What's the Deal with IAM?

IndyAWS

January, 2020

Presented by Caleb Gosnell


53


53


53


53


53

AWS Identity and Access Management

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

- Shared access to your AWS account
- Granular permissions
- Secure access to AWS resources for applications that run on Amazon EC2
- Multi-factor authentication (MFA)
- Identity federation
- Identity information for assurance
- PCI DSS Compliance
- Integrated with many AWS services
- Eventually Consistent
- Free to use

"Use Resources" means make AWS API calls

Authenticated

- password
- keys
- token

Authorized

- allowed by the permissions system

We understand filesystem permissions

```
sfup-aws01% ls -lah /usr/local/
total 116
drwxr-xr-x  19 root  wheel   512B Sep 14 02:15 .
drwxr-xr-x  15 root  wheel   512B Jan 31  2018 ..
drwxr-xr-x   3 root  wheel    16K Sep 14 02:10 bin
drwxr-xr-x  29 root  wheel   1.5K Sep 14 02:15 etc
drwxr-xr-x   5 root  wheel   512B Sep 14 02:15 haproxyctl
drwxr-xr-x  89 root  wheel   5.5K Sep 14 02:10 include
drwxr-xr-x   2 root  wheel   1.0K Jul 22  2019 info
drwxr-xr-x  37 root  wheel    26K Sep 14 02:10 lib
drwxr-xr-x   4 root  wheel   512B Jan 31  2018 libdata
drwxr-xr-x   7 root  wheel   1.0K Jul 22  2019 libexec
```

And, Network ACLs

Type	Protocol	Port Range	Source
HTTP	TCP	80	174.46.184.0/25
HTTP	TCP	80	216.136.125.106/32
HTTP	TCP	80	174.47.106.0/24
HTTP	TCP	80	174.47.106.254/32

Or, any set of rules

Permitted	Subject	Verb	Object
Yes	The schoolchildren The gym instructor	Kick	The sportsball
No	The schoolchildren	Kick	The schoolchildren The bus driver
Yes	The fire alarm	Interrupt	The lecture

Anatomy of an IAM Policy

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": { "AWS": "arn:aws:iam::123456789012:root"},
        "Action": ["iam:ListUsers", "iam:ListRoles"],
        "Resource": "*"
        "Condition" : { "StringEquals": { "aws:RequestedRegion":
                "us-west-1" } }
    }]
}
```

Principal (for resource and trust policies)

AWS account and root user	"Principal": { "AWS": "arn:aws:iam::AWS-account-ID:root" }
IAM users	"Principal": { "AWS": "arn:aws:iam::AWS-account-ID:user/User2"}
Federated users (using web identity or SAML federation)	"Principal": { "Federated": "arn:aws:iam::AWS-account-ID: saml-provider/provider-name"}
IAM roles	"Principal": { "AWS": "arn:aws:iam::AWS-account-ID:role/rolename" }
Assumed-role sessions	"Principal": { "AWS": "arn:aws:sts::AWS-account-ID: assumed-role/role-name/role-session-name" }
AWS services	(via trust policies)
Anonymous users (not recommended)	"Principal": { "AWS" : "*" }

Action (required)

- "Action": "sqs:SendMessage "
- "Action": "iam:ChangePassword "
- "Action": ["ec2:StartInstances", "s3:GetObject"]
- "Action": "s3:*"
- "Action": "iam:*AccessKey*"

Resource

- arn:partition:service:region:account-id:resource-id
- arn:partition:service:region:account-id:resource-type/resource-id
- arn:partition:service:region:account-id:resource-type:resource-id

- "Resource": "arn:aws:s3:::example-bucket"
- "Resource": "arn:aws:s3:::example-bucket/dir/file1"
- "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
- "Resource": "arn:aws:iam::123456789012:policy/InnocentPolicy"
- "Resource":"arn:aws:iam::123456789012:group/*"

Conditions

```
"Condition" : {
  "{condition-operator}" : {
    "{condition-key}" : "{condition-value}"
  }
}
```

A few Operators:

- "StringEqualsIgnoreCase"
- "NumericLessThanEquals"
- "IpAddress"
- "Bool"

A few Keys:

- "aws:username"
- "aws:MultiFactorAuthAge"
- "ec2:ResourceTag/Team"
- "s3:prefix"
- "sts:ExternalId"

Policy Types

Type	Attached to	Defined via	Purpose
Identity policy	IAM principal: user, group, role	IAM API	assign privileges to the identity
Resource policy	Account resource: S3, ECR, Lambda, Secrets Manager, Backup	specific service API	delegate privileges to the resource
Trust policy	IAM role	IAM API	define requirement to use the role
Scope limiting policy	varies	varies	set hard limits on privileges available

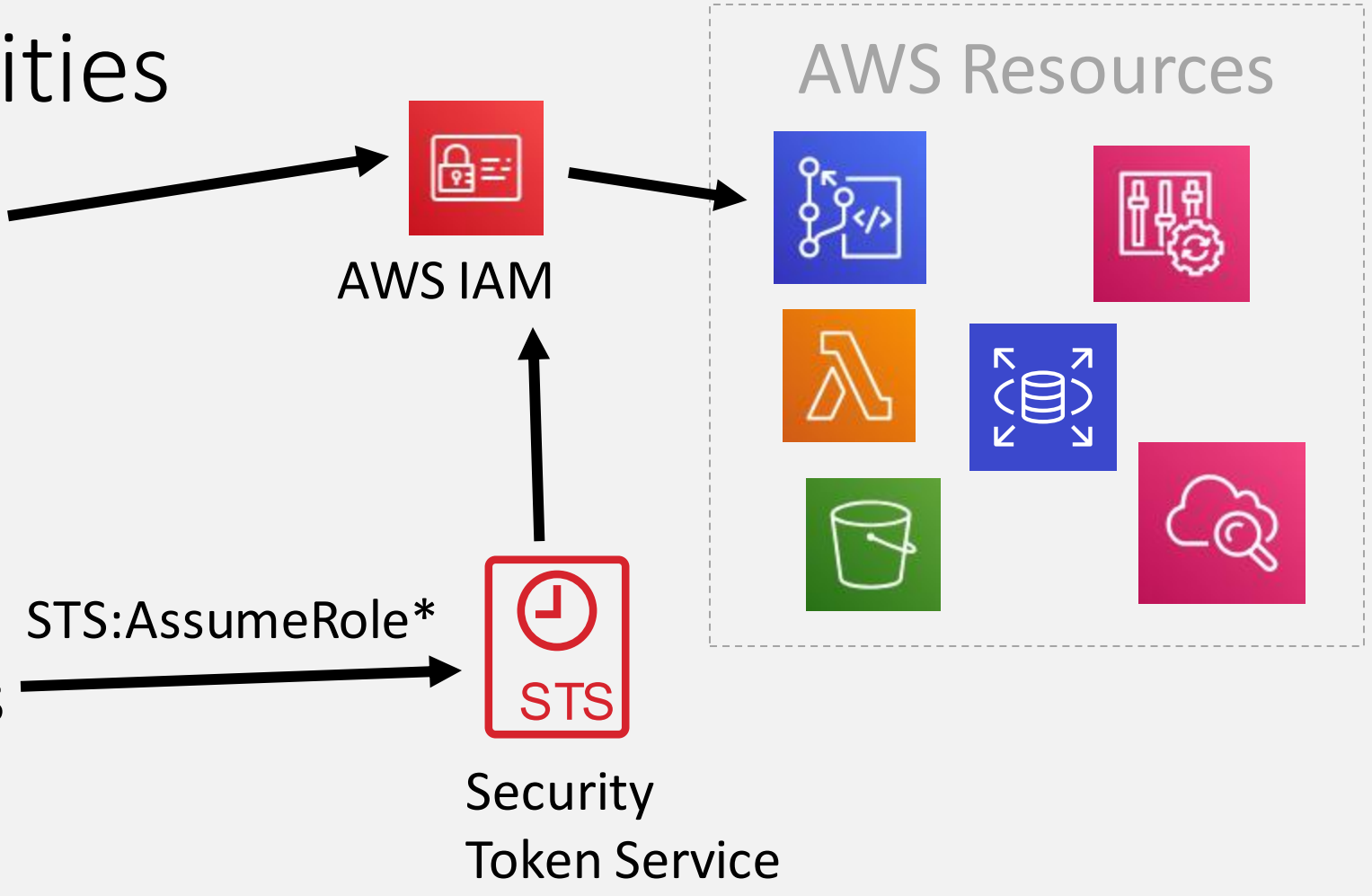
Using IAM identities

Long lived Credentials

- Root User
- IAM Users
- IAM Groups

Temporary Credentials

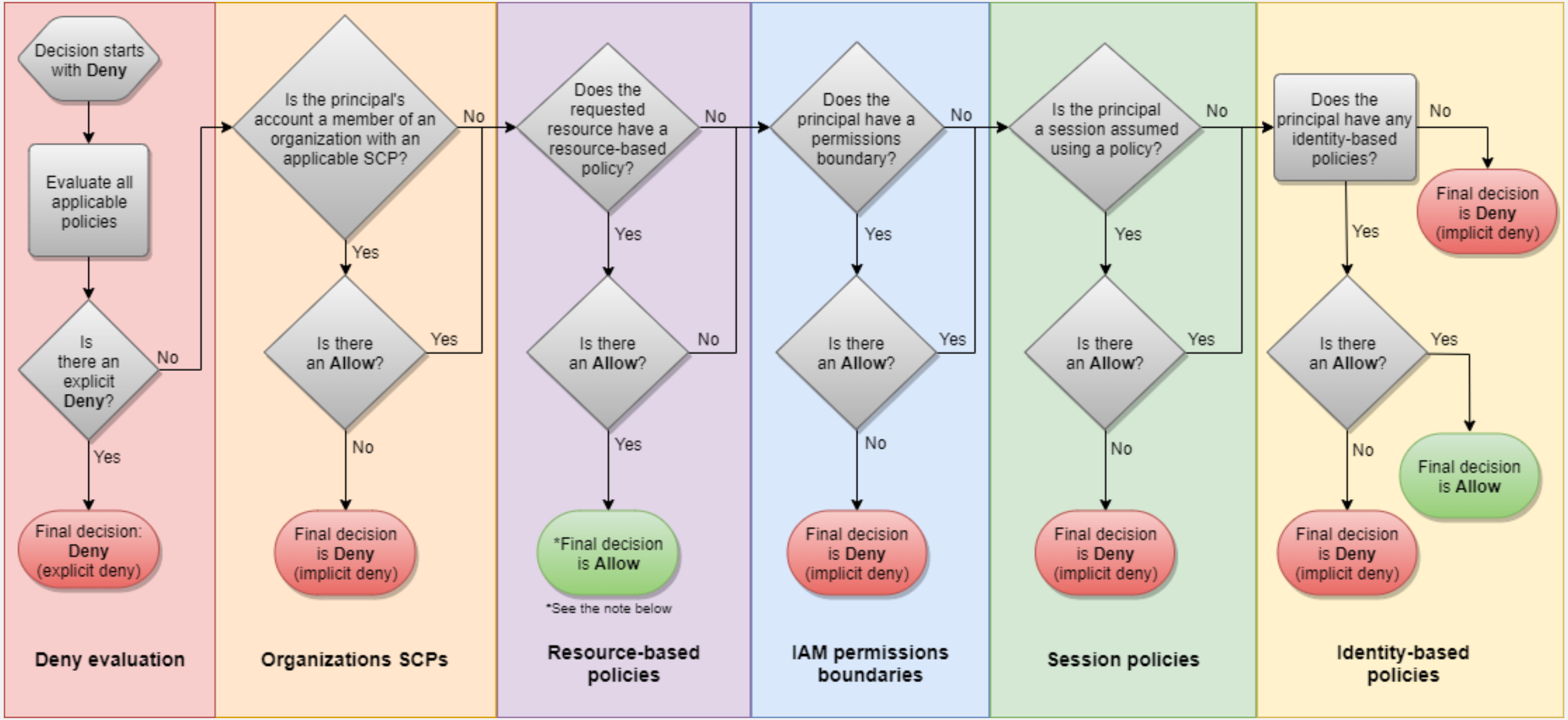
- IAM Roles
  - Service Accounts
  - Federated Users/ Identity Provider

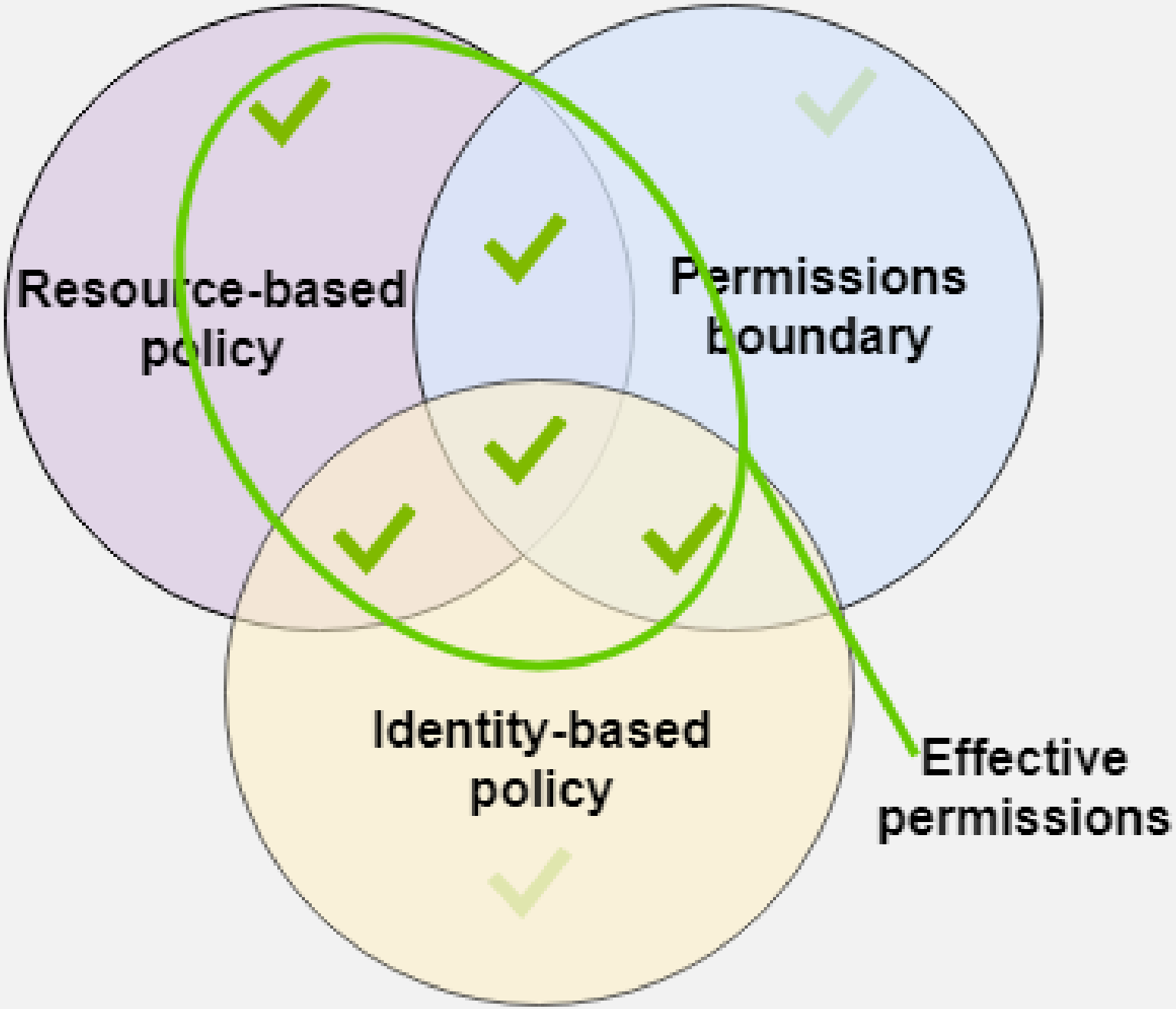


Scope Limiting Policies

- Session Permissions – parameter to STS
- Permissions Boundaries – assigned via IAM
- Service Control Policies – AWS Organizations

Evaluating Permissions




Resource-based policy
Permissions boundary
Identity-based policy
Effective permissions

Tour & Examples

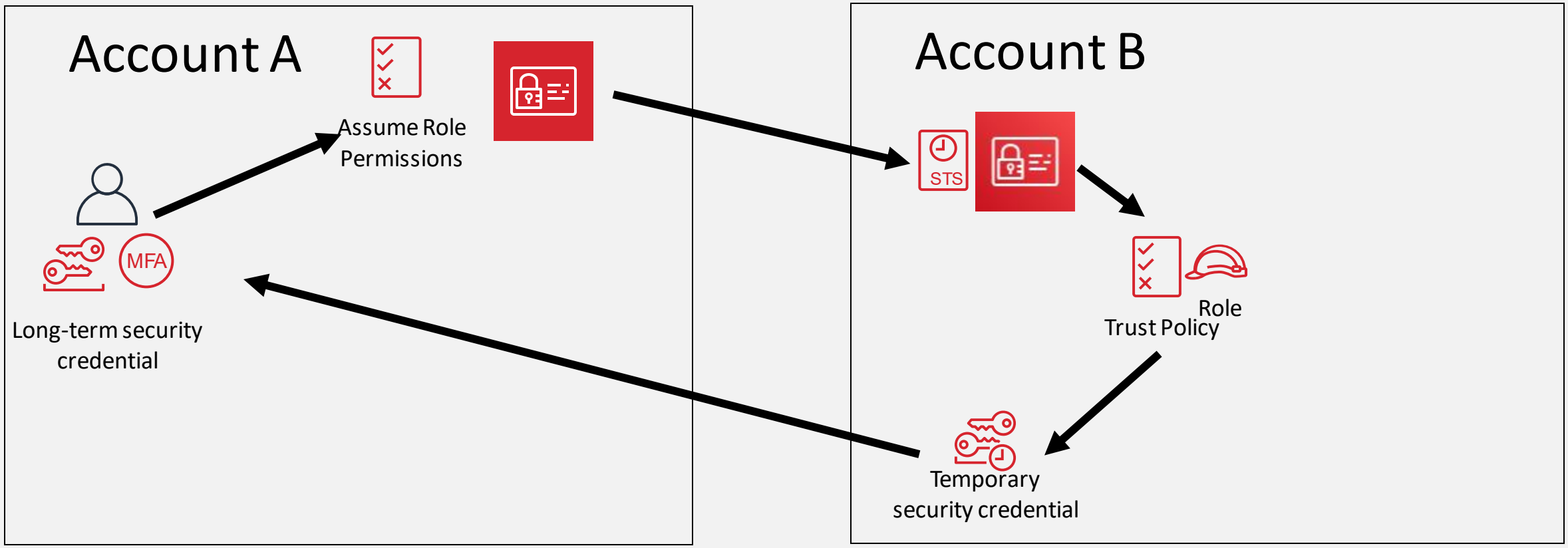
Tour:

- IAM Console
- Policy Editor
- Access Analyzer

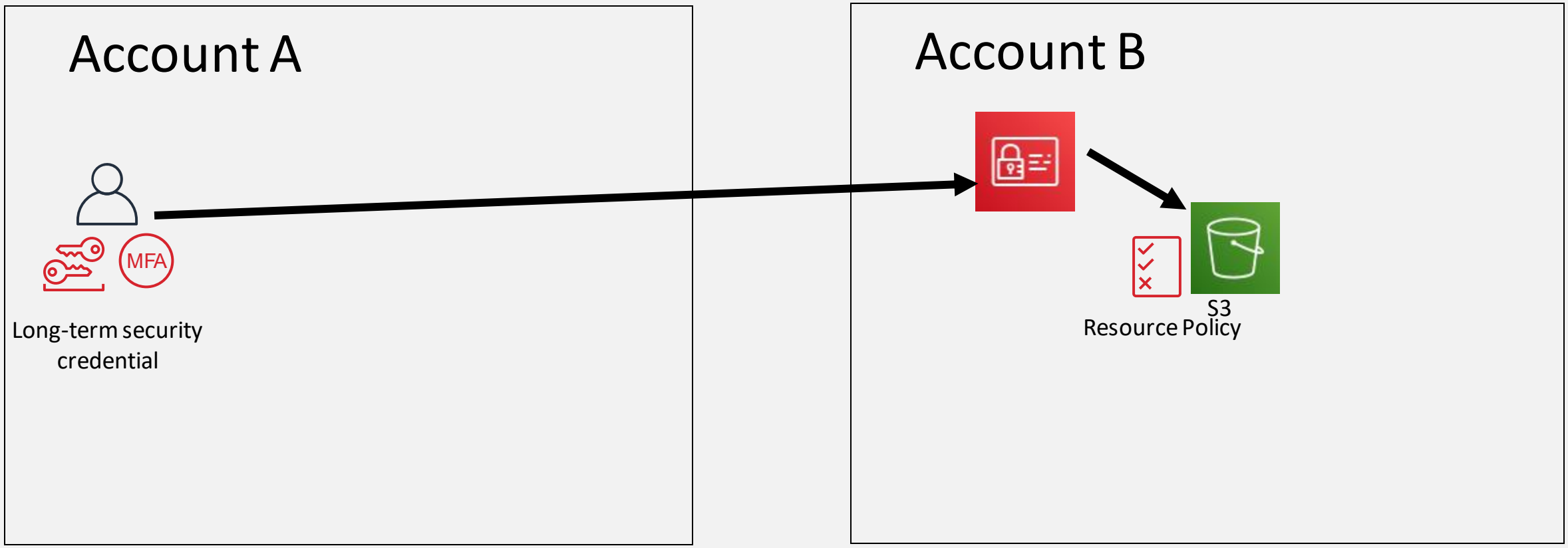
Examples:

- Cross-Account access
- Cross-Account S3 bucket
- Service Control Policy
- EC2 RDS IAM permissions
- User Federation (SAML)

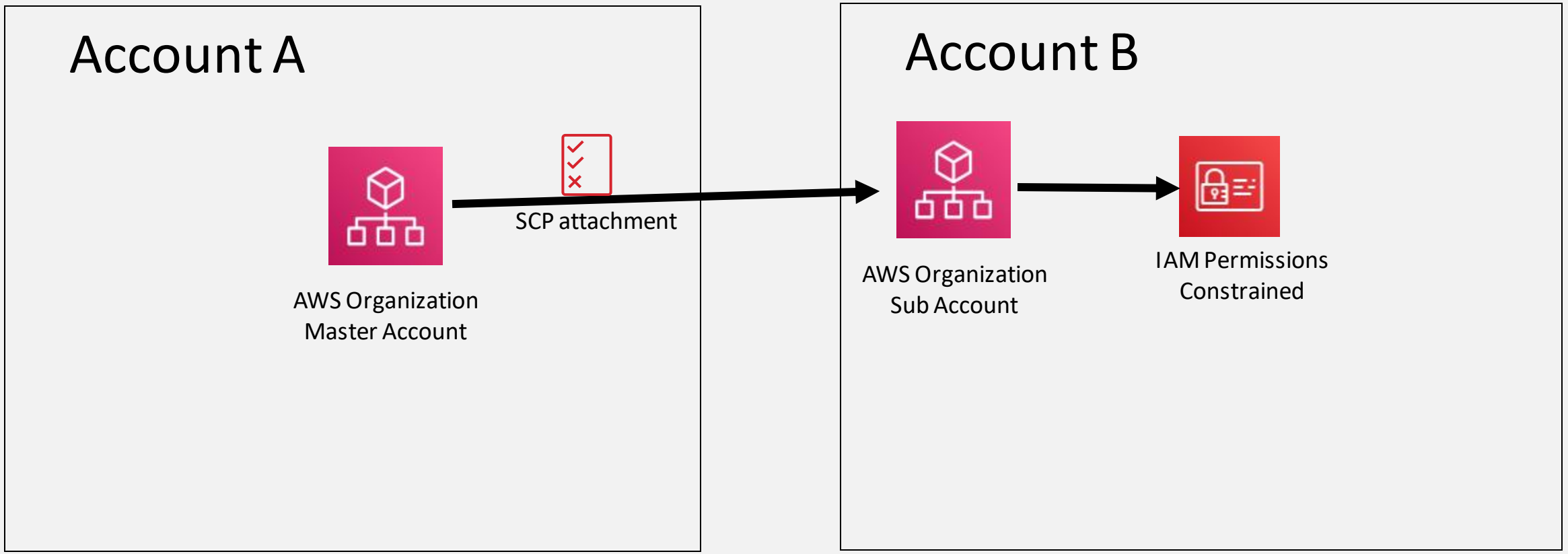
Cross Account Access



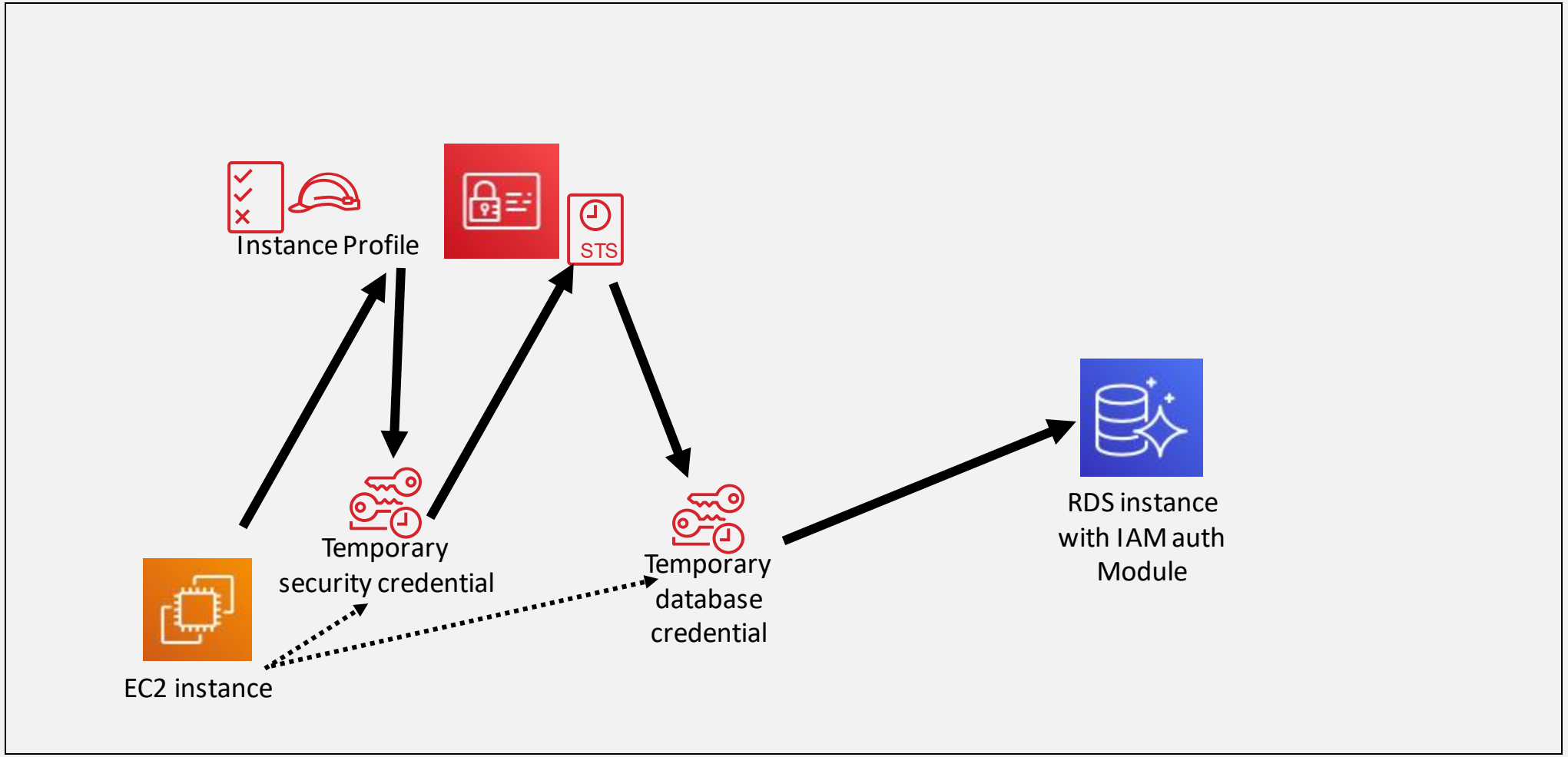
Cross Account S3 Resource Policy



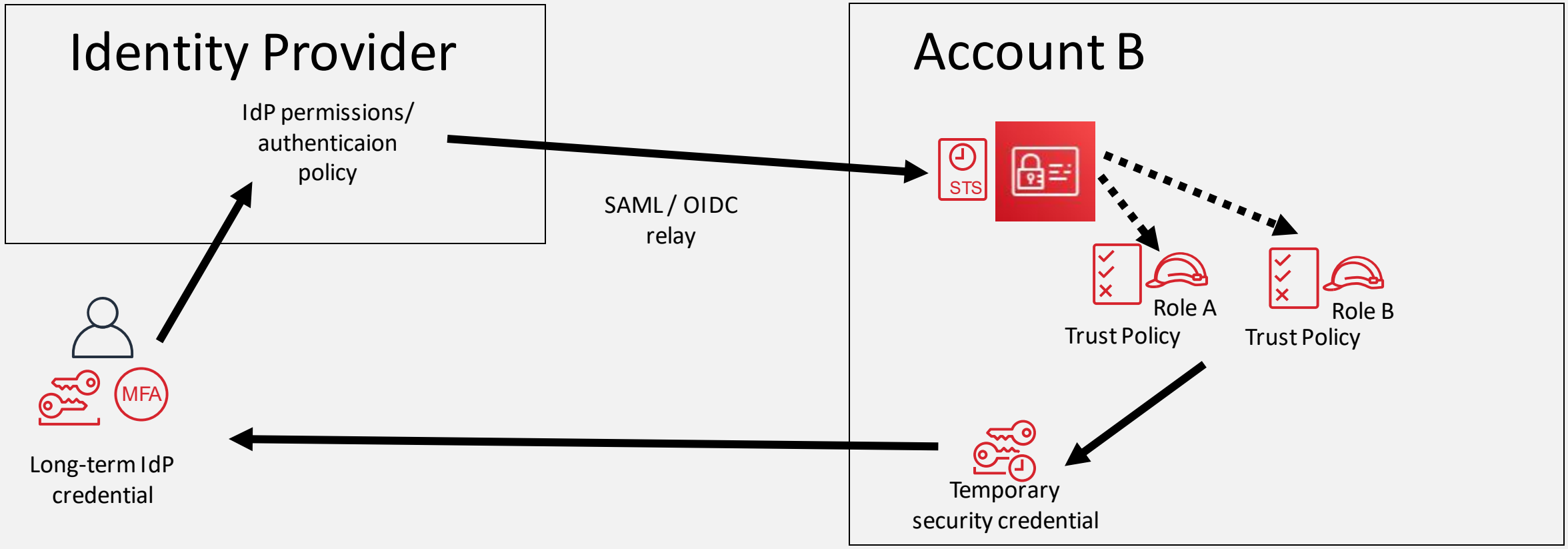
Service Control Policy



EC2 RDS IAM


Instance Profile
STS
Temporary
security credential
Temporary
database
credential
RDS instance
with IAM auth
Module
EC2 instance

SAML Federation



Sources:
https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-ug.pdf
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#access_policies-json
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

API docs:
https://docs.aws.amazon.com/IAM/latest/APIReference/API_Operations.html
https://docs.aws.amazon.com/STS/latest/APIReference/API_Operations.html
https://docs.aws.amazon.com/access-analyzer/latest/APIReference/API_Operations.html

Advanced usage:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_testing-policies.html

Advanced Other
https://know.bishopfox.com/research/privilege-escalation-in-aws

Examples:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#instance-metadata-security-credentials
https://gist.github.com/quiver/509e1a6e6b54a0148527553502e9f55d
https://auth0.com/docs/integrations/aws/sso
https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Amazon-Web-Service
https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s3-resources/
https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html

Photo credits:
https://i.ytimg.com/vi/qktuv-S8Lpg/hqdefault.jpg
https://pbs.twimg.com/profile_images/930577665643438080/VVjqz6XO.jpg
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTfC7dsQqxK0qEOraz8kAwdDygD4KR3TRz_NuITdSCJ1qOnBdFy&s
https://pbs.twimg.com/profile_images/1174385375210606592/cuW5vh3Q_400x400.jpg