
AWS
re:Invent

SEC308

AWS Identity: Next-generation permission management

Brigid Johnson

Senior Manager, AWS Identity

AWS

AWS re:Invent

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

Agenda

Permission management model

Review permission tools

Start with permission guardrails

Embark on least privilege journey with access analysis

Use attributes for fine-grained permission

Recap

Demo!

Demo!



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

Permission management model



AWS re:Invent

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

Access control journey

Where you begin

Business to innovate

Agility to move fast

Give builders freedom



Where you are going

Prevent dangerous actions

Ensure security posture

Achieve least privilege

Let’s go!

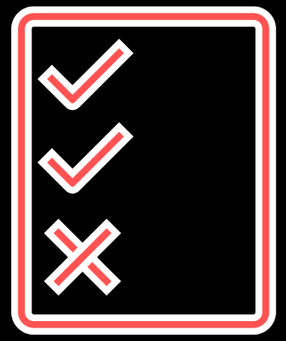
Who has access to what

Who



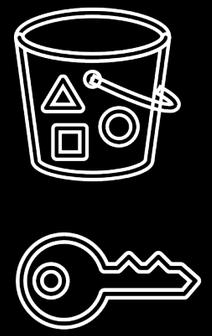
Developers and applications

Can access



Permissions

What



Resources

Permissions model in AWS



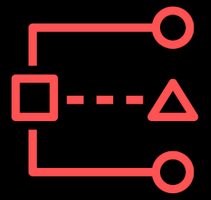
Separate workloads using multiple accounts



Federation using Identity and Access Management (IAM) roles



Prevent Access using permission guardrails



Review and Refine Permissions using access analysis



Fine-grained permissions using attribute-based access control (ABAC)

Review permissions tools in AWS



AWS re:Invent

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

Access management toolbox



Permission guardrails

AWS Organizations service control policies (SCPs)

Permission guardrails to restrict access for principals across account in your organization

IAM permission boundaries

Enable developers to manage permissions and control the maximum permissions they grant

Virtual Private Cloud (VPC) endpoint policies

Require that traffic stays within your VPC

Block public access

Block existing public access and ensure that public access is not granted to newly created items

Access management toolbox



Granting access

IAM principal policies

Attach policies to IAM identities (users, groups, or roles)

- Managed policies are standalone and attached to multiple principals
- Inline policies are attached directly to a single principal

Resource policies

Attach policies to resources to grant principals access cross-account or within the account



IAM Roles



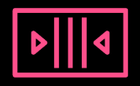
S3 Buckets



Lambda Functions



KMS Keys



SQS Queues

Policy types: How they work together

All access requests start with DENY

If using SCPs → SCP must allow

If using permission boundaries → Permission boundary must allow

---

If same account access → Identity **or** resource policy must allow

If direct cross-account access → Both the identity **and** resource policy must allow

If using session policy → Session and identity policy must allow

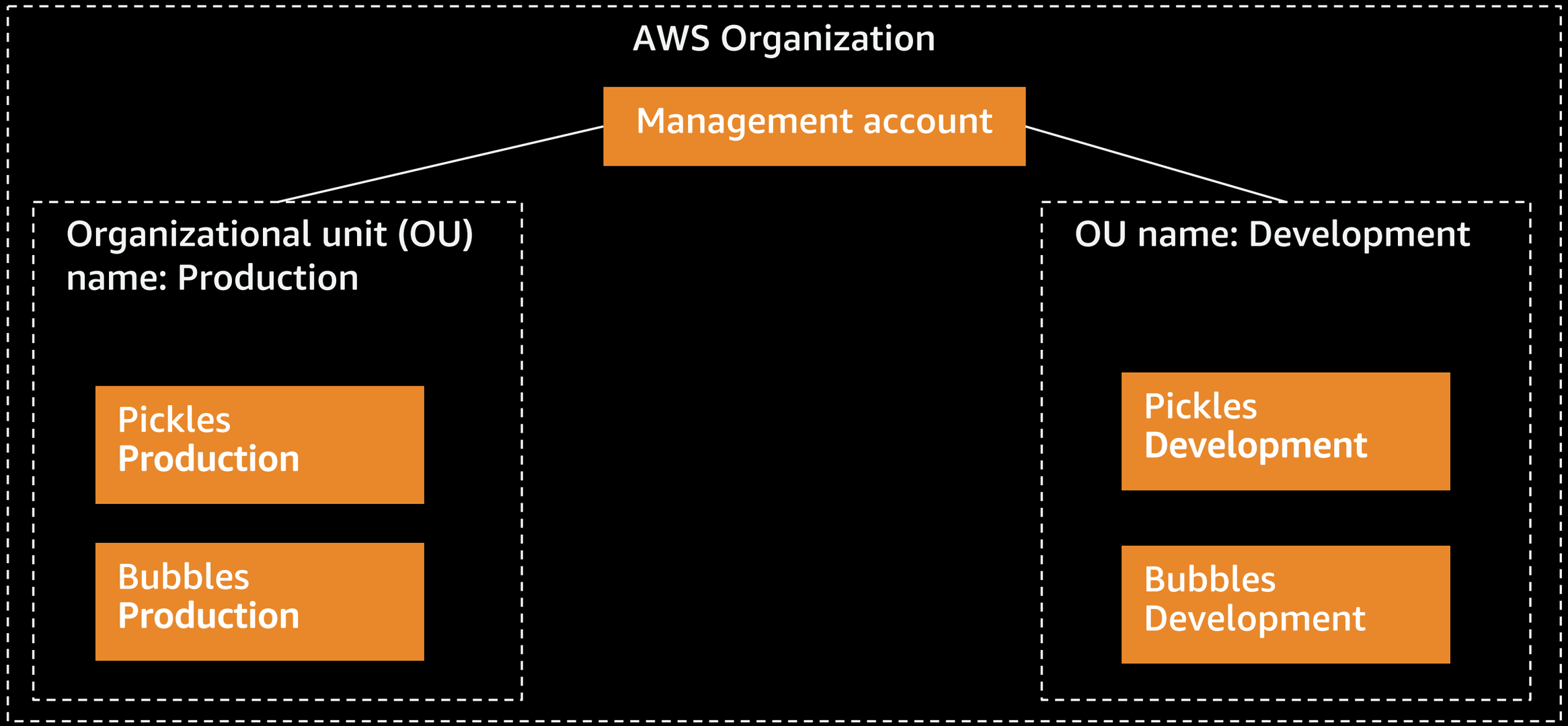
Start with permission guardrails



AWS re:Invent

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

Govern accounts with AWS Organizations



Use SCPs

Establish controls that all IAM principals (users and roles) adhere to across an account, organizational unit, or organization

What you can do

- Restrict access to specific AWS Regions
- Prevent your IAM principals from deleting common resources
- Restrict service actions for all IAM entities except a specific role

Demo: SCPs



AWS re:Invent

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

Demo details: SCPs

Restrict powerful service actions for all IAM entities except a specific role

1. Create SCP in management account

2. Attach SCP to root account of organization

3. Demonstrate access in development OU

Policy to restrict powerful actions



Pro tip: Use AWS PrincipalArn condition key

```
"Effect": "Deny",
"Action": [ "ec2:AssociateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DetachInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:DeleteInternetGateway“ ],
"Resource": "*",
"Condition": {
        "StringNotLike": {
                "aws:PrincipalARN": "arn:aws:iam::*:role/network-admin*“ }       }
```

Deny these actions,
unless you are this role

www.BANDICAM.com

Isengard | AWS Organizations | New Tab

https://console.aws.amazon.com/organizations/home?region=us-west-2#/accounts

Search

Most Visited | Getting Started | Team Building Questi... | Intel Ticket | CM | Competencies (Users.... | Marketing - All Docu... | Hazel (AWS.Auth.IAMI... | Building dashboards f... | AWS re:Invent 2020 | Xinyu's - Action Items ... | SDEIII_Evaluations (Us...

brigidj+2018master@amazon.com - 332207979596 / admin-reInvent-2018-master (Not Production Account)

Ise | AWS Change Control Advisory

aws | Services | admin-reInvent-2018-master/brigidj-Isengard @ 3322-0797-9596 | Global | Support

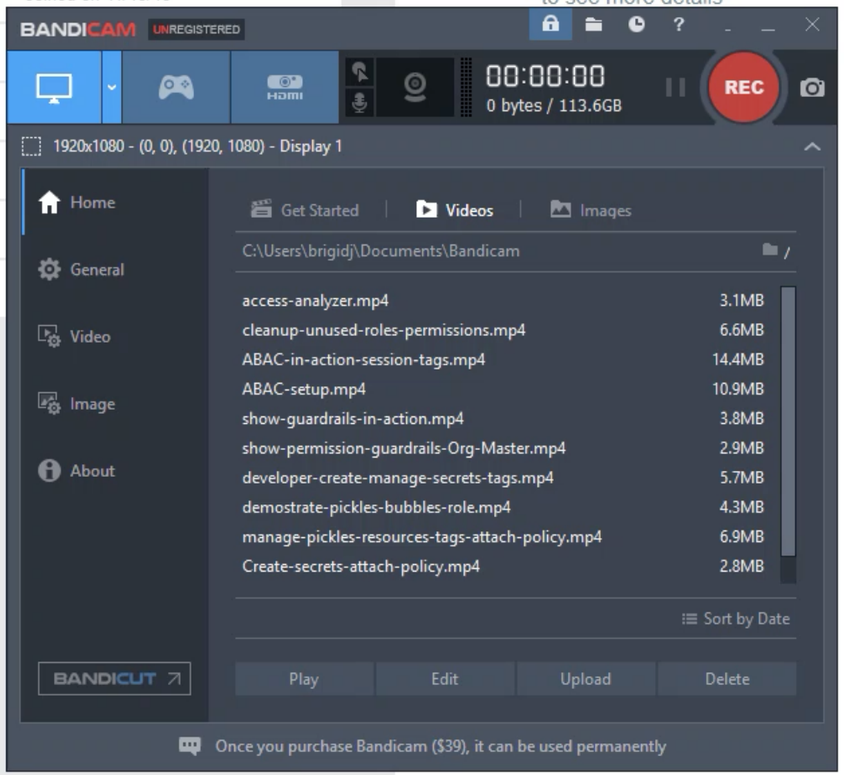
AWS Organizations

Accounts | Organize accounts | Policies | Invitations | Settings

Add account | Remove account | Hide | Failed account creation requests | Filter

		Account name	Email	Account ID	Status
☐	★	aws-reinvent-2018-master	brigidj+2018master@amazon.com	332207979596	Joined on 11/18/18
☐		aws-reinvent-2018-unicorns-prod	brigidj+2018-unicorns-prod@amazo...	730707046050	
☐		dashboardTest	brigidj+dashboardTest@amazon.com	710979372212	
☐		aws-reinvent-2018-zombies-dev	brigidj+2018-zombies-dev@amazon...	432807222178	
☐		aws-reinvent-2018-unicorns-dev	brigidj+2018-unicorns-dev@amazon...	128609111811	
☐		aws-reinvent-2018-zombies-prod	brigidj+2018-zombies-prod@amazo...	125899824188	

Please select an account to see more details



© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

8:39 AM
11/3/2020

Set permission boundaries

Enable developers to create and manage IAM roles
but control the maximum permissions they can grant

What you can do

- Enable developer to create roles without escalating their access
- Require developers to create roles with a boundary

To learn more

Become an IAM Policy Master in 60 Minutes or Less
https://www.youtube.com/watch?v=YQsK4MtsELU

Embark on least privilege journey



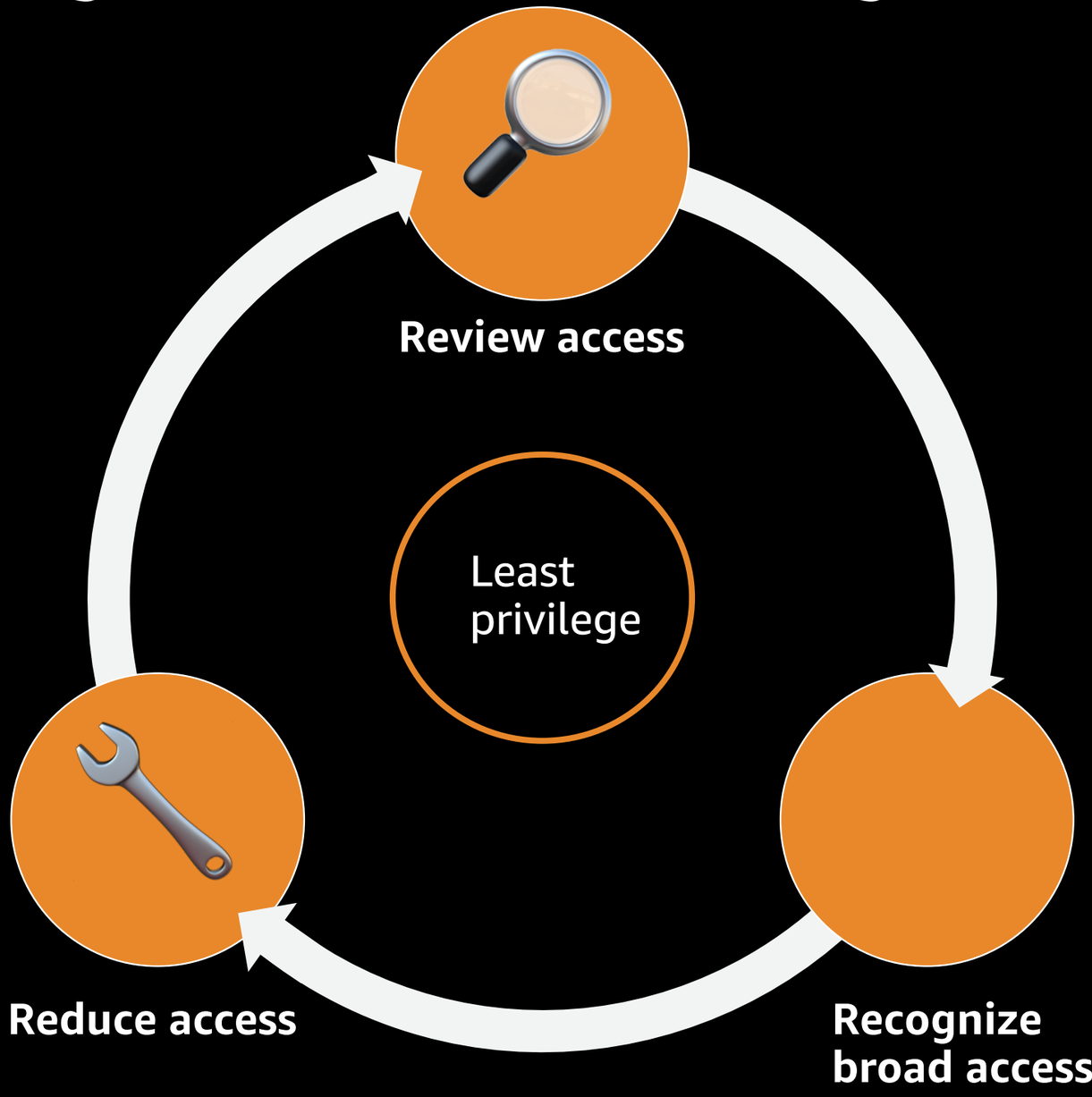
AWS re:Invent

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

Least privilege journey with access analysis



- IAM Access Analyzer
- Service and action last accessed
- Role and access key last used



Use access analysis to reduce broad access



AWS re:Invent

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

Who can access my resources cross-account?

Production account for Project Pickles



Pickles data processing account

Access not intended!

Account to an unapproved third-party partner

Central security account within the organization

Access not intended!

Developer account

IAM Access Analyzer

Analyze access continuously

Identify resources with

- Public
- Cross-account
- Cross-organization access



Comprehensive findings

Uses automated reasoning to determine all access paths and provide with highest levels of security assurance

Recognize broad access

Review findings to identify and remediate unintended access

Demo: Recognize broad access with IAM Access Analyzer



AWS re:Invent

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

Demo details: Analyze broad access

1. Enable IAM Access Analyzer
2. Review my findings for external access
3. Remediate access to bucket and resolve a finding
4. Mark access to a bucket as intended and archive finding



www.BANDICAM.com

Isengard | IAM Management Console

https://us-west-2.console.aws.amazon.com/access-analyzer/home?region=us-west-2#/findings

Most Visited | Getting Started | Team Building Questi... | Intel Ticket | CM | Competencies (Users.... | Marketing - All Docu... | Hazel (AWS.Auth.IAMI... | Building dashboards f... | AWS re:Invent 2020 | Xinyu's - Action Items ... | SDEIII_Evaluations (Us...

brigidj+2018-zombies-dev@amazon.com - 432807222178 / aws-reinvent-2018-zombies-dev (Not Production Account) | AWS Change Control Advisory

aws | Services | aws-reinvent-2018-zombies-dev/brigidj-Isengard @ 4328-0722-2178 | Oregon | Support

Identity and Access Management (IAM)

- Dashboard
- Access management
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCP)

AWS account ID: 432807222178

New: Access Analyser now supports archive rules for existing findings
Archive rules automatically archive new findings that meet the criteria you define. Now, you can apply the rules retroactively to mark existing findings as intended. This lets you focus on remediating findings that help you reduce broad access.

Create an archive rule

IAM > Access Analyzer

Access Analyzer Info

Last scan: 10 hours ago

Analyzer

ConsoleAnalyzer-14e68572-1a5a-4b23-97c4-c5d52c512c6c
Zone of trust: Current account (432807222178)

Active | Archived | Resolved | All

Active findings

Account ID 432807222178

Filter active findings

Finding ID	Resource	External principal	Condition	Shared t
5174af6f-c466-4a6a-a03...	S3 Bucket pickles-application-acc	AWS Account 128609111811	-	Bucket po
16fe1868-dd06-4f21-b2e...	S3 Bucket pickles-application-acc	AWS Account 028103658970	-	Bucket po
d84991f3-0420-4c9a-ab5...	IAM Role acc-developer-abac	Federated User arn:aws:iam::432807222178:saml-provi...	-	-
d487dd8f-4a44-479d-a0d...	S3 Bucket pickles-vpc-only	All Principals	Source VPC vpc-d7de09af	Bucket po

BANDICAM UNREGISTERED
00:00:00
0 bytes / 113.6GB
REC
1920x1080 - (0, 0), (1920, 1080) - Display 1
Home | General | Video | Image | About
Get Started | Videos | Images
C:\Users\brigidj\Documents\Bandicam
DemoVideo-1-SCP.mp4 3.7MB
access-analyzer.mp4 3.1MB
cleanup-unused-roles-permissions.mp4 6.6MB
ABAC-in-action-session-tags.mp4 14.4MB
ABAC-setup.mp4 10.9MB
show-guardrails-in-action.mp4 3.8MB
show-permission-guardrails-Org-Master.mp4 2.9MB
developer-create-manage-secrets-tags.mp4 5.7MB
demostrate-pickles-bubbles-role.mp4 4.3MB
manage-pickles-resources-tags-attach-policy.mp4 6.9MB
Sort by Date
BANDICUT
Play | Edit | Upload | Delete
Once you purchase Bandicam ($39), it can be used permanently

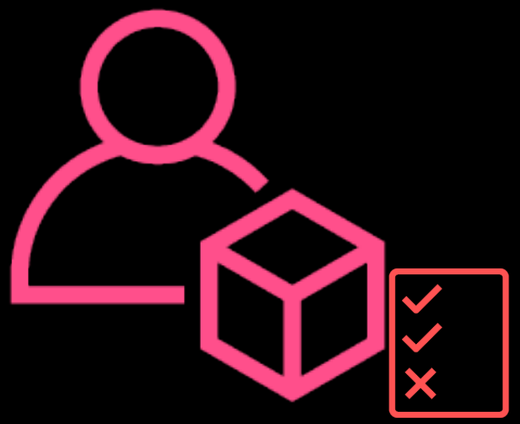
Feedback | English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

8:52 AM
11/3/2020

How can I reduce access?

1



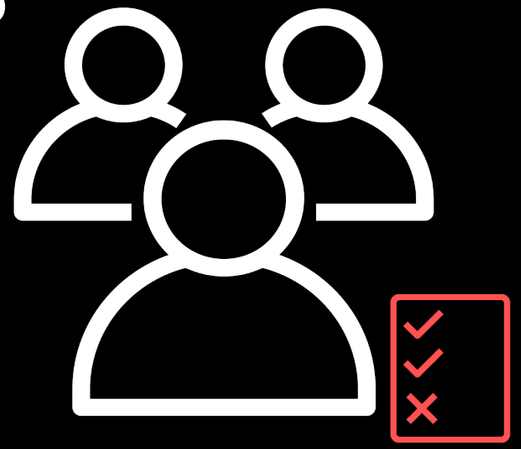
Remove unused permissions from SCPs

2



Remove unused principals, services, and actions in IAM

3



Remove unused Amazon Simple Storage Service (S3) actions from IAM policies

Service and action last accessed information

Review unused permissions with last accessed information

IAM does the heavy lifting and summarizes last access information for roles and users

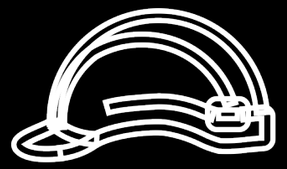
Remove unused permissions with confidence

Review last accessed information and identify permissions to remove



📣 Pro tip: Channel your inner Marie Kondo

Who did access what?



S3 GetBucketVersioning **1 day ago**

S3 GetBucketLocation **1 day ago**

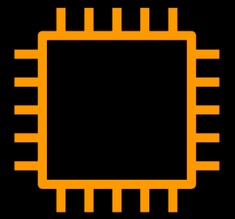
S3 ListAllMyBuckets **110 days ago**

Amazon Elastic Compute Cloud (EC2) **3 days ago**

AWS Elastic Load Balancing **3 days ago**

AWS Cognito **180 days ago**







Demo: Reduce access using last accessed information



AWS re:Invent

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

Demo details: Reduce access

1. Review role last used information
2. Remove roles not used in last 90 days
3. Review application role S3 permissions
4. Remove unused S3 permissions

www.BANDICAM.com

Isengard | IAM Management Console

https://console.aws.amazon.com/iam/home?region=us-west-2#/home

Search

Most Visited | Getting Started | Team Building Questi... | Intel Ticket | CM | Competencies (Users.... | Marketing - All Docu... | Hazel (AWS.Auth.IAMI... | Building dashboards f... | AWS re:Invent 2020 | Xinyu's - Action Items ... | SDEIII_Evaluations (Us...

brigidj+2018-zombies-dev@amazon.com - 432807222178 / aws-reinvent-2018-zombies-dev (Not Production Account)

AWS Change Control Advisory

aws | Services | aws-reinvent-2018-zombies-dev/brigidj-Isengard @ 4328-0722-2178 | Global | Support

Identity and Access Management (IAM)

- Dashboard
- Access management
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
    - Archive rules
    - Analyzers
    - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCPs)

Search IAM

AWS account ID:
432807222178

IAM dashboard

Sign-in URL for IAM users in this account

https://432807222178.signin.aws.amazon.com/console | Customize

IAM resources

Users: 1
Roles: 52
Groups: 1
Identity providers: 1
Customer managed policies: 31

Security alerts

⚠ The root user for this account does not have Multi-factor authentication (MFA) enabled. Enable MFA to improve security for this account.

Best practices

- Grant least privilege access: Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set o functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Enable Identity federation: Centrally manage users and access across multiple applications and services. For federation to multiple accounts in you AWS Organization, you can configure your identity source in AWS Single Sign-on.
- Enable MFA: For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly: Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer: Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.

Learn more about all security best practices.

What's new

Learn about the latest releases for AWS Identity & Access Management (IAM)

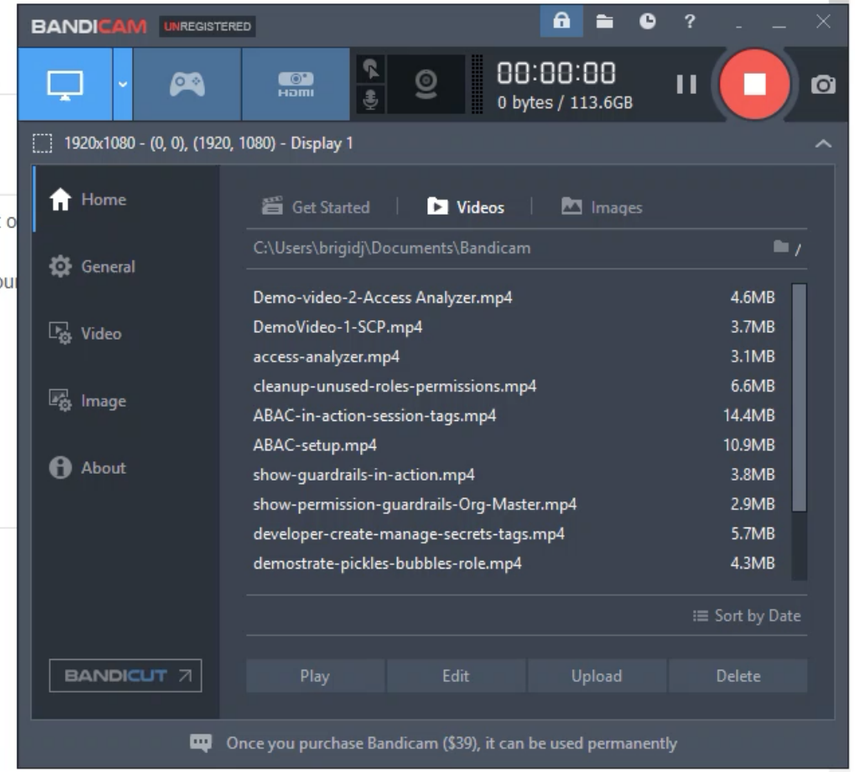
- AWS IAM Access Analyzer now supports archive rules for existing findings
  19 days ago (10/15/2020)
- Amazon Detective introduces IAM Role Session Analysis
  1 month, 2 weeks ago (9/17/2020)
- Now gain longer access to your AWS resources when switching roles in the AWS Management Console
  3 months ago (7/24/2020)
- Manage your AWS Identity and Access Management quotas with AWS Service Quotas
  4 months ago (6/25/2020)

Additional information

IAM documentation
Videos, IAM release history and additional resources

Tools

Web identity federation playground
Policy simulator



Feedback | English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

12:22 PM
11/3/2020

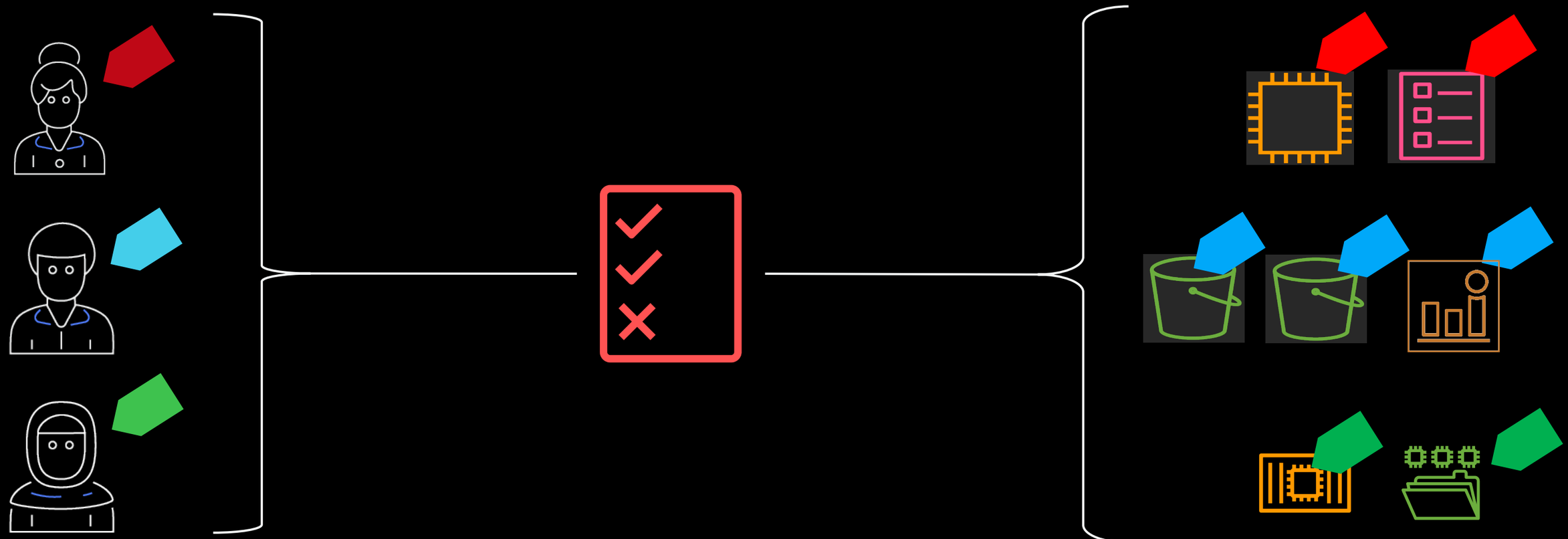
Use attributes for fine-grained permissions



AWS re:Invent

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

Fine-grained permissions using attributes



Workforce users

Permissions

Resources

Benefits of ABAC

Permissions scale with innovation as permissions automatically apply

Easily understand permissions by matching attributes

Granular permissions without a permission update for every item

Audit attributes to determine access



Key takeaways

- Start with permission guardrails
- Use access analysis to reduce broad access
- Leverage attributes for fine-grained permission



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

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.