Security Service

Identify Management

IAM

User

Group

Policy

Role

STS

Monitor

Policy Sample

IAM Policy

```
{
  "Version": "2012-10-17",
  "Id": "S3-Account-Permissions",
  "Statement": [{
    "Sid": "1",
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::mybucket",
      "arn:aws:s3:::mybucket/*"
    ]
  }]
}
```

Trust Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "elasticmapreduce.amazonaws.com",
          "datapipeline.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IAM Role

Service

- Perform action on your behalf
- Only work within AWS account
- Service role for EC2

Delegation

- Cross-Account within AWS account

Federated

- External Access
- SAML2.0 Federation
- Web Identify Federation

IAM Monitor

Credential Report

- Anything about credential
- Login 、logout
- Password changed

Access Advisor

- Monitor usage of policy
- User, Group

  Role or policy level

CloudTrail

- Record all activities
- AWS management console

  CLI tools, SDKs,

  other AWS service

AWS Trusted Advisor

- Recommendation tools
- Security, Performance

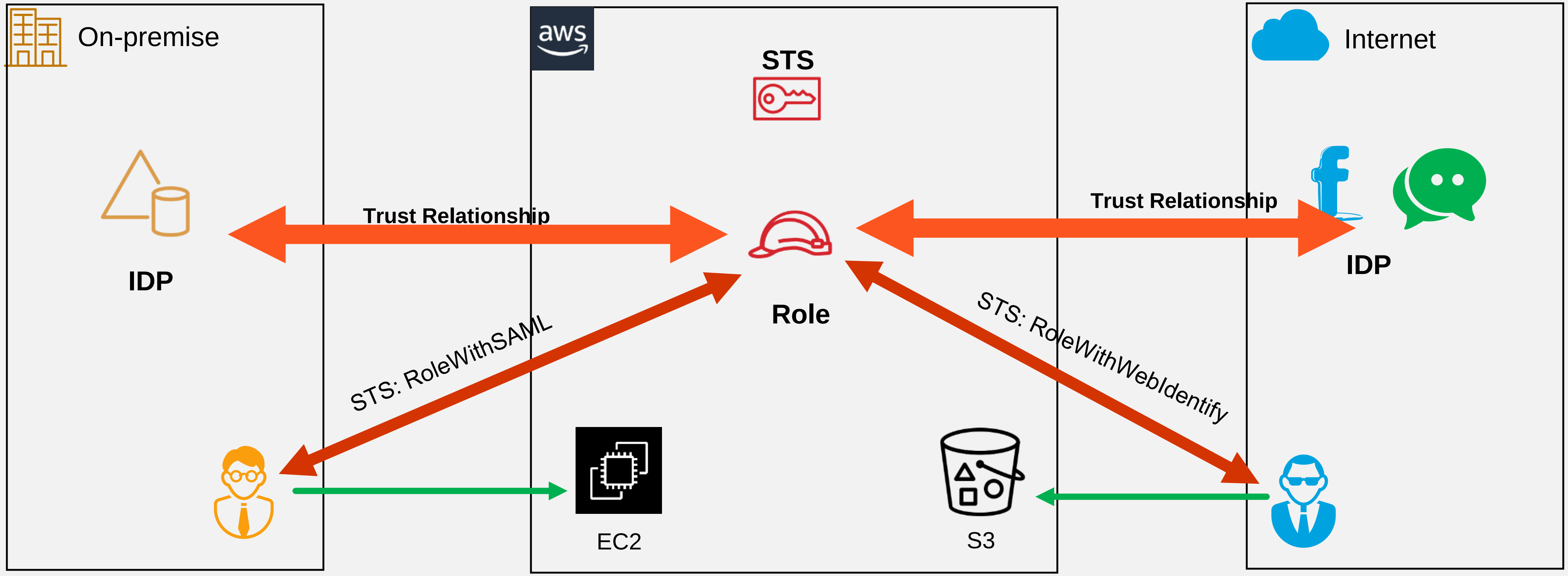
  Cost

AWS Config

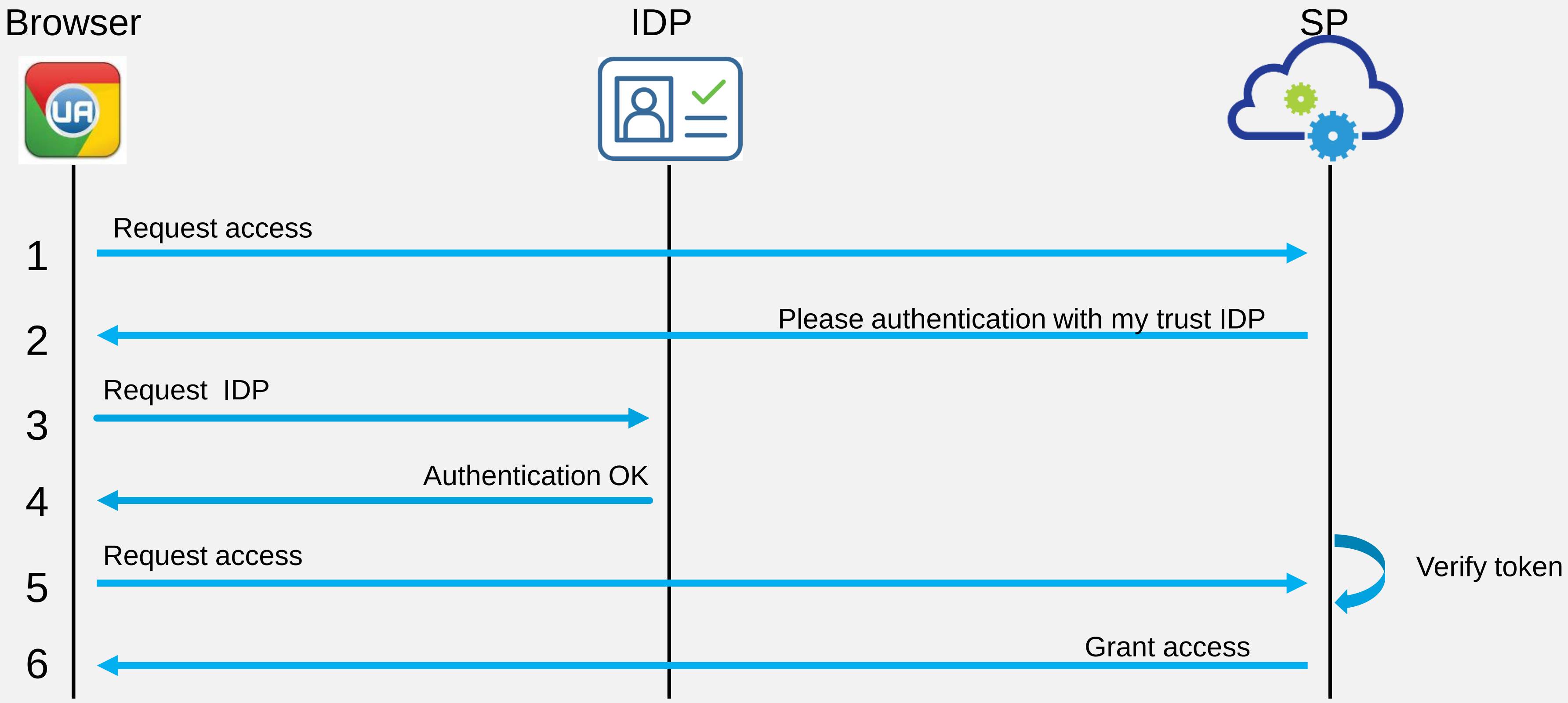
- Enforce requirements
- Assess , Audit, Evaluate

  on resource

Federation Usage



Claim-Based Workflow



Browser

IDP

SP

1 Request access

2 Please authentication with my trust IDP

3 Request IDP

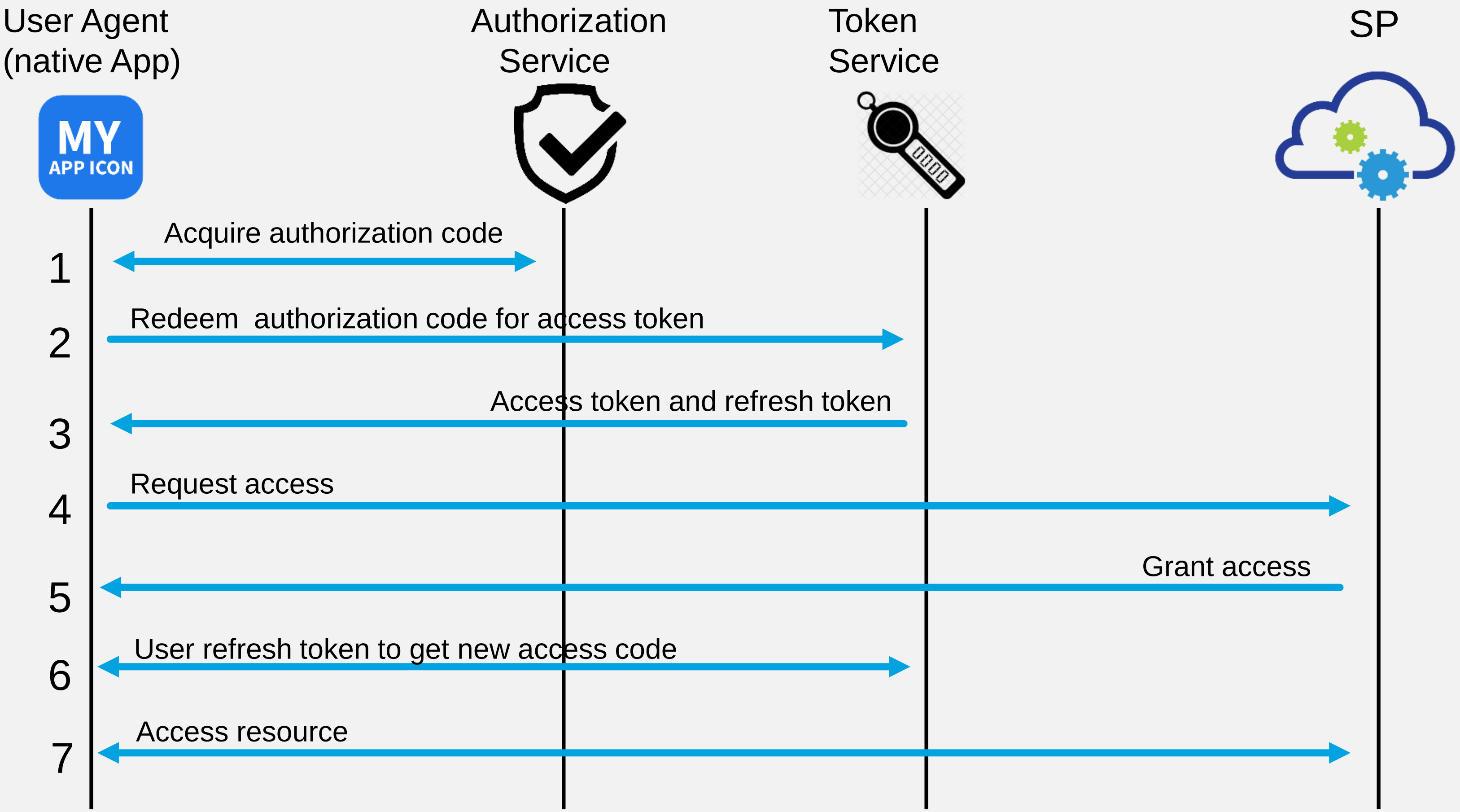
4 Authentication OK

5 Request access

Verify token

6 Grant access

Native Client Workflow


User Agent (native App)
MY APP ICON
Authorization Service
Token Service
SP
1
Acquire authorization code
2
Redeem authorization code for access token
3
Access token and refresh token
4
Request access
5
Grant access
6
User refresh token to get new access code
7
Access resource

Identity Service

IAM	Azure AD
AWS Organization	Azure Policy
AWS Directory Service	Azure Active Directory Domain Services
Cognito	Azure Active Directory B2C
AWS	Azure

AAD Feature

Access View

External Access

Self-Service Password

Self-Service Group

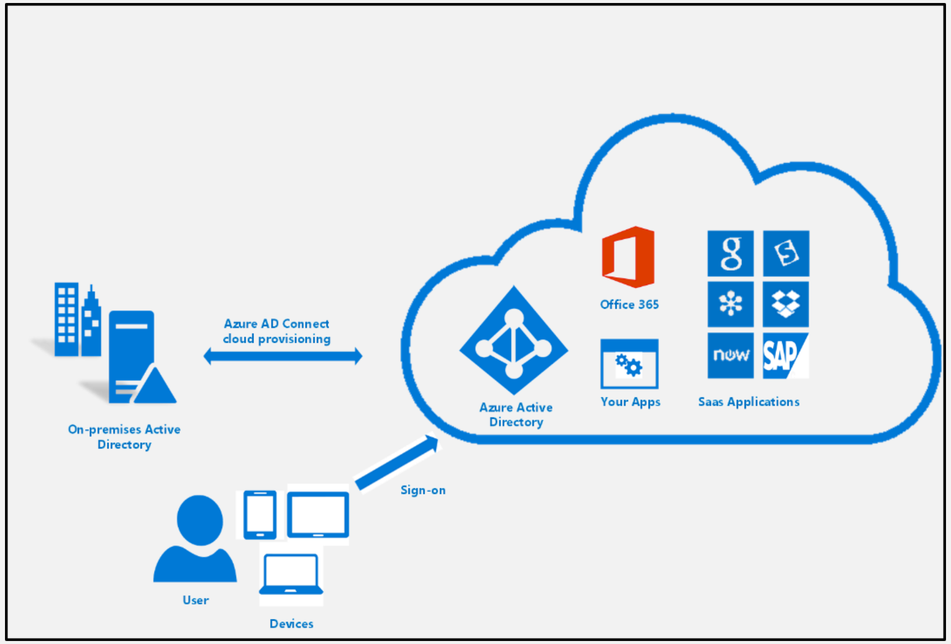
Access Panel

Conditional Access

AAD Component

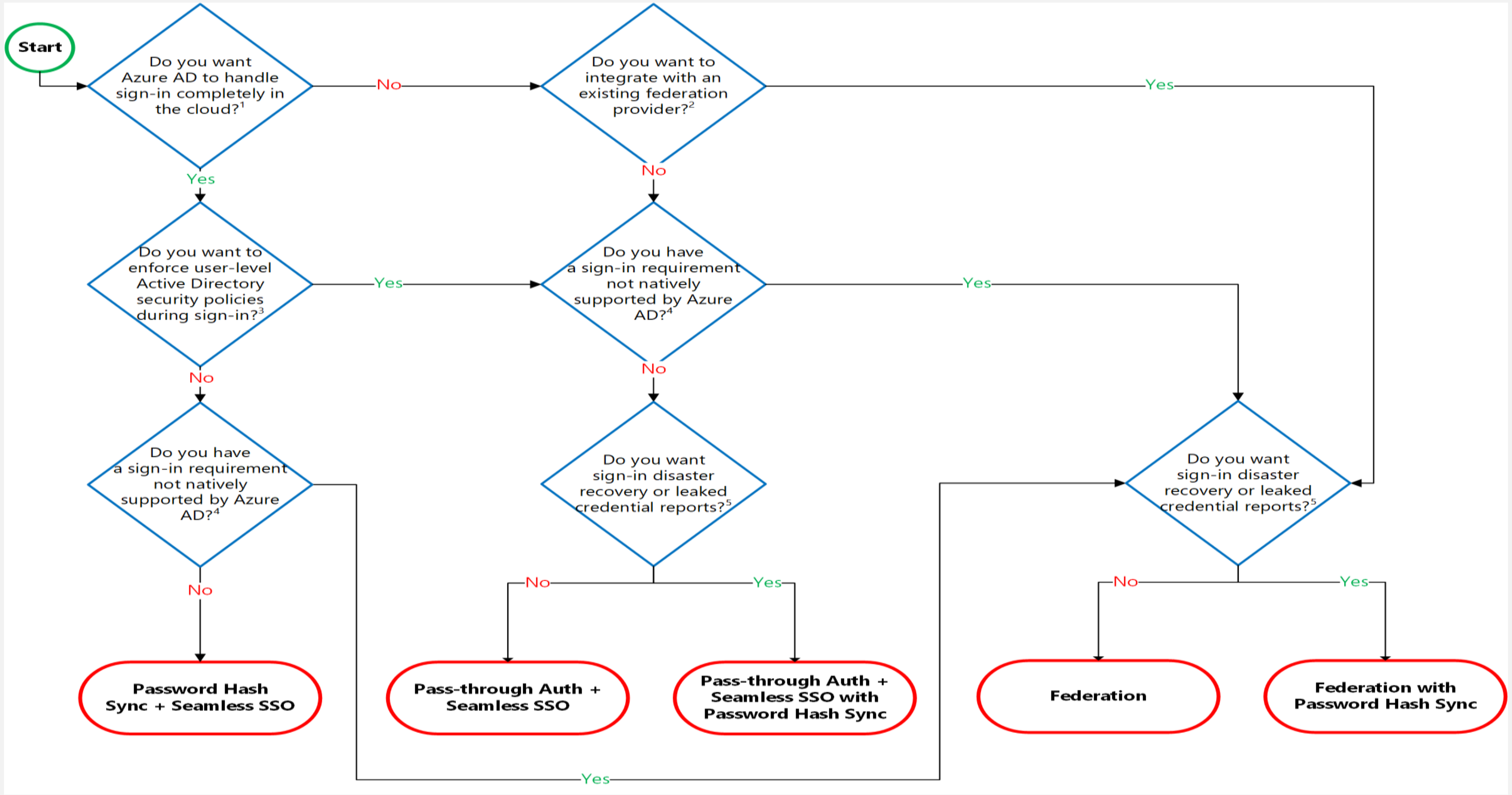
- Tenant
- Domain
- User
- Group
- Device
- Application

AD Connect



- Password hash synchronization
- Pass-through authentication
- Federation with ADFS

Decision Tree


Start
Do you want Azure AD to handle sign-in completely in the cloud?1
No
Do you want to integrate with an existing federation provider?2
Yes
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
Do you have a sign-in requirement not natively supported by Azure AD?4
Yes
No
No
Do you have a sign-in requirement not natively supported by Azure AD?4
Do you want sign-in disaster recovery or leaked credential reports?5
Do you want sign-in disaster recovery or leaked credential reports?5
No
No
Yes
No
Yes
Password Hash Sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth + Seamless SSO with Password Hash Sync
Federation
Federation with Password Hash Sync
Yes

Azure AD Comparison

AAD	AD
Multi-tenant	Single-tenant
AD Graph API for query	LDAP for query
SAML, OAuth, WS-Federation for authentication	Kerberos for authentication
RBAC	OU and Group Policy

Data Security

Security Solution

Key Management Service

CloudHSM

Server-side encryption with KMS

AWS

Azure Storage Service Encryption

Azure Key Vault

Azure

Data Protection

- At-Rest
- In-Transit
- In-Use

Data Encryption

- Azure Disk Encryption
- Key Management System vs Azure Key Vault
- SQL Transparent Data Encryption(at-rest)
- SQL Column-Level Encryption(in-use)

Access Control

- Shared Access Signatures(SAS)
- SQL access security mode
- Azure AD

Data Reliability

- LRS、ZRS、GRS、RA-GRS
- Azure Backup
- Site Recovery

Network Security

Security Solution

NSG & WAF	NSG & WAF
Inspector	Security Center
GuardDuty	Azure Advanced Protection
AWS Shield	Azure DDos Protection Service
AWS	Azure