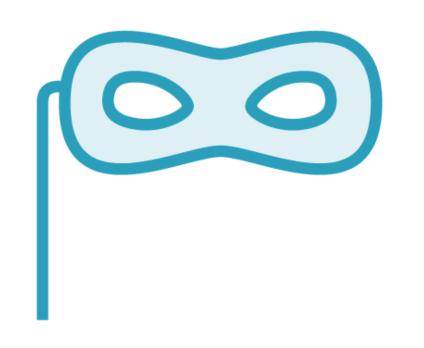
IAM Role Switching and Identity Federation



Saravanan Dhandapani SOFTWARE ARCHITECT

@dsharu

Why Identity Federation?



Leverage organization's current access control

Ease the cloud migration process

SAML based identity federation

- Security Assertion Markup Language

Non-SAML based identity federation using AWS managed Microsoft AD

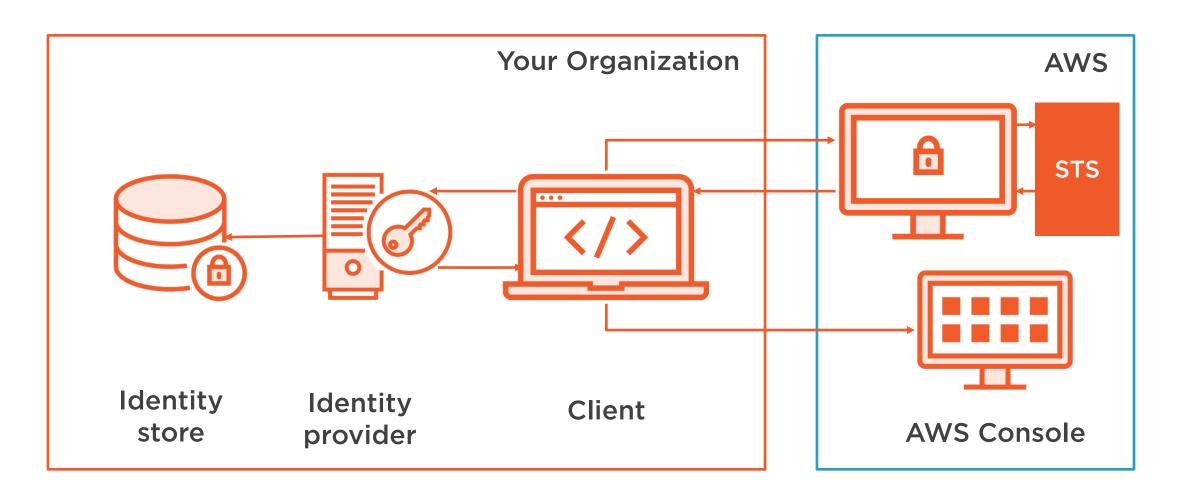


Sample SAML Document

```
<saml:Response>
 <saml:lssuer>http://idp.example.com/metadata.php</saml:lssuer>
 <saml:Status>
  <saml:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
 </saml:Status>
 <saml:Assertion>
 <saml:lssuer>http://idp.example.com/metadata.php</saml:lssuer>
 <ds:KeyInfo>
 <ds:X509Data>
  <ds:X509Certificate>MIICa...ROMASTWNg==</ds:X509Certificate>
 </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject><saml:NameID>_ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
  </saml:Subject>
  <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
  </saml:Conditions>
<saml:AttributeStatement>
   <Saml:Attributes>
  </saml:AttributeStatement>
 </saml:Assertion>
</saml:Response>
```

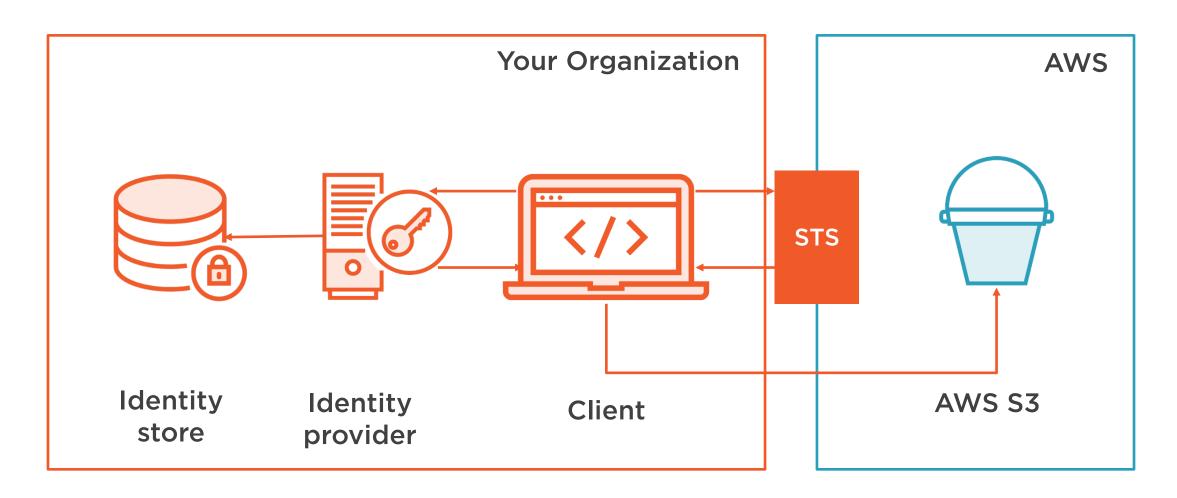


Enabling SSO to AWS Console





API Access to AWS from Client App





Corporate Identity Federation Use Cases

AssumeRole

GetFederation tokens

Client Application

AssumeRolewithSAML API

SAML compliant identity provider



Web Identity Federation



Web Identity Federation

Web/mobile applications leverage authentications provided by Google/Facebook/Amazon

Web identity federation playground

- Behind the scenes federated access



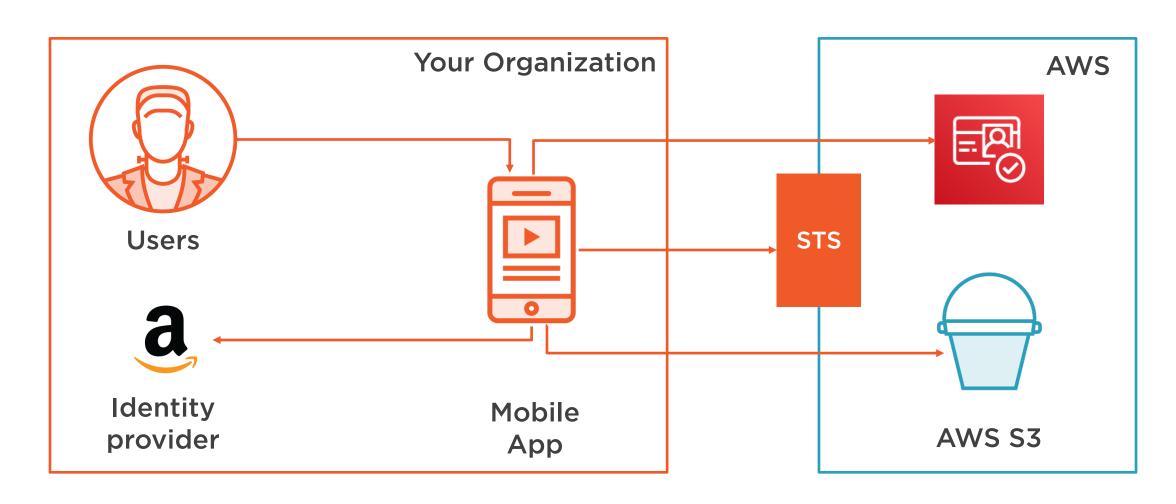
Demo



Web identity federation playground



Web Identity Federation





IAM Role Switching



IAM Role Switching



Minimize the complexity of managing multiple AWS accounts

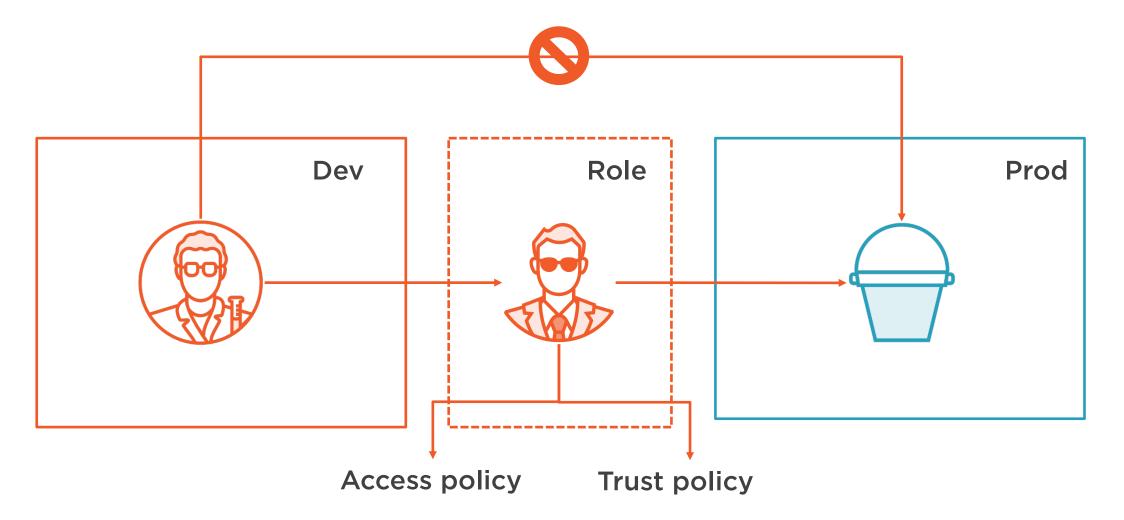
Switching to other AWS accounts using IAM role

Create a custom IAM policy to fine tune the permission

Can be achieved from AWS console/CLI/API



IAM Role Switching



Delegating the Access across AWS Accounts



Demo



Give read only access to a production resource



Optimize costs using AWS Trusted Advisor and CloudWatch Billing

