
AWS
re:Invent

SEC312

AWS identity: Ten identity health checks to improve security in the cloud

Cassia Martin

Senior Security Solutions Architect

AWS

AWS re:Invent

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



Ten places your security group should spend time

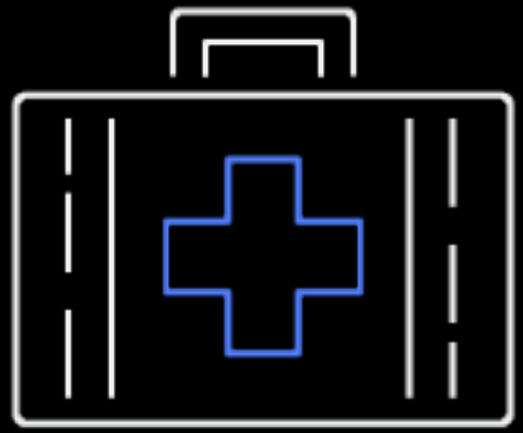
1. Accurate account info
2. Use MFA
3. No hard-coding secrets
4. Limit security groups
5. Intentional data policies
6. Centralize AWS CloudTrail logs
7. Validate IAM roles
8. Take action on GuardDuty findings
9. Rotate your keys
10. **Being involved in dev cycle**

AWS re:Invent

Source: Schmidt, “Leadership session: AWS security,” 2019. https://youtu.be/oam8FDNJhbE?t=624

Identity health checks





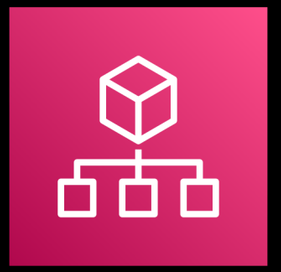
Identity health checks

1. Use multiple AWS accounts
2. Create intentional OU structure
3. Use SCPs
4. Secure root
5. Federate identity for human users
6. Use roles
7. Validate trust role policies
8. Continuously review your policies
9. Audit IAM for unused principals
10. Monitor your resource access

1. Use multiple AWS accounts

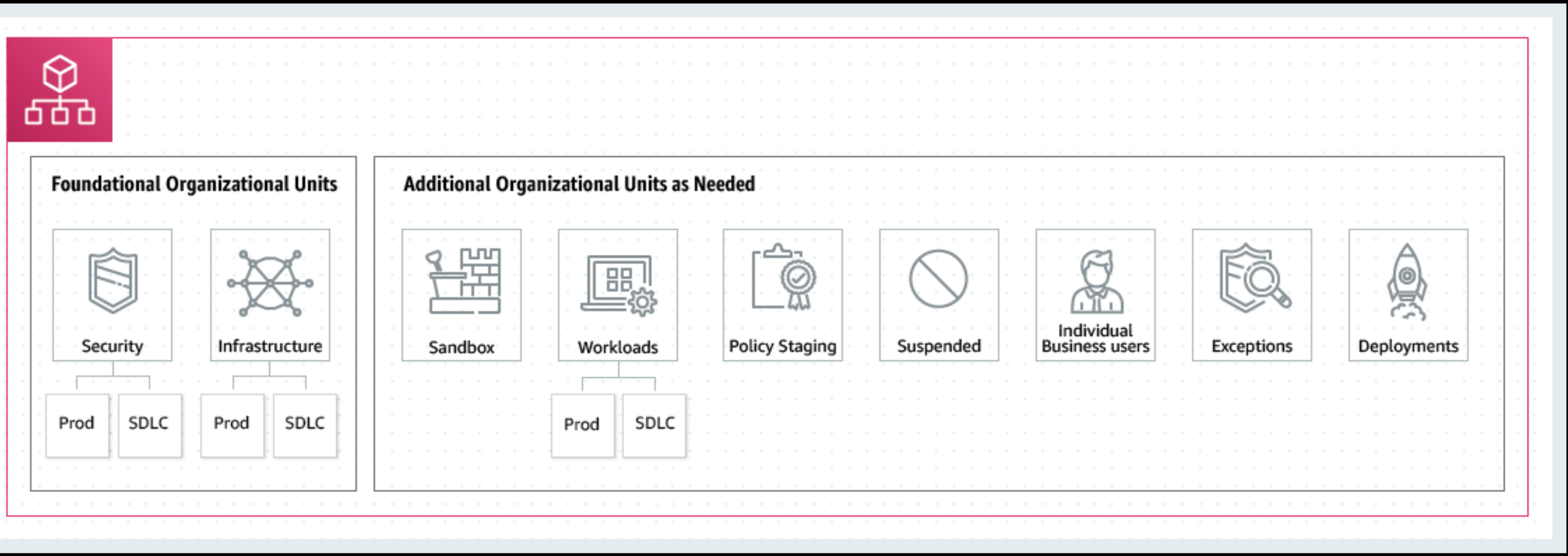


- Multiple accounts
- Isolation



- AWS Organizations
- All features

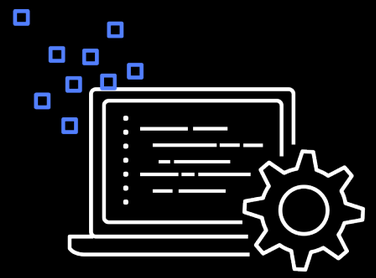
2. Create intentional OU structure



3. Use service control policies (SCPs)

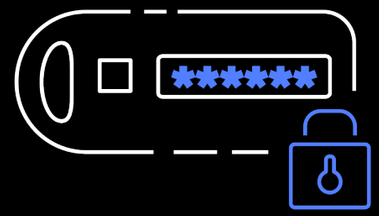
- Restrict regions
- Restrict services
- Restrict principals
- Require Amazon S3 encryption
- Deny organizations:* on root
- Limit allowed Amazon EC2 types
- Require MFA for EC2 stop
- Block root access to EC2
- Block disabling AWS CloudTrail
- Block disabling Amazon CloudWatch
- Block VPC Flow Logs deletion
- Lock in AWS Config rules
- Require a tag for making resources
- Limit VPC internet access changes

4. Secure root



Don’t use root

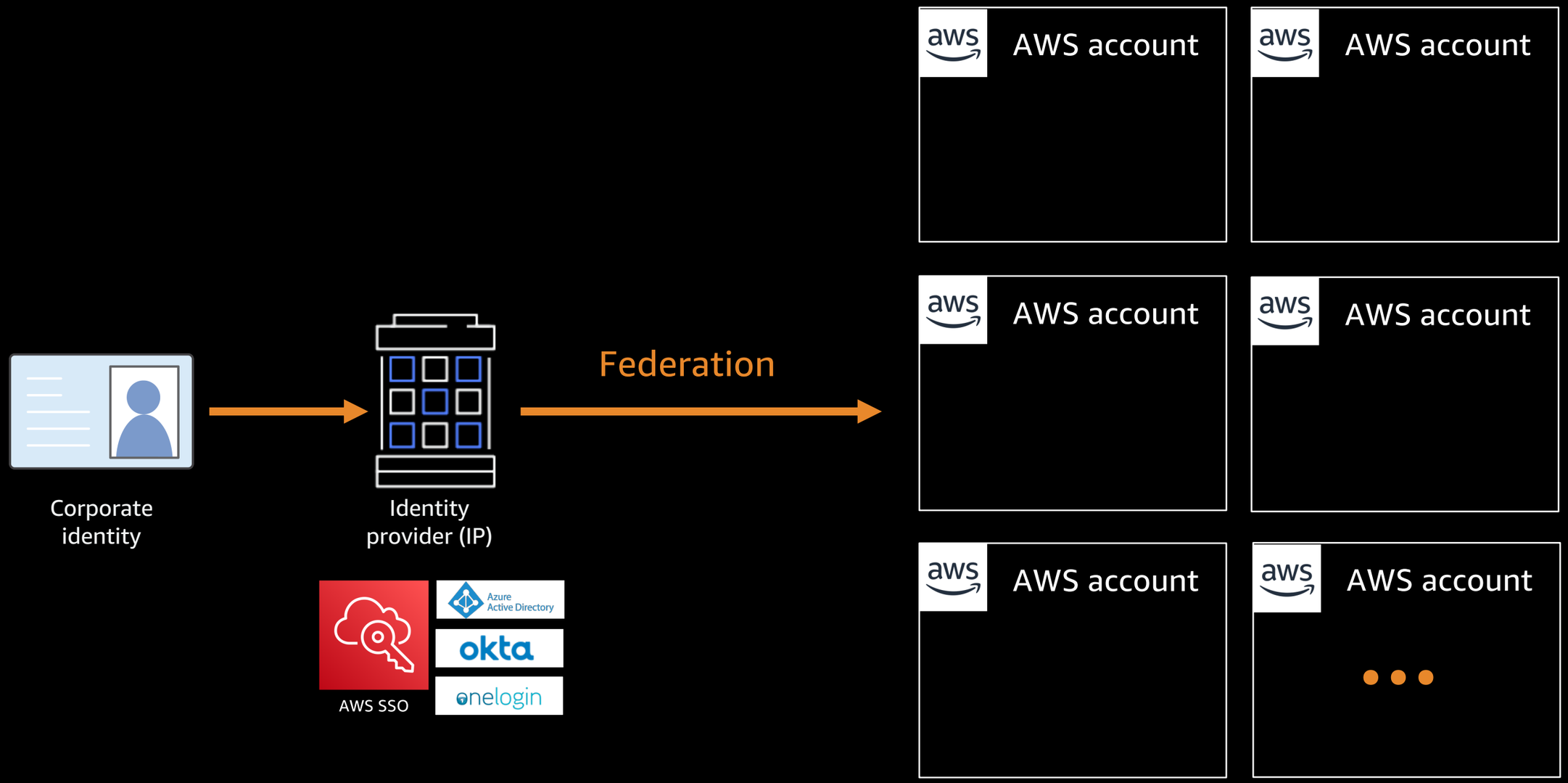
- Delete access keys
- Use SCP to restrict root actions
- Monitor and notify on root login



Secure root

- Enable MFA – store in safe
- Strong, random password
- Split control
- Set root email to a distribution list

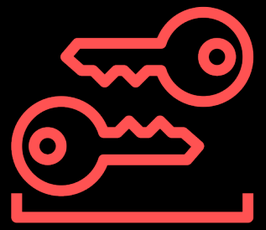
5. Federate identity for human users



6. Use roles



Assumed by human or machine users



Grants temporary, limited-privilege credentials



Permissions attached to the IAM role

7. Validate trust role policies

DOS



- Grant least privilege
  - Review principals for role access
- Simplify
  - Limit roles to one level of role assumption
- Segregate roles' purposes
  - Make different roles for humans vs. machines

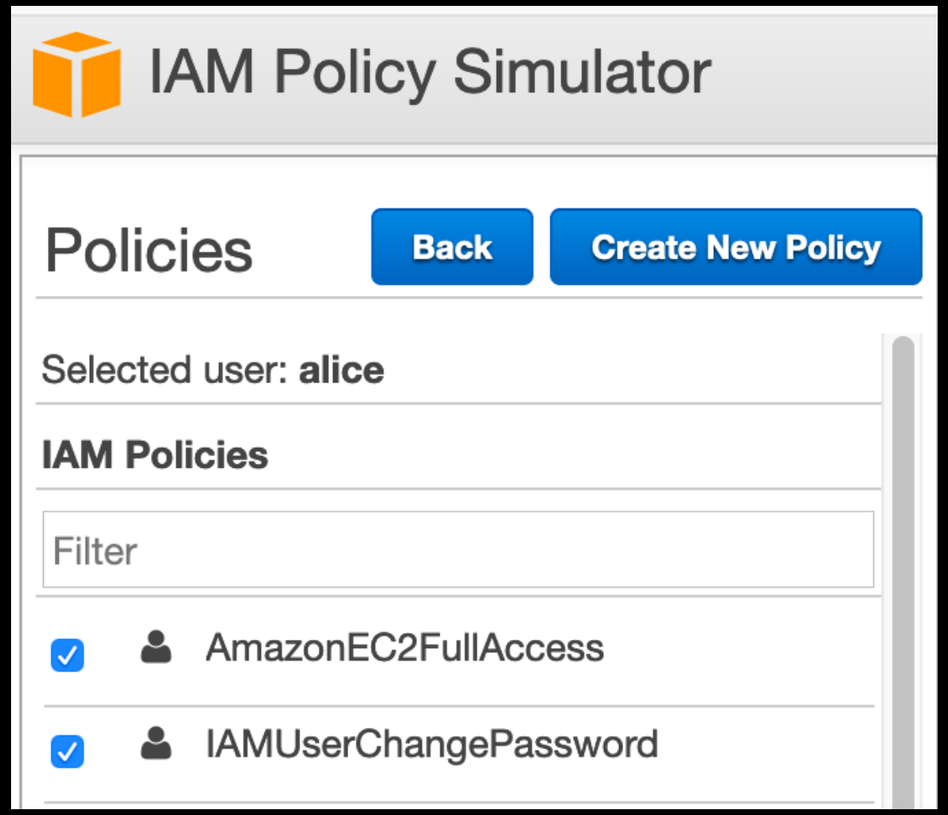
DON'TS



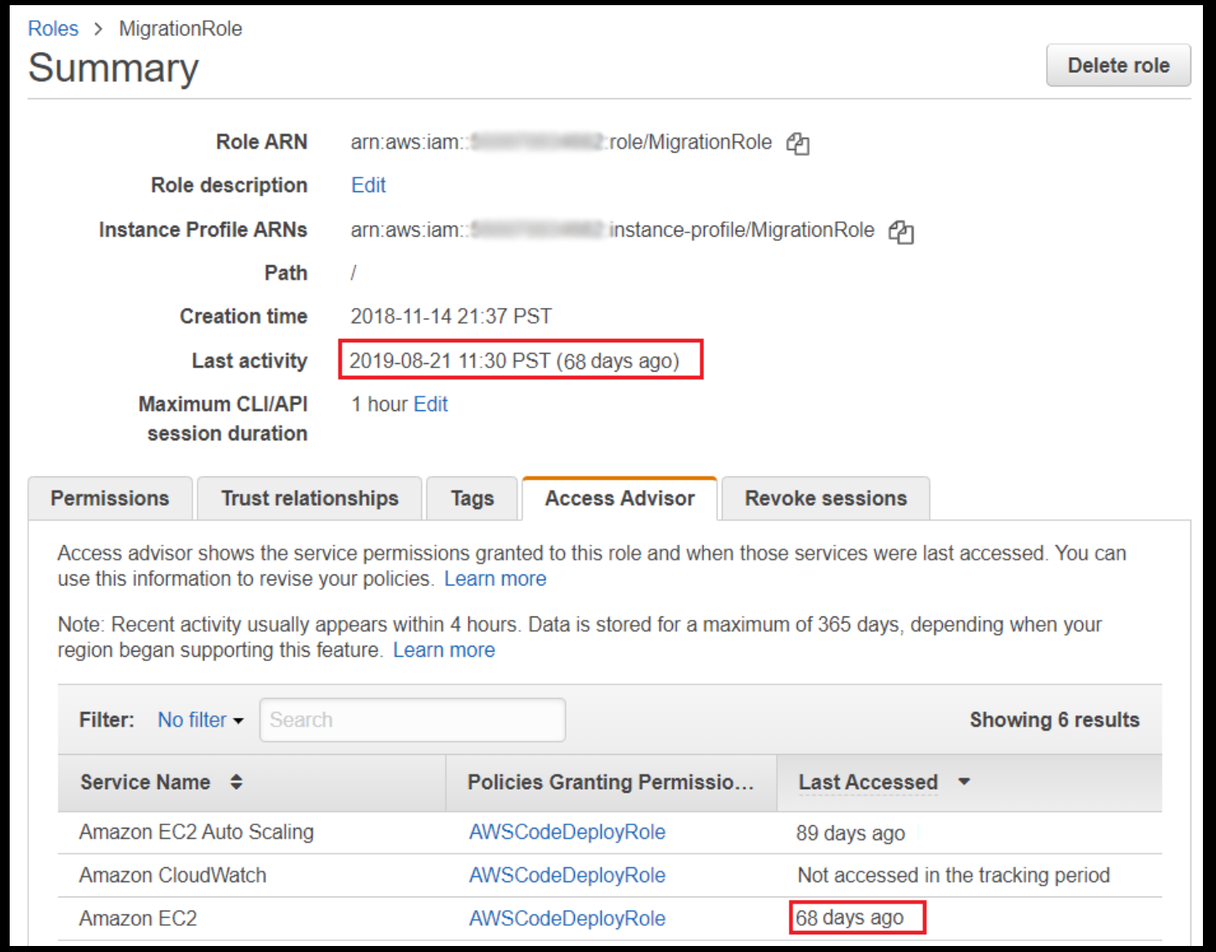
- Grant broad access
  - sts:assumerole:*
- Use role chaining
  - Role hierarchies complicate attribution
  - e.g., role A → allowed to assume role B
- Overload roles
  - Don't let two applications use the same role

8. Continuously review your policies

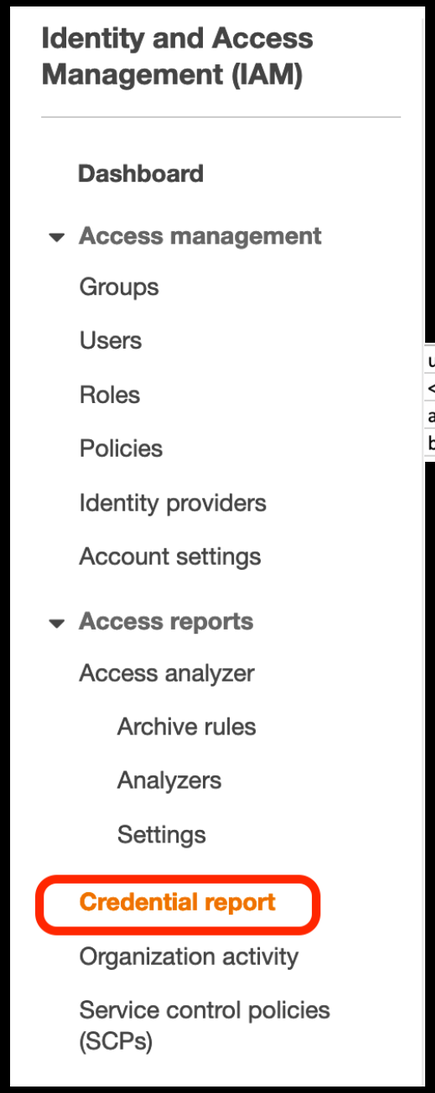
IAM Policy Simulator



Access advisor



9. Audit IAM for unused principals



Use IAM credential report

user	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date
<root_account>	2018-10-08T16:52:10+00:00	not_supported	2018-10-08T17:05:50+00:00	not_supported	not_supported	TRUE	FALSE	N/A	N/A
alice	2019-08-12T18:05:34+00:00	TRUE	2020-07-09T19:21:56+00:00	2020-07-10T00:07:20+00:00	N/A	FALSE	TRUE	2019-12-05T19:05:03+00:00	2019-12-05T19:09:00+00:00
bob	2020-06-29T15:18:03+00:00	TRUE	no_information	2020-06-29T15:18:04+00:00	N/A	FALSE	TRUE	2020-06-29T15:18:04+00:00	N/A

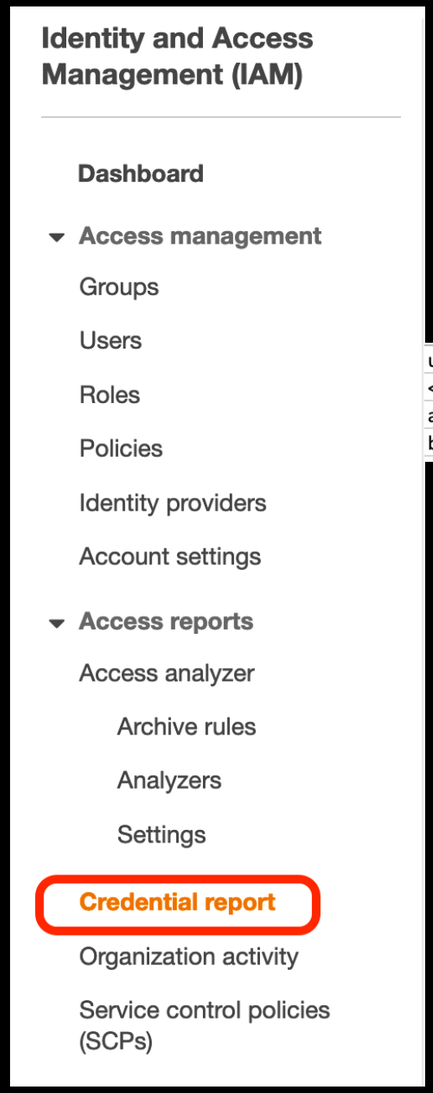
Password-enabled?

When was it last used?

When was it last rotated?

9. Audit IAM for unused principals

Use IAM credential report

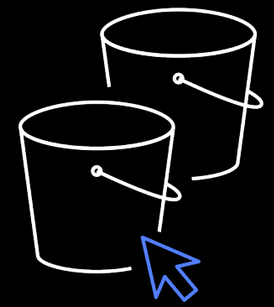


user	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_activ	access_key_1_last_rotated	access_key_1_last_used_date
<root_account>	2018-10-08T16:52:10+00:00	not_supported	2018-10-08T17:05:50+00:00	not_supported	not_supported	TRUE	FALSE	N/A	/A
alice	2019-08-12T18:05:34+00:00	TRUE	2020-07-09T19:21:56+00:00	2020-07-10T00:07:20+00:00	N/A	FALSE	TRUE	2019-12-05T19:05:03+00:0	019-12-05T19:09:00+00:00
bob	2020-06-29T15:18:03+00:00	TRUE	no_information	2020-06-29T15:18:04+00:00	N/A	FALSE	TRUE	2020-06-29T15:18:04+00:0	/A

API Key Enabled?
When was it last used?
When was it last rotated?

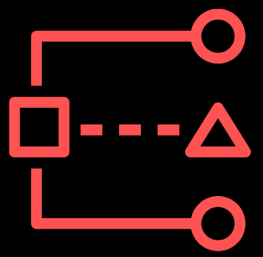
10. Monitor your resource access

- Block public access at the account or organization level



Disable public buckets

- Create IAM Access Analyzer detectors
  - Create account-specific detectors in each region
  - Create an organization-specific detector in each region



AWS IAM Access Analyzer

Are we done?

- Use permission boundaries
- Access key rotation
- Use KMS key policies and key grants for granular, temporary access
- EC2 roles should have srcIP or srcVPC condition
- VPC endpoint policies with PrincipalOrgId
- Use KMS integrations wherever available

Nope!

- Enforce IMDSv2
- Eradicate S3 access control lists
- Enforce tags on creation
- CloudTrail logs
- S3 access policies
- Remove inline policies
- Vet AWS managed policies
- Automation

Takeaways

- Use the isolation power of AWS Organizations and accounts
- Federate identity into highly granular roles with limited trust policies
- Use IAM tools like credential report, IAM access advisor, policy simulator, and IAM Access Analyzer to help you achieve least privilege



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

Resources

Steve Schmidt re:Invent Leadership session: SEC201-L

- https://youtu.be/oam8FDNJhbE?t=624

Top 10 security items to improve in your AWS account

- https://aws.amazon.com/blogs/security/top-10-security-items-to-improve-in-your-aws-account/

SCP examples

- https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html

Tasks that require root

- https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html

Federation Lab: Choose your own SAML adventure

- https://identity-federation.awssecworkshops.com

© 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.