

The background of the image is a vibrant blue with a complex, abstract pattern of overlapping, curved lines that create a sense of depth and movement. The lines are in various shades of blue and purple, with some areas appearing lighter and more saturated than others. The overall effect is a dynamic, almost architectural feel, reminiscent of a modern building's facade or a digital data visualization.

AWS re:Inforce

JULY 26 – 27, 2022 | BOSTON, MA

I A M 3 0 9

Designing a well-architected identity & access management solution

Djamel Bourokba (Dee-Jay)

Sr. Global Solutions Architect –
Automotive
AWS

Steve Vinsik

Sr. Manager, Product Management –
Workforce Identity
AWS



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Identity positioning

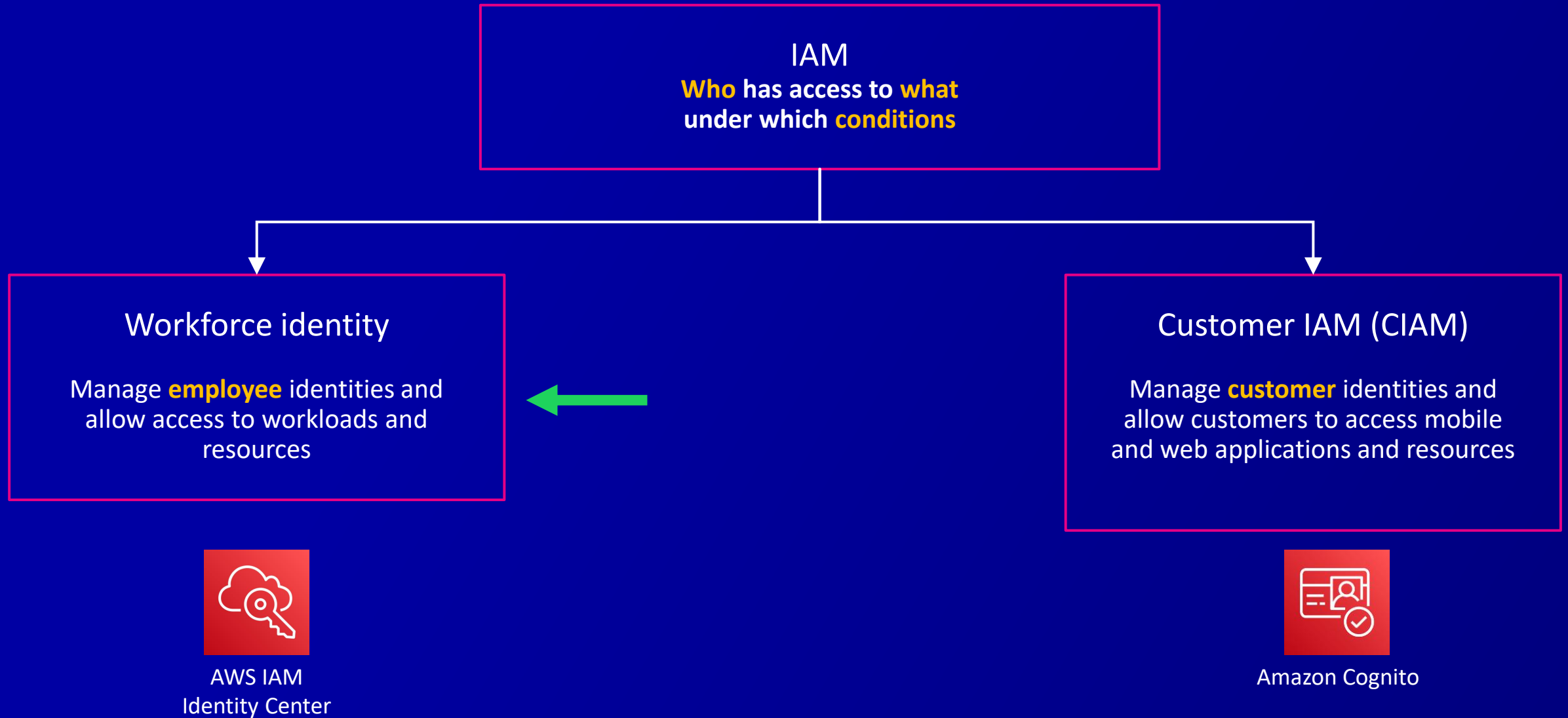
AWS federation options

AWS IAM Identity Center

RBAC, ABAC, and delegation models

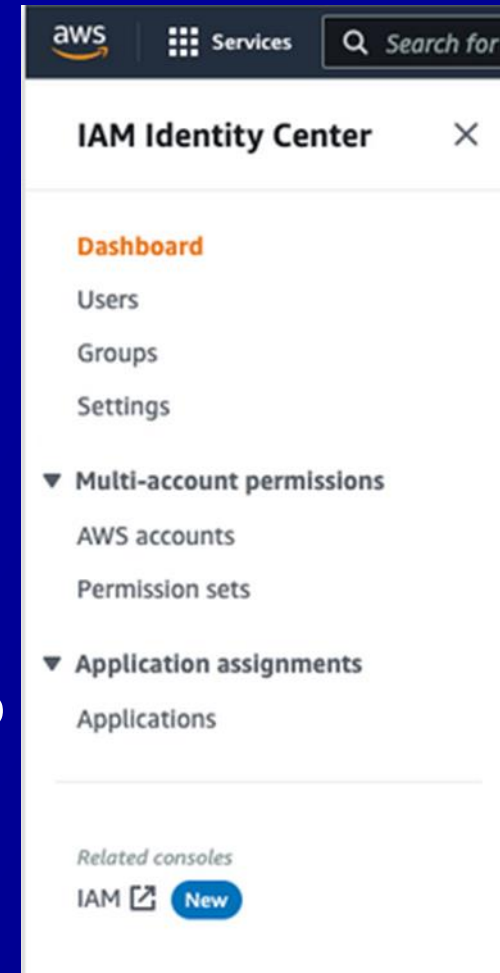
DR & resiliency

Identity and access management



AWS SSO is now AWS IAM Identity Center

- **One place to create or connect your workforce identities** and centrally manage secure access across AWS
- **Freedom to choose** your preferred identity source for use across AWS
- **Multi-account permissions** to manage fine grained access at scale
- **Application assignments** to manage access to IAM Identity Center enabled and other cloud applications



What Changes

New service name

New console name

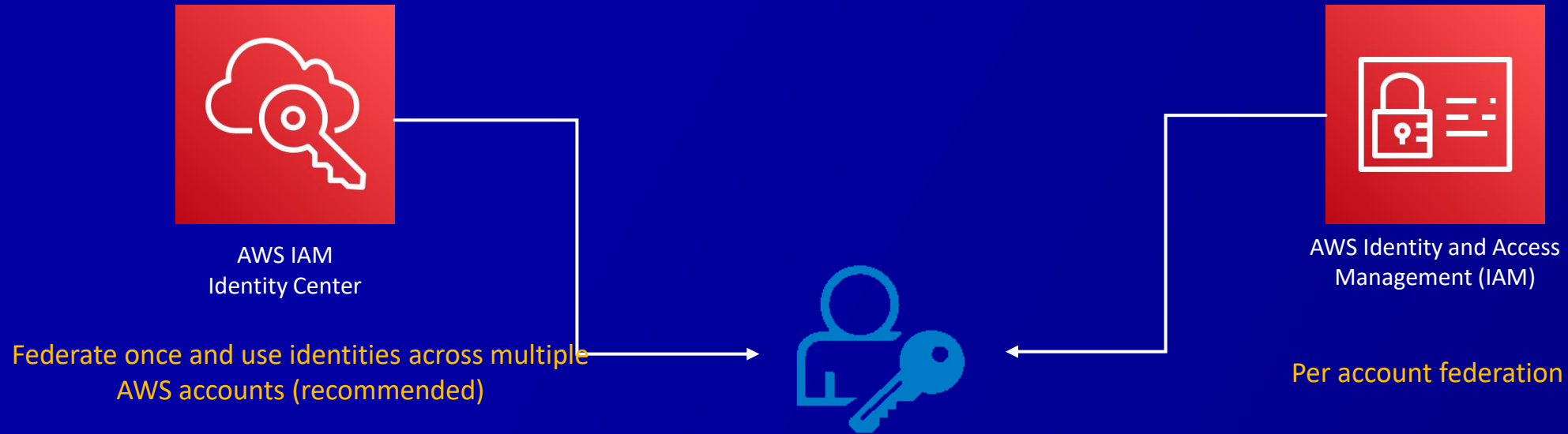
Improved console navigation

What does NOT change

No technical changes

No API changes

Federation options on AWS



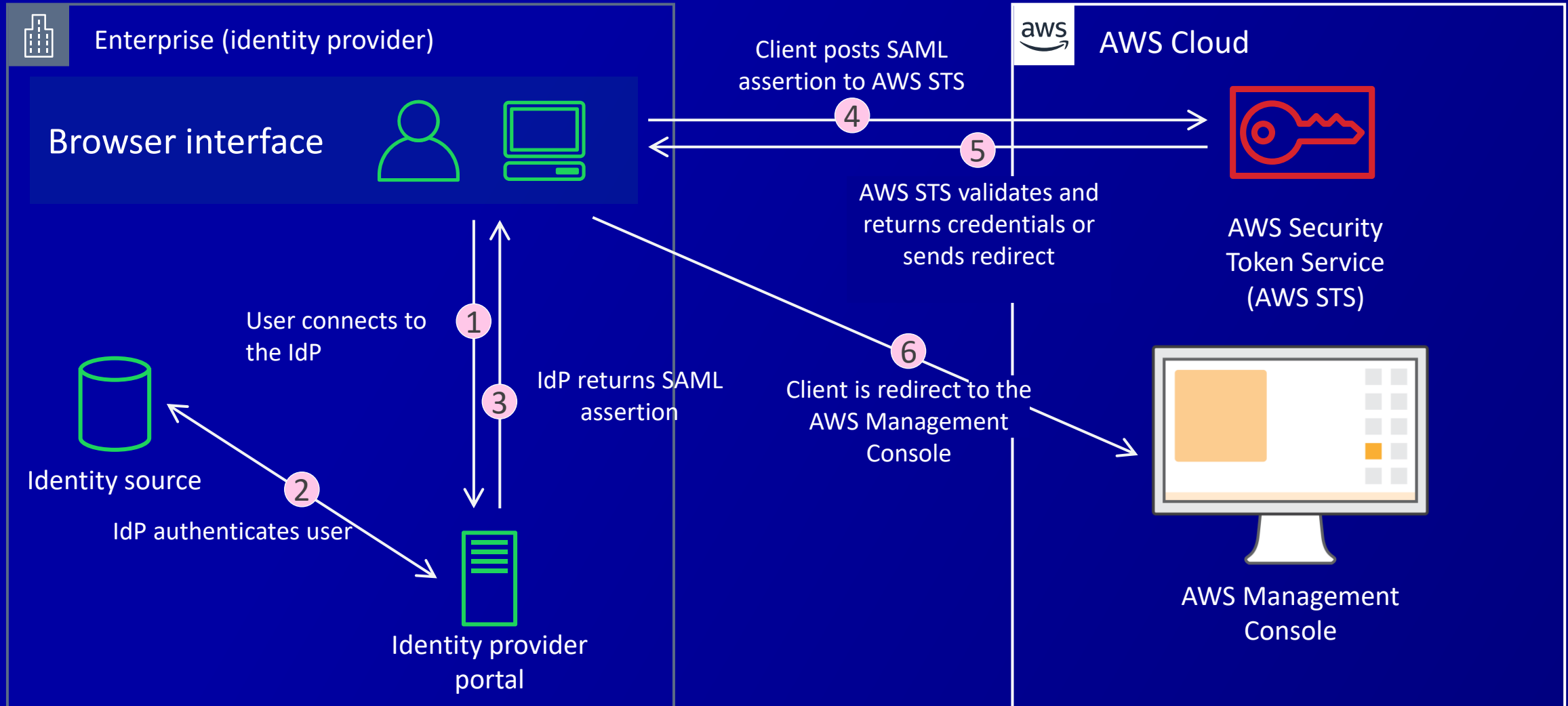
New setup

- Start with AWS IAM Identity Center Federate using existing IDP
- Or create users and groups in AWS IAM Identity Center

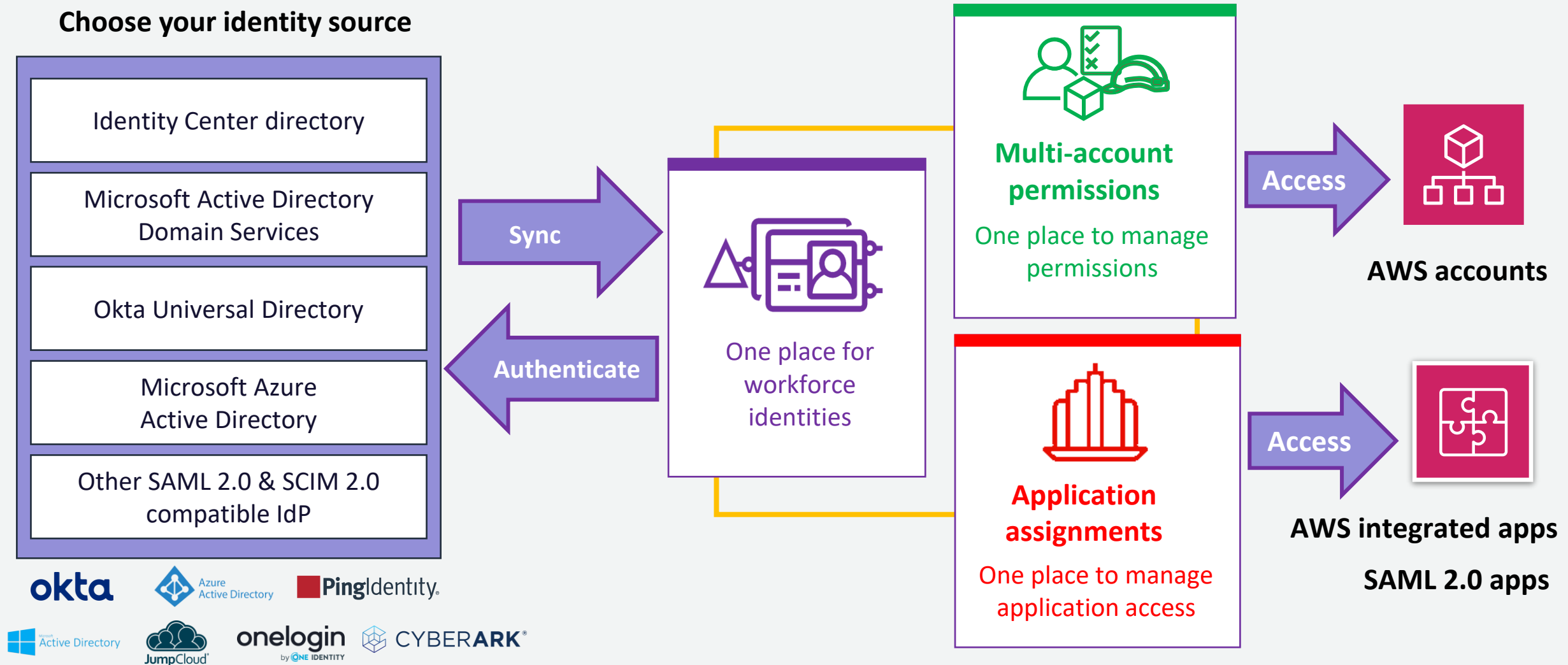
Existing setup

- Use both IAM and AWS IAM Identity Center
- Recommend migration to AWS IAM Identity Center

IAM federation – SAML 2.0

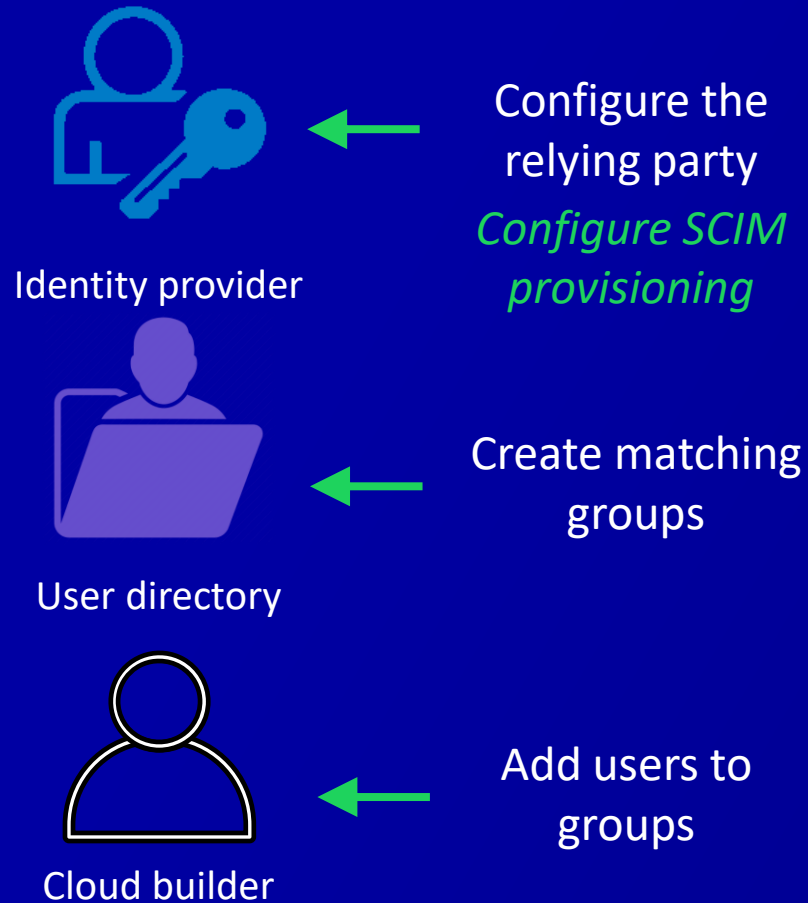


How IAM Identity Center Works

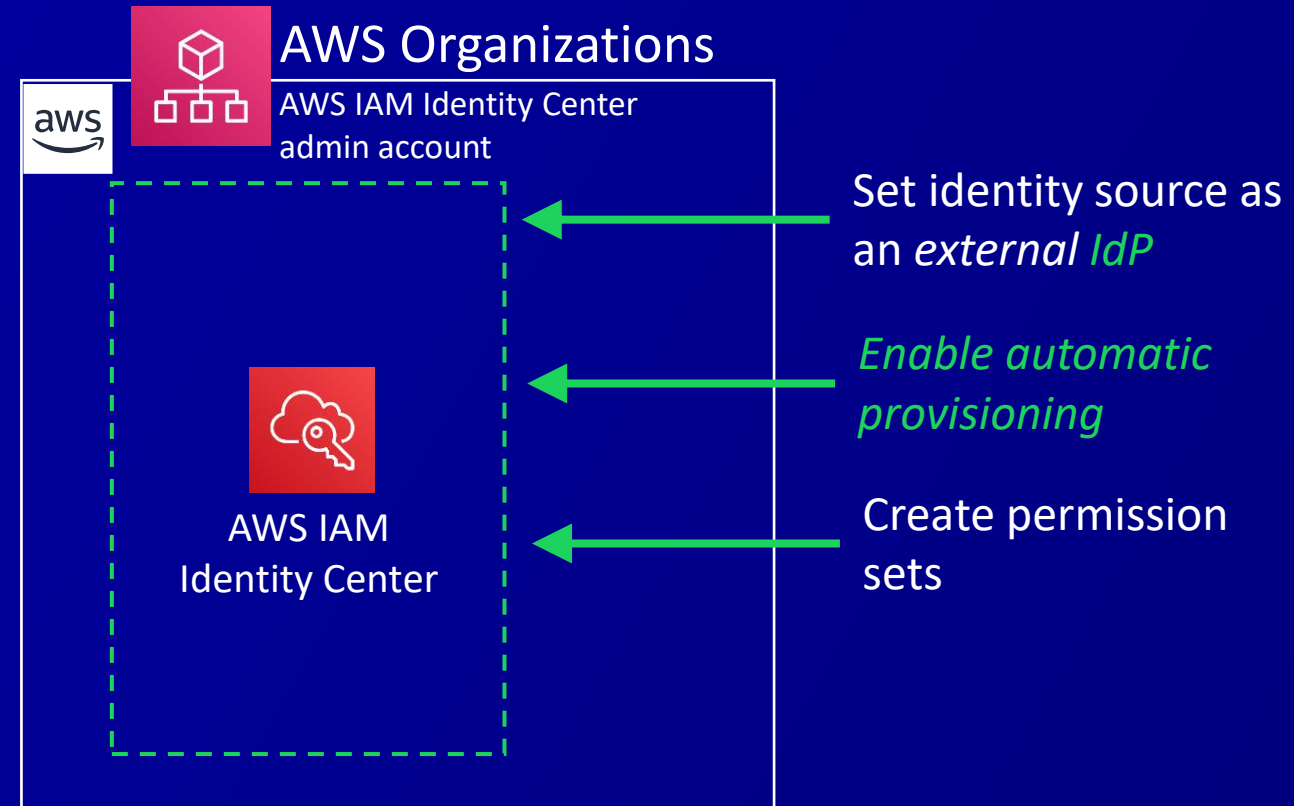


AWS IAM Identity Center with external IdP

IdP configuration

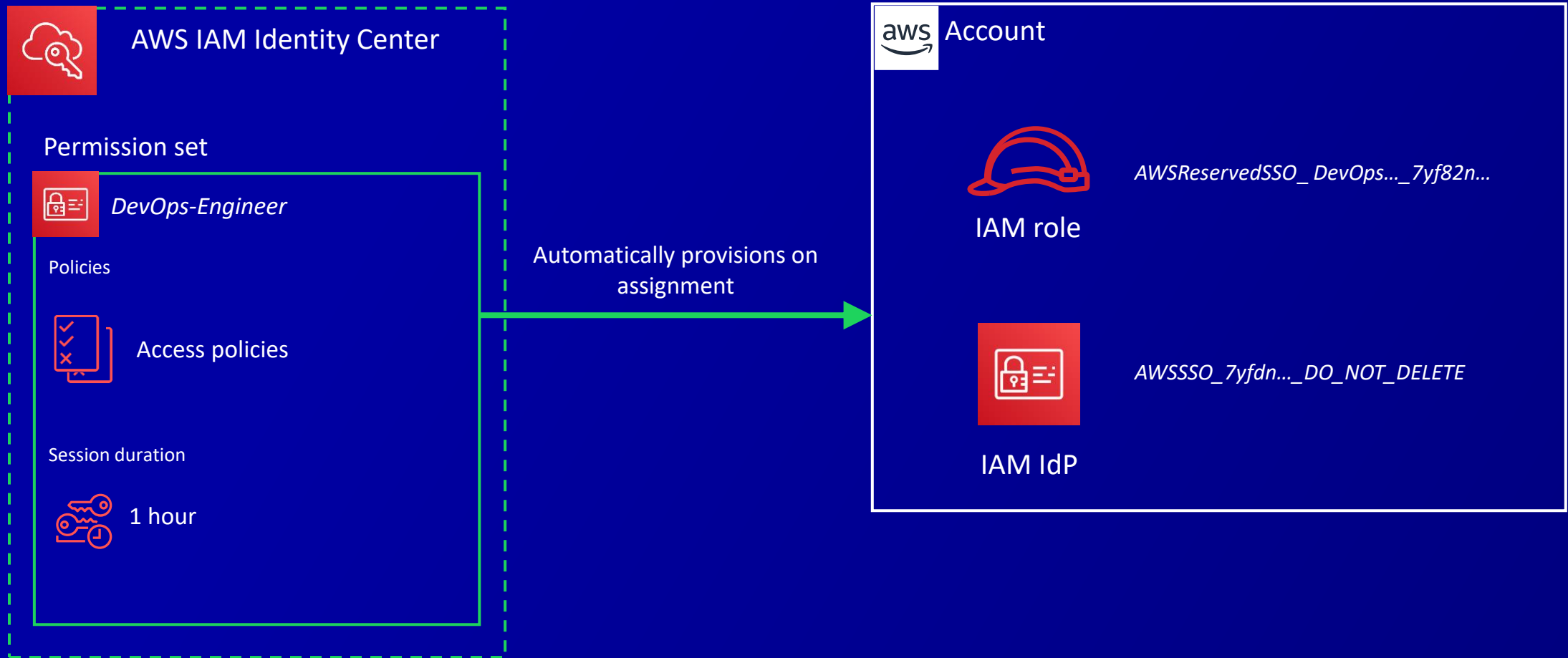


AWS configuration

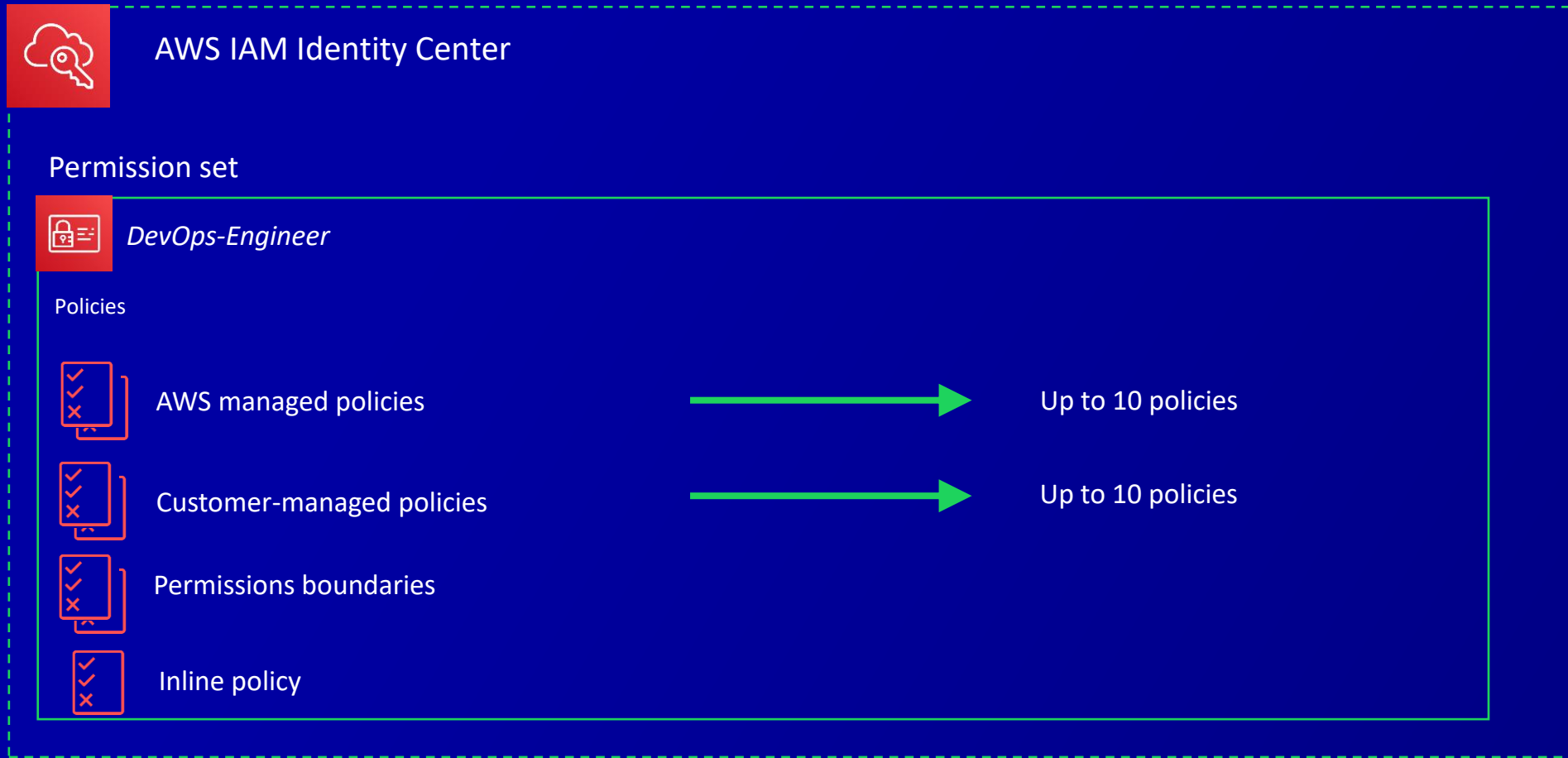


AWS IAM Identity Center – Permission sets

Permission sets are role definitions



AWS IAM Identity Center – Permission set options



AWS IAM Identity Center – Applications assignments

[Amazon Grafana](#) > [Workspaces](#) > Create new workspace

Step 1
[Specify workspace details](#)

Step 2
Configure settings

Step 3
[Service managed permission settings](#)

Step 4
[Review and create](#)

Configure settings [Info](#)

Authentication access [Info](#)

Choose at least one authentication method.

☒ **AWS Single Sign-On (AWS SSO)** ✔ Enabled

You can enable SSO by creating a user. This new user does not automatically have access to the Grafana console. You will still need to assign this user later, once this workspace is created.

☐ **Security Assertion Markup Language (SAML)**

You will need to complete additional steps to finish SAML configuration once this workspace is created.

Permission type [Info](#)

☒ **Service managed**

We will automatically provision the permissions for you based on the AWS services you choose in the next step.

☐ **Customer managed**

Manually create your own IAM role based on the suggested policies.

which user attributes in your application map to

▼

▼

▼

Remove

Remove

Cancel

Previous

Next

Cancel

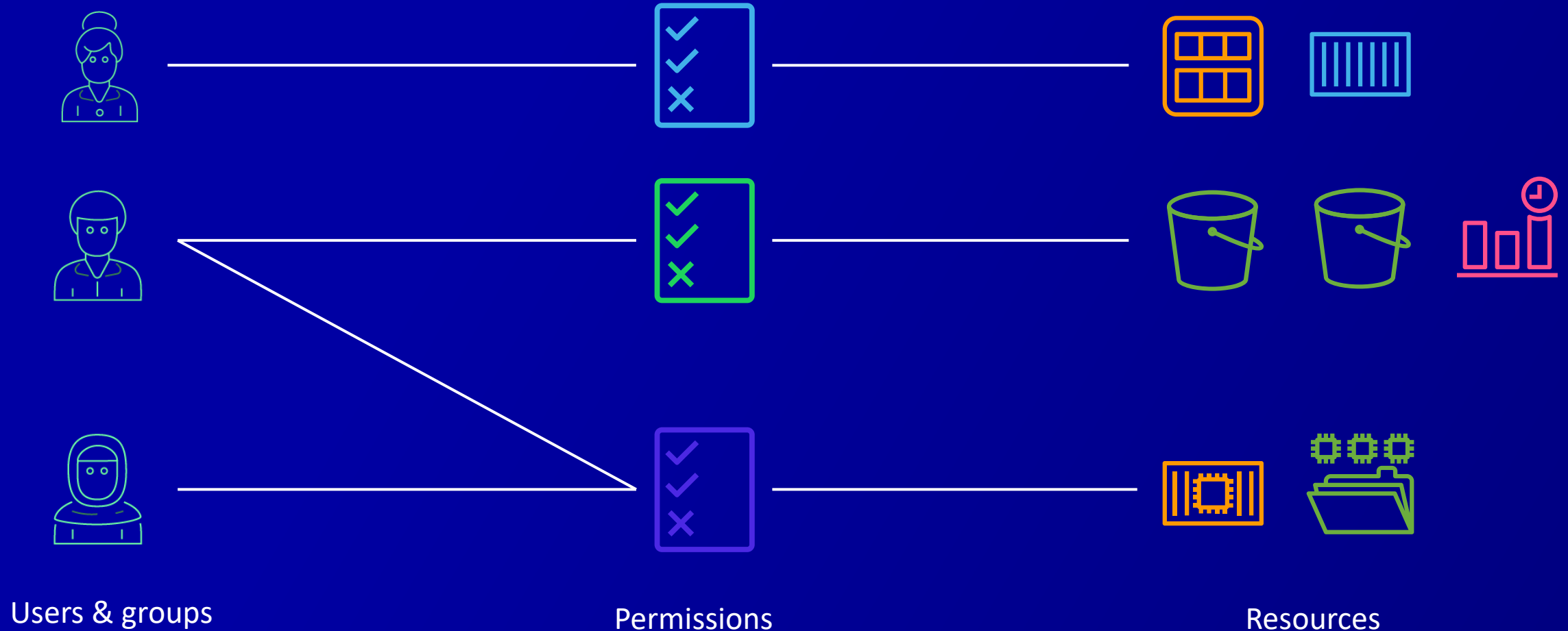
Save changes



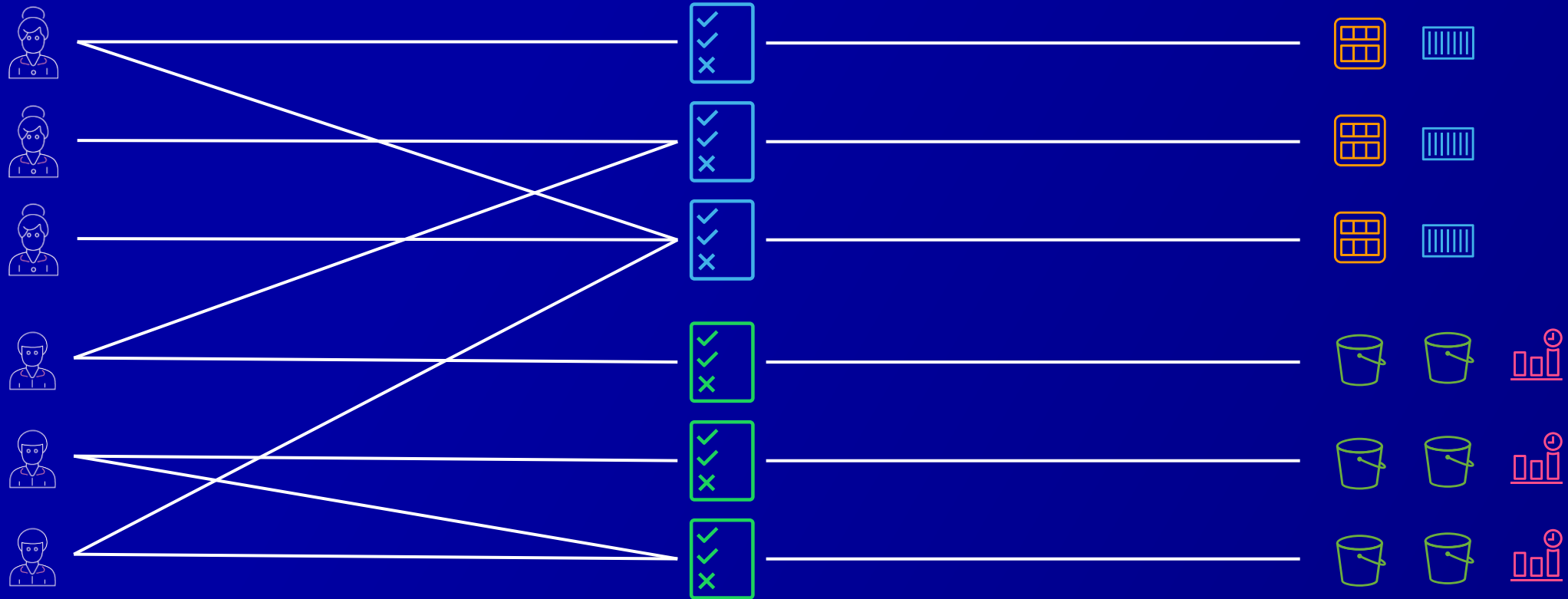
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scaling permissions in multi-account environments

Role-based access control (RBAC)



What ends up happening

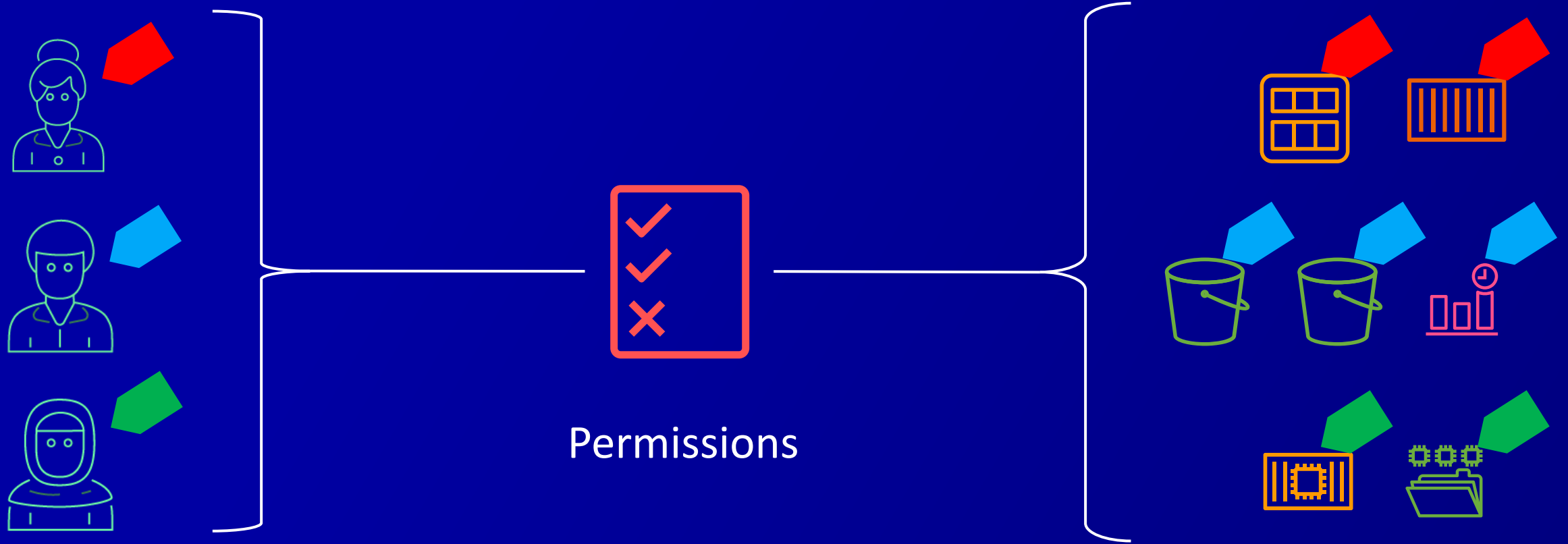


Users & groups

Permissions

Resources

A scalable permissions model based on attributes



Workforce teams

Resources

Benefits of ABAC

Permissions **scale with innovation**, allowing workforce users to build

Teams move fast, as **permissions automatically apply** based on attributes

Granular permissions are possible without requiring a permissions update for every new user or resource

Audit attributes are available to determine access

Examples of attribute-based permissions

Engineering department requires read and write **access** to their project resources

Engineering department requires developers to **assign their project** to new resources

Grant project serverless read access **to their team** resources

Manage only the resources that **I own**

Learn more: <https://aws.amazon.com/identity/attribute-based-access-control/>

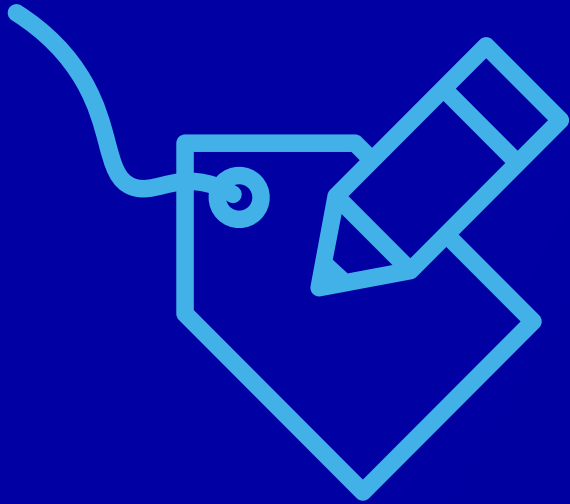


A little bit about attributes on AWS

Attributes are known as tags on AWS

Attributes are a key or a key and value pair

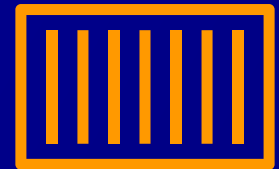
Use attributes for cost allocation, discovery, and access control



Examples



Team = Engineering
Project = Serverless



Team = Engineering
Project = Serverless

Sample ABAC policy for session tags

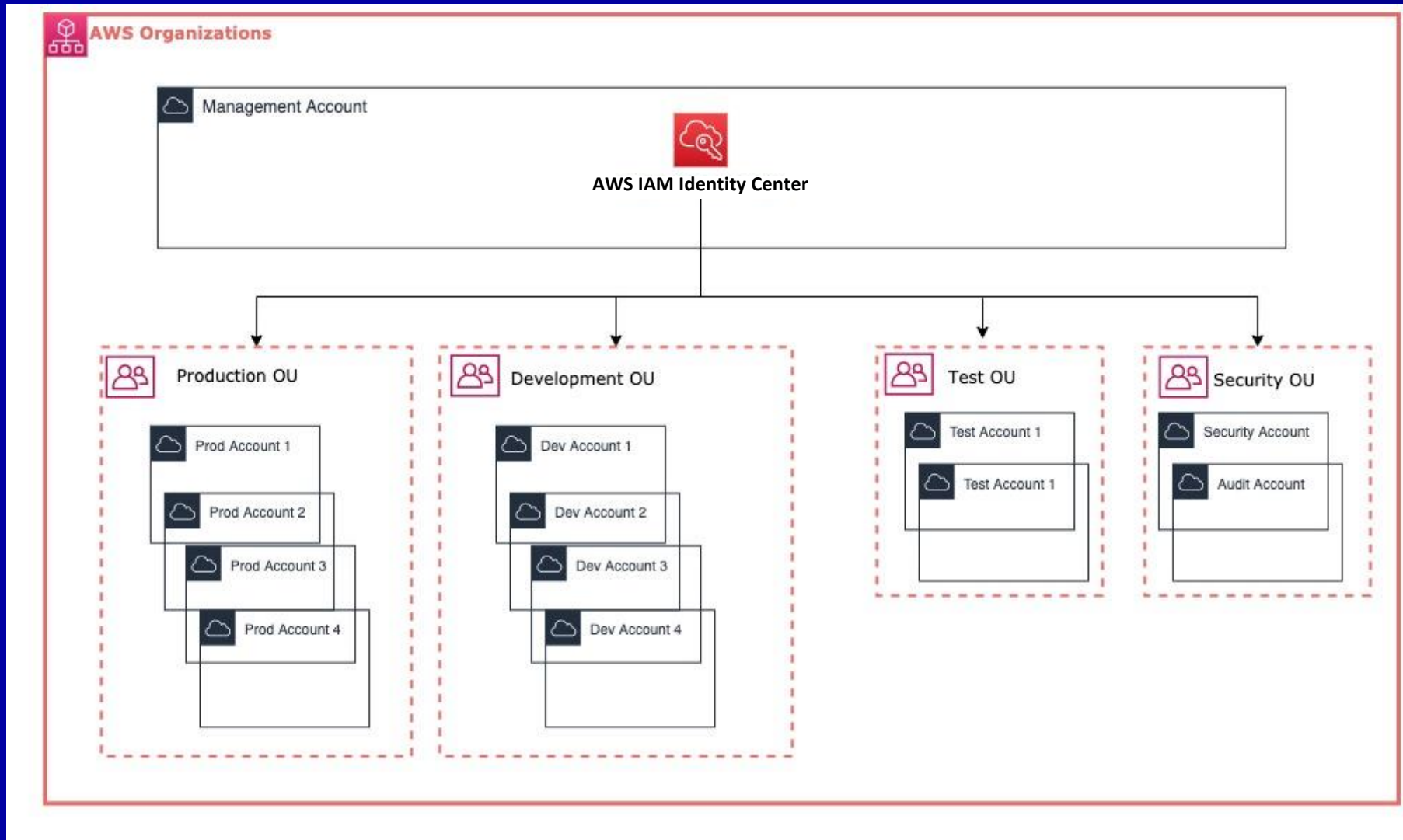
```
{
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:GetSecretValue",
    "secretsmanager:UpdateSecret"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "secretsmanager:ResourceTag/project": "${aws:PrincipalTag/project}"
    }
  }
}
```

**Only manage resources
that match user's project**

Permission delegation



AWS IAM Identity Center delegation



AWS IAM Identity Center delegation example (account)

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect": "Allow",
    "Action": [
      "sso:CreateAccountAssignment",
      "sso:ProvisionPermissionSet",
      "sso:....."
    ],
    "Resource": [
      "arn:aws:sso:::instance/ssoins-<sso-ins-id>/*",
      "arn:aws:sso:::account/112233445566",
      "arn:aws:sso:::account/223344556677",

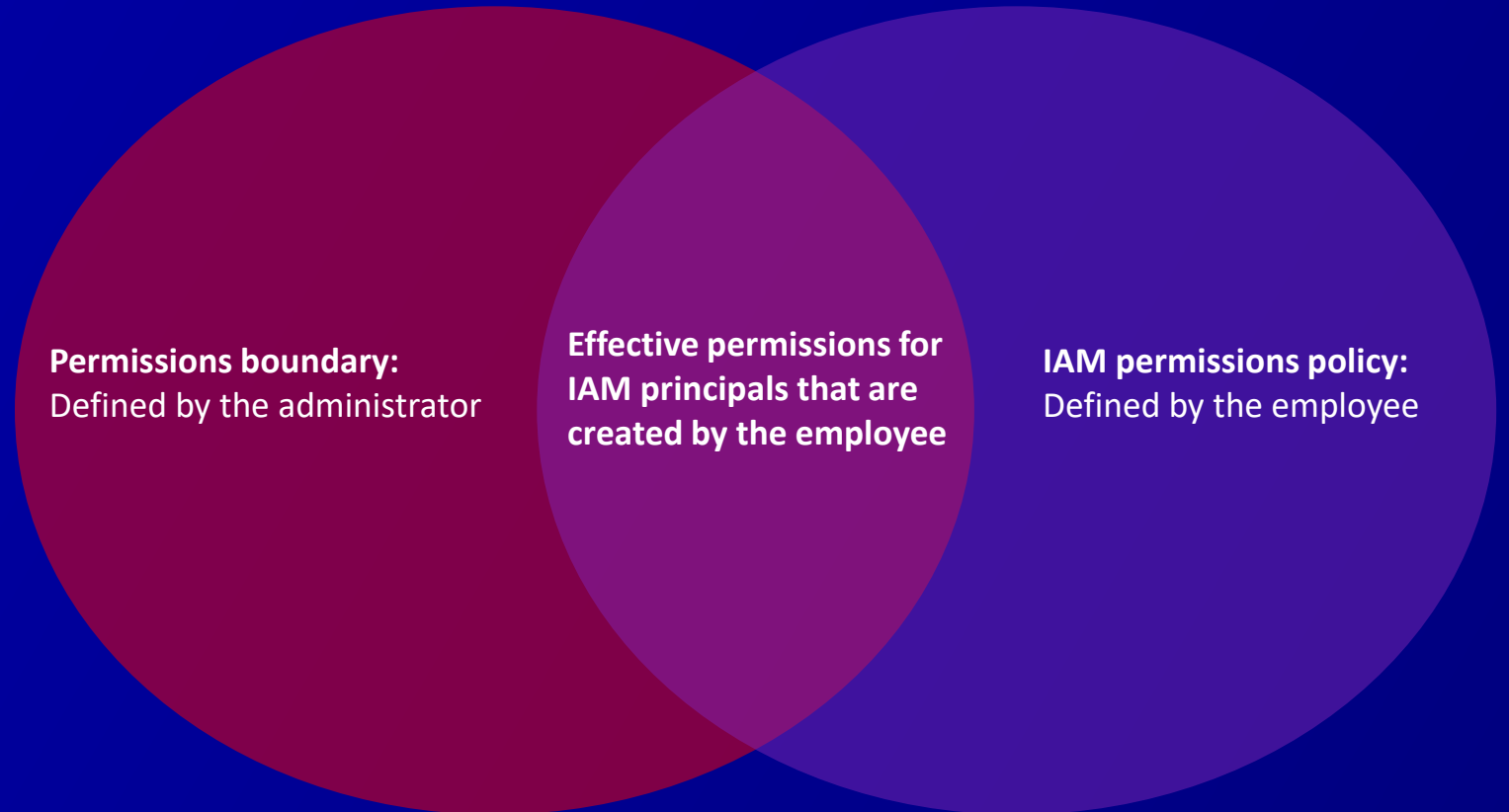
    ]
  }
}
```

AWS IAM Identity Center delegation example (account and permissions)

```
{  
  "Version" : "2012-10-17",  
  "Statement" : [ {  
    "Effect": "Allow",  
    "Action": [  
      "sso:CreateAccountAssignment",  
      "sso:ProvisionPermissionSet",  
      "sso:....."  
    ],  
    "Resource": [  
      "arn:aws:sso:::instance/ssoins-<sso-ins-id>/*",  
      "arn:aws:sso:::permissionSet/ssoins-1111111111/ps-112233abcdef123",  
      "arn:aws:sso:::account/112233445566",  
      "arn:aws:sso:::account/223344556677"  
    ]  
  }  
}
```

Permissions boundaries

- Apply permissions boundaries to the **IAM roles created by developers**, rather than to the developers themselves
- Use IAM identity policies and AWS Organizations service control policies (SCPs) to **restrict developer access**
- Group your **permissions boundaries into categories** that fit the scope of similar application functions (such as system automation and analytics)



Permissions boundary walkthrough

Admin step 1: Create the permissions boundary (managed policy)

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect": "Allow",
    "Action": [
      "dynamodb:PutItem",
      "dynamodb:UpdateItem",
      "dynamodb:DeleteItem"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": { "aws:RequestedRegion": "eu-central-1" }
    }
  } ]
}
```

arn:aws:iam::<ACCOUNT_NUMBER>:policy/boundaries/dynamodb_eu

Permissions boundary walkthrough

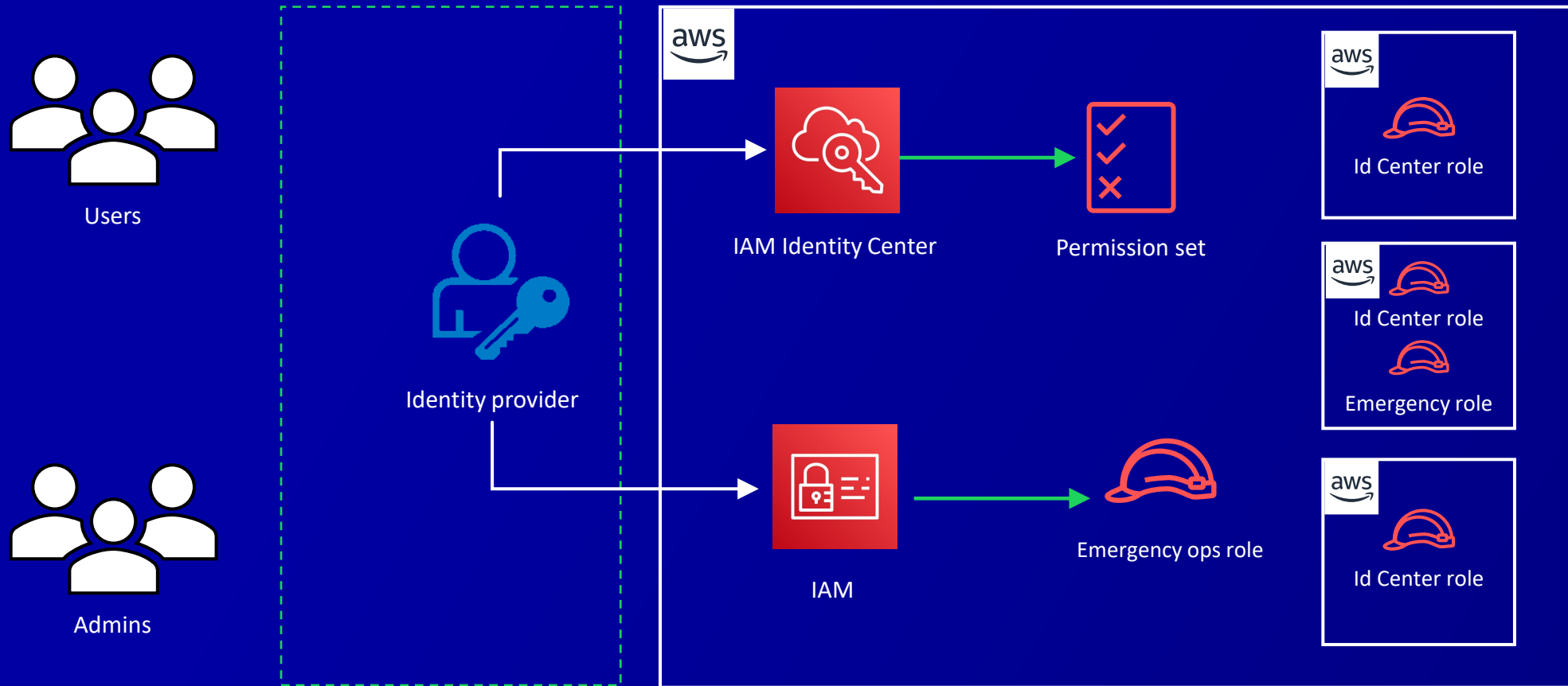
```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": [ "iam:CreateRole", "iam:AttachRolePolicy", "iam:DetachRolePolicy" ],
    "Resource": "arn:aws:iam::<ACCOUNT_NUMBER>:role/executionroles/MyTestApp*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary":
          "arn:aws:iam::<ACCOUNT_NUMBER>:policy/boundaries/dynamodb_eu"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [ "iam:CreatePolicy", "iam:CreatePolicyVersion", "iam:DeletePolicyVersion" ],
    "Resource": "arn:aws:iam::<ACCOUNT_NUMBER>:policy/delegatedadmin/*"
  } ]
}
```

Admin step 2: Allow role creation, but only within boundary

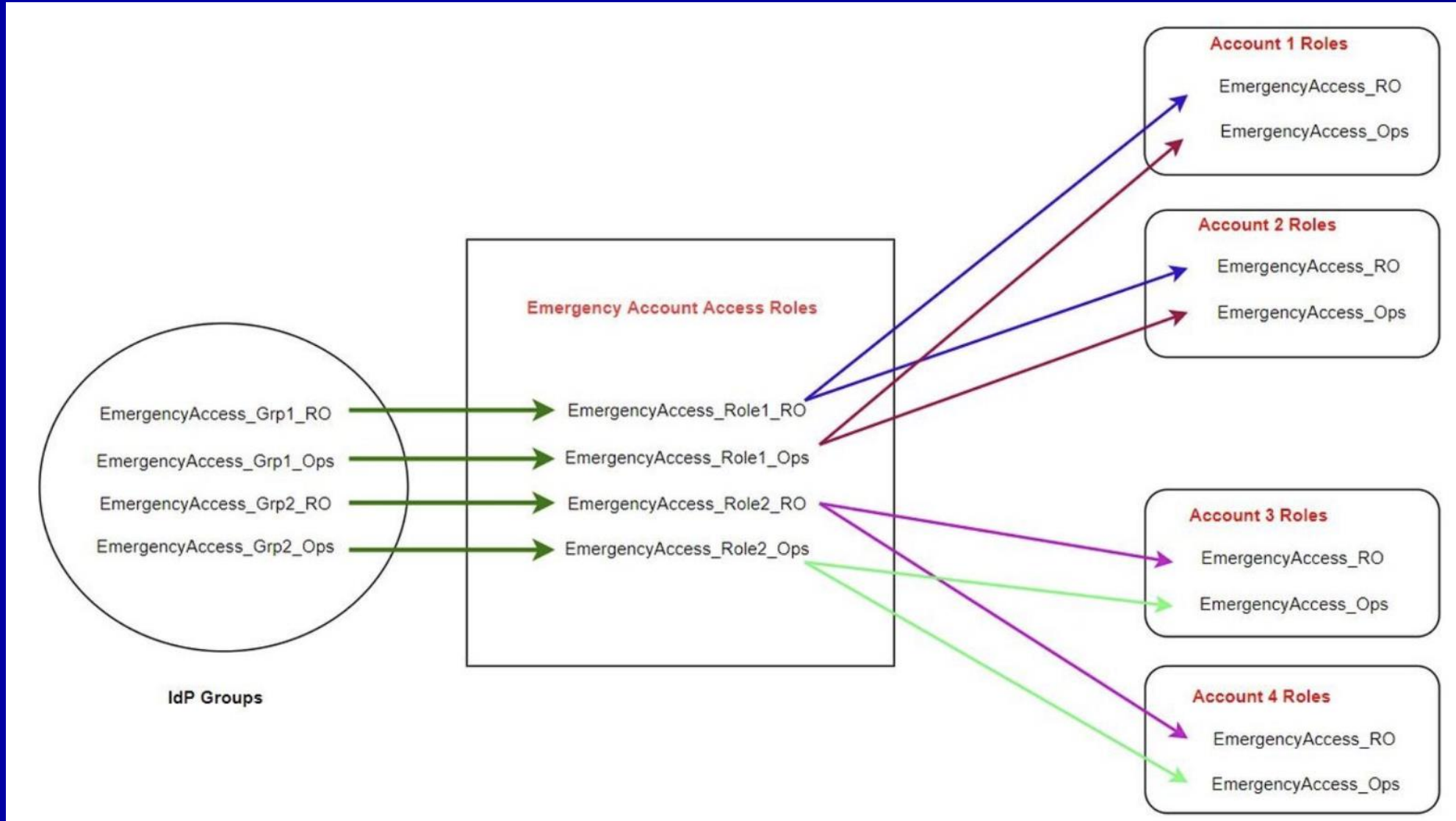
DR and resiliency



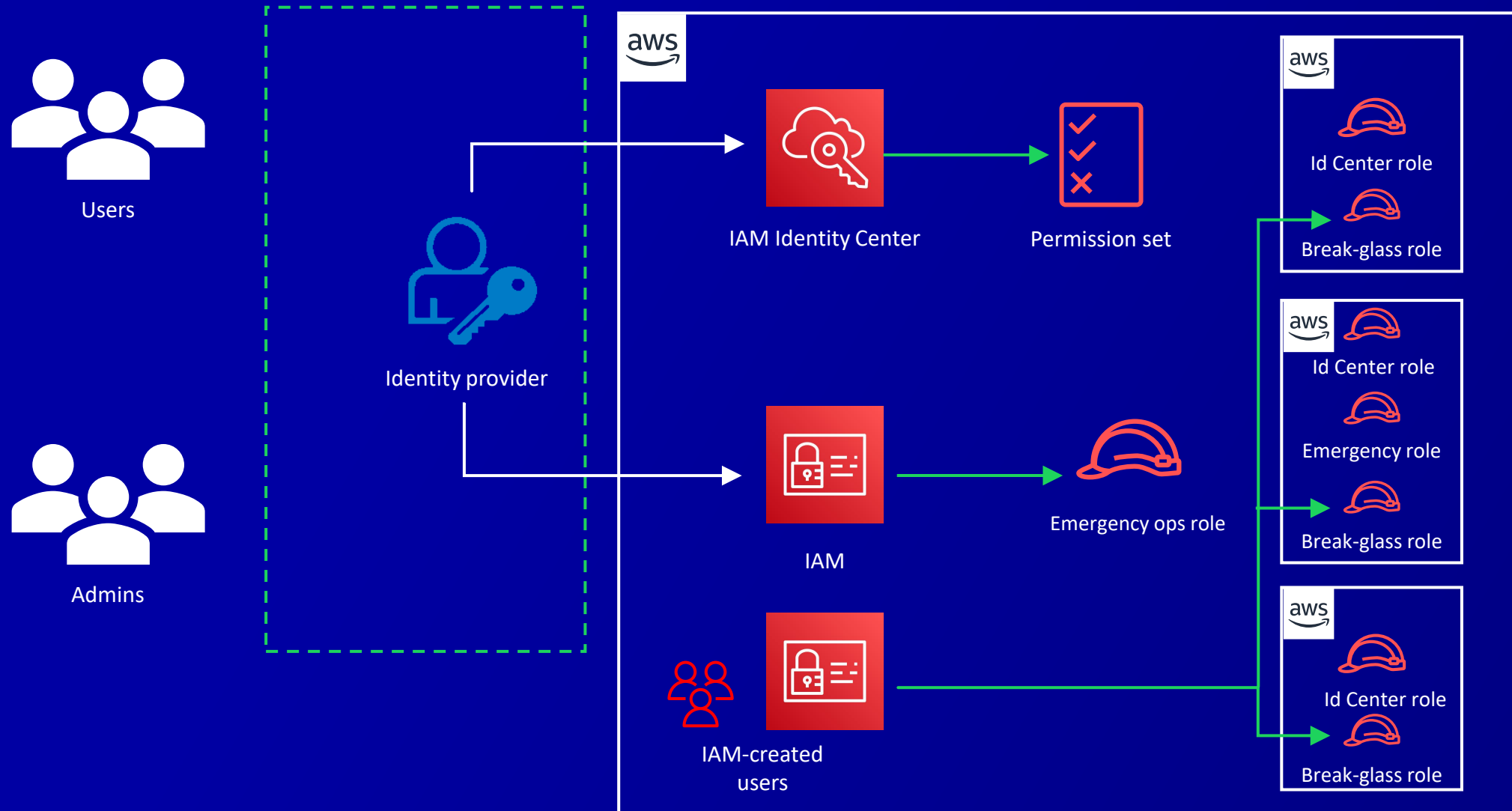
AWS IAM Identity Center DR scenario



AWS IAM Identity Center DR scenario



IdP DR scenario



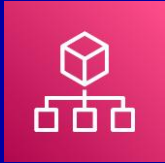
AWS identity services help you better secure a variety of workloads

Applications running on AWS

Use fine-grained access controls to grant employees, devices, and applications the access needed to AWS services and resources



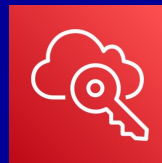
AWS Control Tower



AWS Organizations



IAM



IAM Identity Center



AWS Resource Access Manager (AWS RAM)



AWS Directory Service



Amazon Cognito

Hybrid workload deployments

Create or connect to an existing identity source to establish a single identity and access strategy across your on-premises and AWS environments

Customer-facing web and mobile applications

Create a simple, secure, scalable, and standards-based sign-up and sign-in customer experience for your applications

Thank you!

Djamel Bourokba

Sr. Global Solutions Architect –
Automotive

 @dbourokba

Steve Vinsik

Sr. Manager, Product Management –
Workforce Identity

