Section 23) Advanced Identity

STS( Security Token Service) Overview

**STS: allow to get temporary access**

Machine generated alternative text:
AWS STS — Security Token Service 
STS 
• Allows to grant limited and temporary access to AWS resources (up to I hour). 
• AssumeRole: Assume roles within your account or cross account 
• AssumeRoIeWithSAML• return credentials for users logged with SAML 
• AssumeRoleWithWebldentity 
• return creds for users logged with dP ogin, Google Login, OIDC compatible... ) 
• ANS recommends against using this, d Pools instead 
• GetSessionToken: for MFA, from a r or A account root user 
• GetFederationToken: obtain temporary creds for a federated user 
• GetCallerldentity. return details about the IAM user or role used in the API call 
• DecodeAuthorizationMessage: decode error message when an AWS API is denied 

The **sts**:**AssumeRole** action is the means by which such temporary credentials are obtained. To use it, a user or application calls this API using some already-obtained credentials, such as a user's fixed access key, and it returns (if permitted) a new set of credentials to act as the role

Machine generated alternative text:
Using STS to Assume a Role 
• Define an IAM Role within your 
account or cross-account 
• Define which principals can access 
this IAM Role 
• Use AWS STS (SecurityToken 
Service) to retrieve credentials d 
impersonate the IAM Role you 
have access to (AssumeRole API) 
• Temporary credentials can be valid 
between 15 minutes to I hour 
Role (same or 
other account) 
AssumeRole API 
temporary 
security 
credential 
o 
AWS STS 
permissions 

Machine generated alternative text:
Cross account access with 
STS 
Development Acccnsnt 
Group: Testers 
Group: 
2_ Admin grants members ofthe 
group Developers permission to 
assume the role 
Production Account 
1. Admin creates role that grants 
Development account read/write 
access to productionapp bucket 
3 
to role 
S, User u es 
product ionapp 
by using the role 
credentials 
htt 
Role: Vpda 
Amazon S3 bucket: 
docs.aws.amazo 
ommon-scenarios aws-accounts.html 
m IAM atest UserGuide Id roles 

Machine generated alternative text:
STS with MFA 
• Use GetSessionToken from STS 
• Appropriate IAM policy using 
IAM Conditions 
• aws:MultiFactorAuthPresent.true 
• Reminder, GetSessionToken 
returns: 
• Access ID 
• Secret Key 
• Session Token 
• Expiration date 
"Ve rs ion 
"2ø12-1ø-17", 
"Statement": 
"Effect": "Allow", 
"Action": 
"ec2:StopInstances " , 
"ec2:TerminateInstances" 
"Resource": 
"Condition": 
"Boot": 
"aws:MultiFactorAuthPresent": 
"true" 

**Advanced IAM**

**Note : if we want to access dynamodb but explicit deny policy win first**

**Note : explicit deny has higher policy then explicit allow**

Machine generated alternative text:
Advanced IAM - Authorization Model 
Evaluation of Policies, simplified 
If there's an explicit DENY, end decision and DENY 
2. If there's an ALLOW, end decision with ALLOW 
3. Else DENY 
Final 
decision 
"deny" 
No 
Allow? 
Yes 
Final 
decision 
"allow" 
Decision 
starts at 
DENY 
Evaluate all 
Explici 
applicable 
Deny? 
Policies 
Yes 
Final 
decision : 
"deny" 

Machine generated alternative text:
IAM Policies & S3 Bucket Policies 
• IAM Policies are attached to users, roles, groups 
• S3 Bucket Policies are attached to buckets 
• When evaluating if an IAM Princip perform an operation X on a 
bucket, the union of its and Bucket Policies will 
S3 Bucket 
IAM Policy 
Policy 
Total Policy 
Evaluated 

**Imp:--**

Machine generated alternative text:
Example I 
• IAM Role attached to EC2 instance, authorizes RW to "my bucket" 
• No S3 Bucket Policy attached 
• EC2 instance can read an 
-•••to y_bucket" 

Machine generated alternative text:
Example 2 
• IAM Role attached to EC2 instance, authorizes RW to "my bucket" 
• S3 Bucket Policy attached, explicit deny to the IAM Role 
• EC2 instance cannot rea an ••••rite o"my_bucket" 

Machine generated alternative text:
Example 3 
• IAM Role attached to EC2 instance, no S3 bucket permissions 
• S3 Bucket Policy attached, explicit RW allow to the IAM Role 
• EC2 instance can read an y_bucket" 

Machine generated alternative text:
Example 4 
• IAM Role attached to EC2 instance, explicit deny S3 bucket permissions 
• S3 Bucket Policy attached, explicit RW allow to the IAM Role 
• EC2 instance cannot read and write to "my_bucket" 

Machine generated alternative text:
Dynamic Policies with IAM 
• How do you assign each user a /home/Kuser» folder in an S3 bucket? 
• Option l: 
• Create an IAM policy allowing geo 
have access to /home/georges 
• Create an IAM policy allowing rah h access to /home/sarah 
• Create an IAM policy allowing a 
c 
One policy per used 
• This doesn't scale 
• Option 2: 
• Create one dynamic policy with IAM 
• Leverage the special policy variable 
ccess to /home/matt 

Machine generated alternative text:
Dynamic Policy example 
/ home/ S aws : username) / * " 
"Sid": 
"AllowA11S3Action 
"Effect" : "Allow" , 
"Resource" 
n serFol 
: my ompa 

**Imp:**

Machine generated alternative text:
Inline vs Managed Policies 
• AWS Managed Policy 
• Maintained by AWS 
• Good for power users and administrators 
• Updated in case of new service 
• Customer Managed Policy 
ed'€o principals 
• Best Practice, re-usable, can be PI, 
• Version Controlled + rollback central-chånge management 
• Inline 
• Strict one-to-one relationship between policy and principal 
• Policy is deleted if you delete the IAM principal 

**Aws and customer managed policy**

Machine generated alternative text:
Identity and Access 
Management (IAM) 
Dashboard 
Access management 
Groups 
Users 
Roles 
Policies 
Identity providers 
Account settings 
Access reports 
Access analyzer 
Archive rules 
Analyzers 
Settings 
Credential report 
Organization activity 
Service control oolicies 
Create policy 
Filter policies 
POLICY TYPE 
Policy actions 
Q Search 
Reset filters 
Type 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Customer managed 
Used as 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Permissions policy (1) 
Description 
Policy used in trust relationship with CodePipeline 
Customer managed (25) 
AWS managed (714) 
AWS managed - job function (10) 
POLICY USE 
Used for permissions (55) 
Used for boundary (0) 
Not used (694) 
AWSLambdaBasicExecutio... 
AWSLambdaBasicExecutio... 
AWSLambdaBasicExecutio... 
AWSLambdaBasicExecutio... 
C) 
C) 
C) 
C) 

**Granting a user permission to pass a role to an AWS Service**

Machine generated alternative text:
Granting a User Permissions to Pass a Role to 
an AWS Service 
• To configure many AWS services, you must pass an IAM role to the service 
(this happens only once during setup) 
• The service will later assume the role and perform actions 
• Example of passing a role: 
• To an EC2 instance 
• To a Lambda function 
• To an ECS task 
• To CodePipeIine to allow it to invoke 
rvices 
• For this, you need the IAM permission iam:PassRole 
• It often comes with iam:GetRole to view the role being passed 

Machine generated alternative text:
Can a role be passed to any service? 
• No: Roles can only be passed to what their trust allows 
• A trust policy for the role that allows the service to assume the role 
"Version 
"Statement 
"2ø12-1ø-17", 
"Sid": "TrustP01icyStatem t 
"Effect 
"Allow", 
"Principal": 
"Service": "ec2.amazonaws.com" 
"Action": 
38 people have written a note here. 
2ServiceToAssumeTheAttachedR01e" , 

Machine generated alternative text:
aws 
Identity and Access 
Management (IAM) 
Identity providers 
settings 
Access reports 
Resource Groups 
e role 
Q Search 
AWS 
AWS 
AWS E2 
AWS 
ES•tzkS 
AWS 
datx 
323 days 
4 days 
Globa Support 
81 results 
38 people have written a note here. 

**Note : to pass a role we need to create correct trust relationship**

Machine generated alternative text:
Edit Trust Relationship 
"Ver s ion" 
• -zø12-rø-17-, 
"Statement" : L 
"Effect" : 
-principal": 
"Service" : - 
"Action": -Sts: 

**Directory Service Overview**

**Active Directory** stores information about objects on the network and makes this information easy for administrators and users to find and **use**. **Active Directory uses** a structured data store as the basis for a logical, hierarchical organization of **directory** information.

Machine generated alternative text:
What is Microsoft Active Directory (AD)? 
• Found on any Windows Server 
with AD Domain Services 
• Database of objects: User 
Accounts, Computers, Printe 
File Shares, Security Groups 
• Centralized security 
management, create account, 
assign permissions 
• Objects are organized in trees 
• A group of trees is a forest 
Domain Controller 
John 
Password 

Machine generated alternative text:
AWS Directory Services 
• AWS Managed Microsoft AD 
• Create your own AD in AWS, manage users 
locally, supports MFA 
• Establish 'trust" connections with your on- 
premise AD 
• AD Connector 
auth 
On-prem AD 
trust 
proxy 
auth 
MS 
AWS Managed AD 
auth 
AD Connector 
Simple AD 
• Directory Gateway (proxy) to redirect to on- 
premise AD 
• Users are managed on the on-premise AD 
On-prem AD 
• Simple AD 
• AD-compatible managed directory on AWS 
• Cannot be joined with on-premise AD 

Machine generated alternative text:
awS 
Resource Groups 
Directory Service Directories Setup a directory 
tmland 
Step 1: 
Select directory type 
Step 2: 
Enter directory 
information 
Step 3' 
Choose VPC and subnets 
Step 4: 
Review & create 
Select directory type 
Directory types 
O 
O 
o 
AWS Managed Microsoft AD 
Simple AD 
AD Connector 
Amazon Cognito User pools 
AWS Managed Microsoft AD 
WiffAWS Managed Microsoft AD, you can easily 
enable your Active Directory-aware workloads and 
"'S resources to use mapaged actual Microsoft 
Aceve Directory in the AWS Cloud. Workload ex- 
ples include Amazon EC2, Amazon RDS for SQL 
Server, custom .NET applications, and AWS Enter- 
prise IT applications such as Amazon Workspaces. 
Learn more e 
View use cases 
Cancel 
Next 