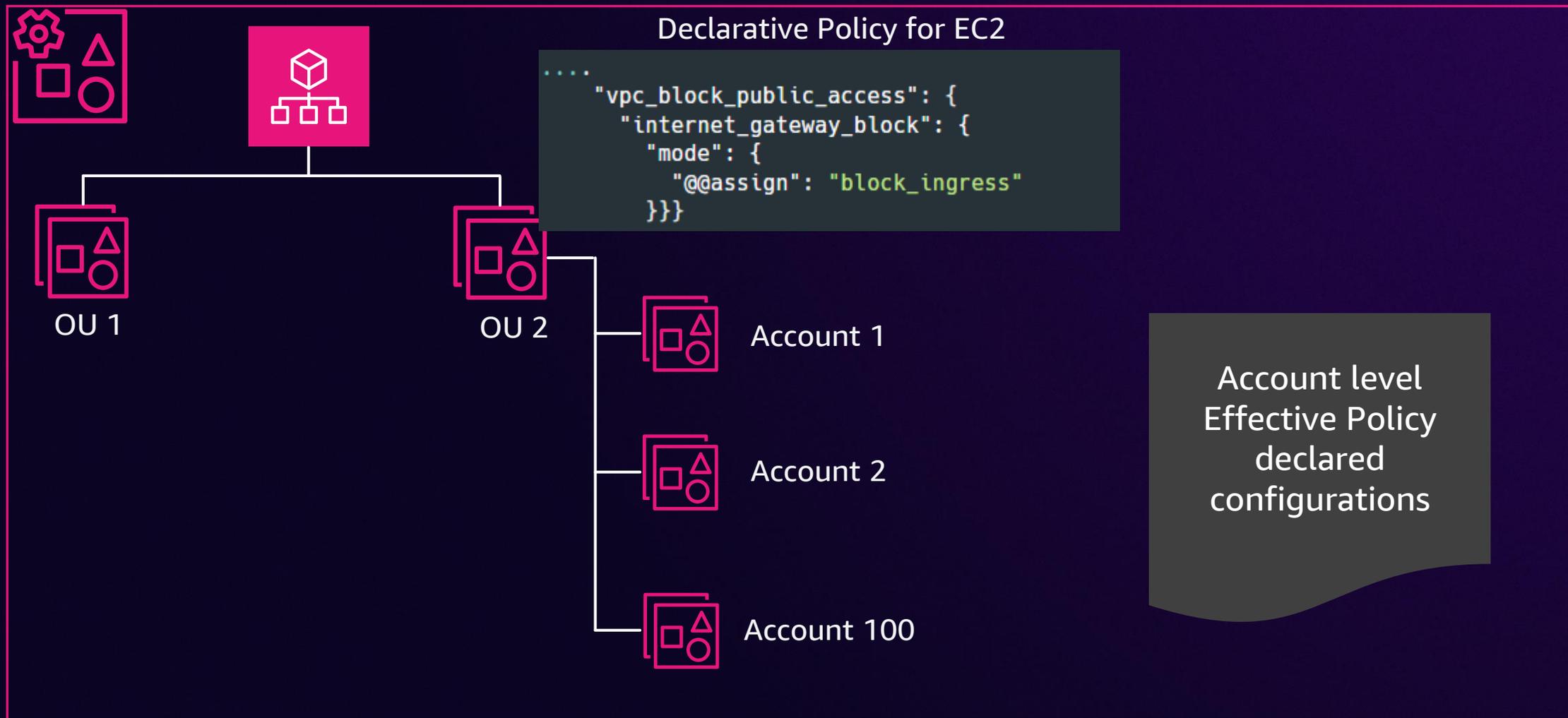
Block Public Access to VPC in accounts under DEV OU

Do not Block Public Access to VPC in accounts under Test OU

Declarative Policies - DEMO

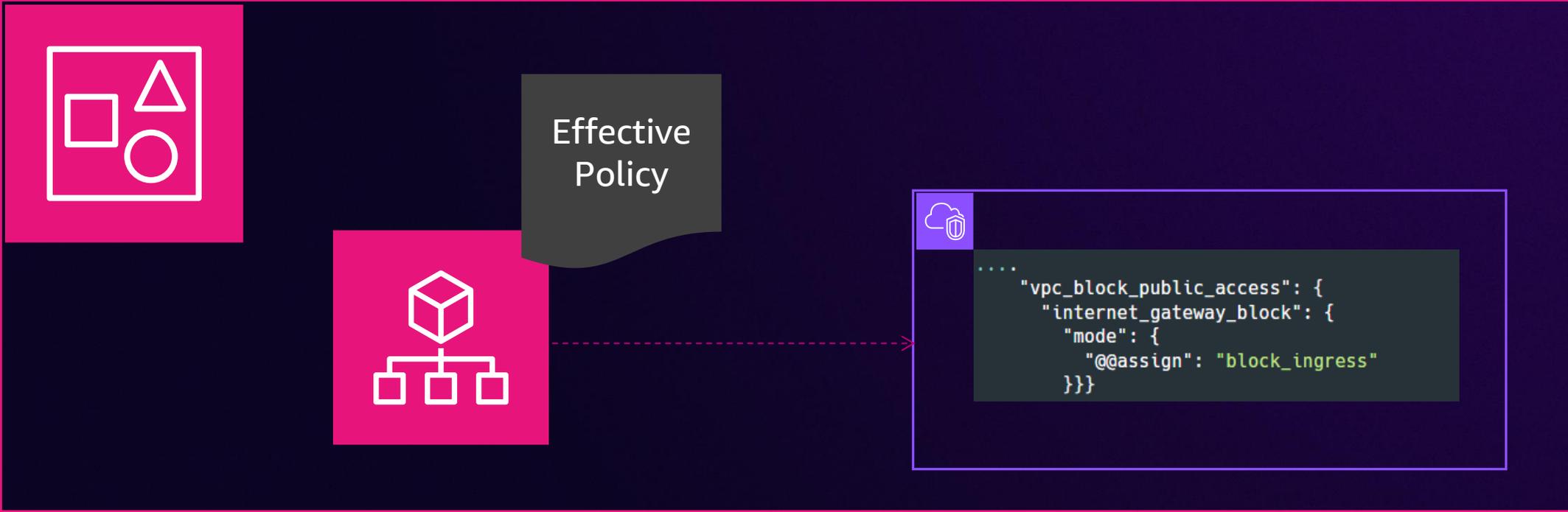
The screenshot shows the AWS Organizations console interface. At the top, a green banner displays the message: "Successfully deleted the policy named 'VPCBPADEMO'." Below this, the main content area is titled "AWS accounts" and includes an "Add an AWS account" button. A descriptive paragraph explains that the listed accounts are members of the organization and that the management account is responsible for billing. A search bar and view toggles for "Hierarchy" and "List" are present. The "Organizational structure" section shows a tree view with a "Root" unit containing two sub-units: "Dev" and "Test". Under "Dev", there is a member account "NavravMemAcc" (117270798863) joined on 2024/03/02. Under "Test", there is a member account "NavravTestMemAcc" (536697252114) created on 2024/11/30. At the bottom of the structure, the "NavravMgmtAcc" (148723167457) is identified as the "management account" and joined on 2024/03/02. The left sidebar shows navigation options like "Invitations", "Services", "Policies", and "Settings". The bottom of the image shows a Windows taskbar with the date 12/1/2024 and time 6:22 PM.

How does it work?



How does it work?

Account 1



When to use Declarative Policies?

Always use Declarative Policies when the configuration outcome is supported

Declarative Policies – why?

Declare and enforce desired configuration of a given AWS service in your AWS environment.



Set up is easy with a few simple clicks or commands

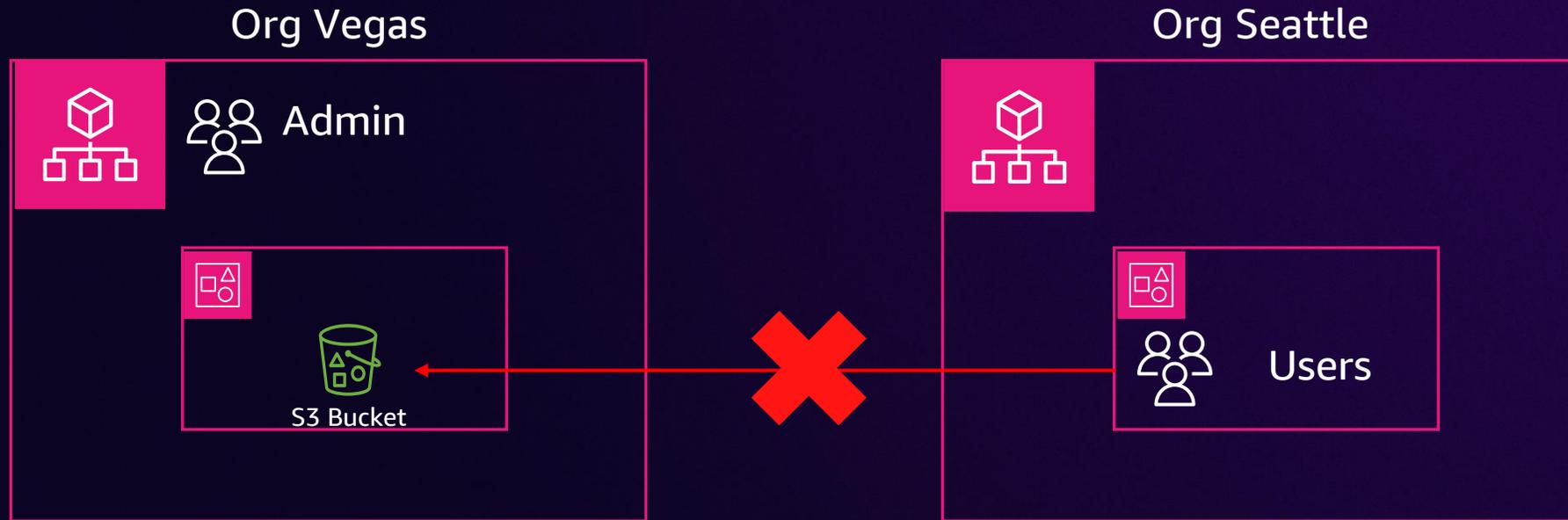


Set once and forget as it is always maintained and enforced regardless of authorization context



Transparent as it supports developer friendly custom error messages

Pop Quiz



Can you use a SCP in Org Vegas to block a user from Org Seattle to access a S3 bucket in Org Vegas?

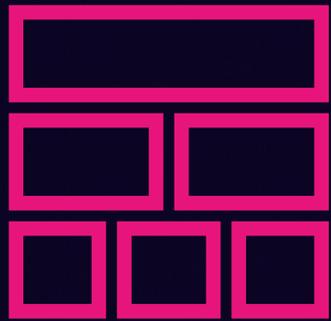
This is what you used to do!!

Use a Resource-based policy

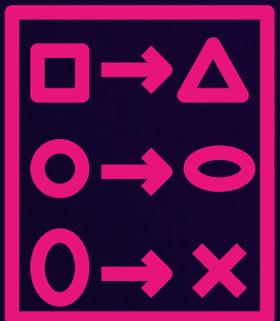
```
...
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": "*"
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgID": "<my-org-id>"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
...

```

Customer Challenges



No central mechanism



Continuously monitor



Pace of innovation

Resource Control Policies

Centrally define and enforce consistent access controls on resources at scale

Resource Control Policies - Benefits

Build a data perimeter around AWS resources at scale



Centrally define and enforce



Restrict access to your resources
with **preventive controls**



Empower your teams to
innovate faster while staying
secure

Interested in diving deeper on RCPs?

SEC337 Scaling IAM: Advanced administration and delegation patterns – Dec 4th & 5th

SEC 307 Data Perimeter Challenge – Builder session – Dec 5th

SCPs, RCPs, and Declarative Policies

	Service Control Policies	Resource Control Policies	Declarative Policies
Why?	Enforce consistent access controls on principals at scale	Enforce consistent access controls on resources at scale	Enforce default service configuration at scale

SCPs, RCPs, and Declarative Policies

	Service Control Policies	Resource Control Policies	Declarative Policies
Why?	Enforce consistent access controls on principals at scale	Enforce consistent access controls on resources at scale	Enforce default service configuration at scale
How?	By controlling permissions of principals at an API level	By controlling permissions for resources at an API level	By declaring the desired outcome (Not at an API level)

SCPs, RCPs, and Declarative Policies

	Service Control Policies	Resource Control Policies	Declarative Policies
Why?	Enforce consistent access controls on principals at scale	Enforce consistent access controls on resources at scale	Enforce default service configuration at scale
How?	By controlling permissions of principals at an API level	By controlling permissions for resources at an API level	By declaring the desired outcome (Not at an API level)
Implementation	IAM / Auth implementation	IAM / Auth implementation	Service control plane implementation
Feedback	Auth access denied	Auth access denied	Configurable error per policy
Example	Deny access to unapproved regions	Only trusted identities can access my resource	Configure Block Public Access for AMIs

SCPs, RCPs, and Declarative Policies

	Service Control Policies	Resource Control Policies	Declarative Policies
Why?	Enforce consistent access controls on principals at scale	Enforce consistent access controls on resources at scale	Enforce default service configuration at scale
How?	By controlling permissions of principals at an API level	By controlling permissions for resources at an API level	By declaring the desired outcome (Not at an API level)
Implementation	IAM / Auth implementation	IAM / Auth implementation	Service control plane implementation
Feedback	Auth access denied	Auth access denied	Configurable error per policy
Example	Deny access to unapproved regions	Only trusted identities can access my resource	Configure Block Public Access for AMIs

Observability and governance

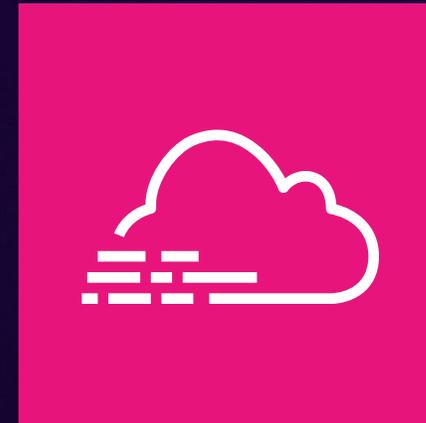


What is AWS CloudTrail?

Operational auditing

Risk auditing

Enable governance



AWS CloudTrail

Using CloudTrail in governance



Log API calls



Conduct audits



Monitor user activity



Detect suspicious behavior

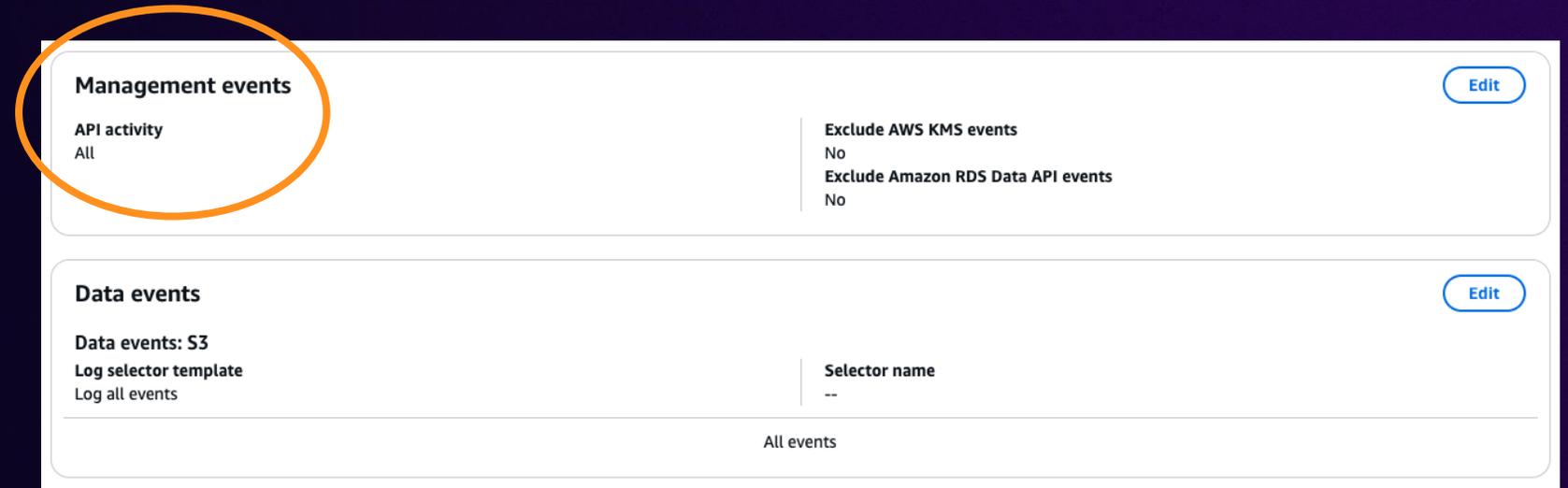


CloudTrail event types



Management Events in CloudTrail

Operations ON resources
"Control Plane Operations"
Default setting



The screenshot shows the AWS CloudTrail console settings for a trail. The "Management events" section is circled in orange. It includes an "API activity" dropdown set to "All", and two checkboxes: "Exclude AWS KMS events" (set to "No") and "Exclude Amazon RDS Data API events" (set to "No"). An "Edit" button is in the top right. The "Data events" section includes a "Data events: S3" dropdown, a "Log selector template" dropdown set to "Log all events", and a "Selector name" dropdown set to "--". An "Edit" button is in the top right. At the bottom, there is a link for "All events".



Create Amazon S3 bucket



Register devices



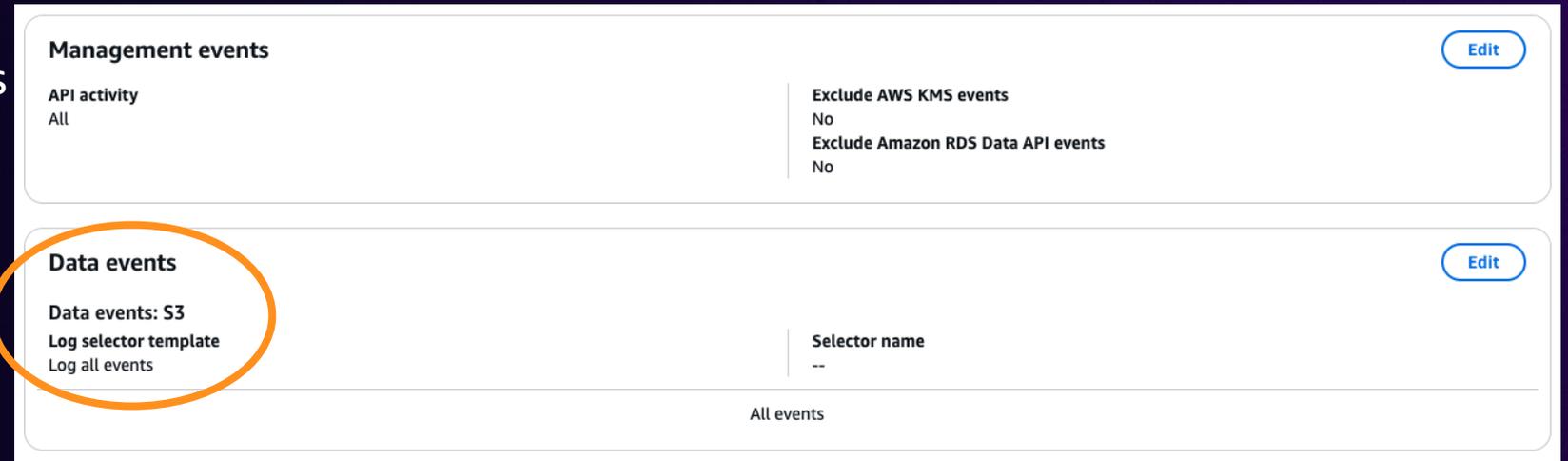
Configure rules

Data Events in CloudTrail

Data operations ON or IN resources

“Data plane operations”

Optional



The screenshot shows the AWS CloudTrail console with two event filter cards. The top card is for 'Management events' and the bottom card is for 'Data events'. The 'Data events' card is circled in orange. The 'Data events' card shows 'Data events: S3' and 'Log selector template: Log all events'. The 'Management events' card shows 'API activity: All' and 'Exclude AWS KMS events: No'.

Event Type	API activity	Exclude AWS KMS events	Exclude Amazon RDS Data API events	Selector name
Management events	All	No	No	--
Data events	Data events: S3			--



Amazon S3 object-level activity



Amazon SNS Operations



AWS Lambda function execution activity

Introducing Network Activity events in Cloud Trail

Network activity events
API calls traversing VPC endpoints
Optional

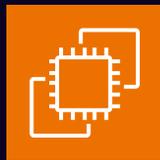
In Preview



AWS CloudTrail



AWS Secrets Manager



Amazon EC2



AWS Key Management Service (AWS KMS)

The screenshot displays the AWS CloudTrail console configuration for a trail. It is divided into four sections, each with an 'Edit' button:

- Management events:** API activity is set to 'All'. There are two toggle options: 'Exclude AWS KMS events' (set to 'No') and 'Exclude Amazon RDS Data API events' (set to 'No').
- Data events:** Data events are set to 'S3'. The log selector template is 'Log all events'. The selector name is '--'. The events are listed as 'All events'.
- Insights events:** API call rate is set to 'Enabled'. The events are listed as 'All events'.
- Network activity events:** This section is circled in orange. Network activity events are set to 'ec2.amazonaws.com'. The log selector template is 'Log all events'. The selector name is '--'. The events are listed as 'All events'.

What is a VPC endpoint?



Amazon Virtual Private
Cloud (Amazon VPC)



Endpoints

Connect to AWS Services

Connect to VPC endpoint services

Within AWS network

No internet



VPC endpoint policies

Resource based

Principals access

Cannot override other policies

Not all services

Default policy: Full access

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```



VPC endpoint policy in place

Only trusted principals
can make requests from
VPCs that I own

```
{  
  "Sid": "AllowRequestsByOrgsIdentitiesToOrgsResources",  
  "Effect": "Allow",  
  "Principal": "*",  
  "Action": "*",  
  "Resource": "*",  
  "Condition": {  
    "StringEquals": {  
      "aws:PrincipalOrgID": "<my-org-id>",  
      "aws:ResourceOrgID": "<my-org-id>"  
    }  
  }  
},
```

Full policy



Use VPC network activity events to improve VPC endpoint policies

Logging set up for all management and network activity events for multiple event sources

Security team finds valid requests that are denied by policy

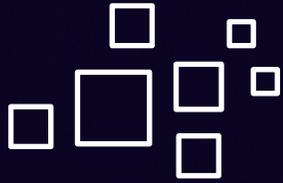
Policy updated to allow certain exceptions

```
aws cloudtrail put-event-selectors \  
--region region \  
--trail-name TrailName \  
--advanced-event-selectors '[  
  {  
    "Name": "Log all management events",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["Management"]  
      }  
    ]  
  },  
  {  
    "Name": "Log all network activity events for CloudTrail APIs",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["NetworkActivity"]  
      },  
      {  
        "Field": "eventSource",  
        "Equals": ["cloudtrail.amazonaws.com"]  
      }  
    ]  
  }  
'
```

Final thoughts

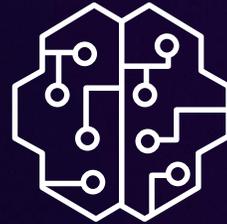


Summary of the three launches



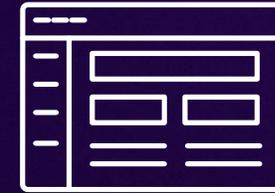
Declarative Policies

Declare and enforce desired configuration for a given AWS service at scale across your organization



Resource Control Policies

Centrally define and enforce consistent access controls on resources at scale



Network Activity Events

Use CloudTrail to have visibility of events within VPC endpoints

Related breakout sessions

- COP383 – Achieving governance at scale
- COP327 – Accelerating auditing and compliance for generative AI on AWS
- COP402 – Dive deep on AWS Cloud Governance
- COP335 – Unlock powerful insights with your logs
- COP338 – Architecting AWS accounts for scale
- COP343 – Best practices for cloud governance
- COP 342 – Top controls for a secure, well-architected environment

Try AWS Organizations & AWS Control Tower



Getting started with
AWS Organizations



Getting started with
AWS Control Tower

Try these new features



Declarative
Policies



Resource
Control Policies



Network Activity
Events in
CloudTrail

Thank you!

Tim Honychurch

timhon@amazon.com



[LinkedIn](#)

Naveen Ravisanker

navrav@amazon.com



[LinkedIn](#)



Please complete the session survey in the mobile app

