Access management in cloud environments is critical for ensuring security, compliance, and operational efficiency. AWS offers robust tools and services to manage access to resources, including the AWS Security Token Service (STS). STS enables users to obtain temporary, limited-privilege credentials to access AWS resources securely without the need to share long-term credentials like IAM user access keys.

This document outlines the role assumption process using STS for accessing AWS cloud assets. It covers the following topics in detail:

1. Explanation of STS and its role in access management.
2. Step-by-step instructions on how to assume a role using STS, including adding users to Active Directory (AD) groups and executing aws\_sts.exe in the command prompt.
3. Discussion of the validity period of assumed roles and customization options.
4. Advantages of using STS for role assumption compared to traditional IAM role and policy creation methods.

By understanding and following this role assumption process, organizations can effectively manage access to AWS resources, mitigate security risks, and maintain compliance with regulatory requirements.

AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS services. It provides a way to grant users access to AWS resources without having to share long-term credentials like IAM user access keys. STS offers several methods for controlling access, including role assumption, federated access, and cross-account access.

2. How to Assume a Role

To assume a role in AWS using STS, follow these steps:

a. Add User to Active Directory (AD) Group: Ensure that the user is added to an Active Directory group that has the necessary permissions to assume the required role in AWS.

b. Execute aws\_sts.exe in Command Prompt:

Open a command prompt.

Run aws\_sts.exe to retrieve a list of available roles. This executable facilitates the role assumption process and presents a menu of roles for the user to choose from.

c. Select Role to Assume:

From the list of roles provided by aws\_sts.exe, select the role that corresponds to the permissions needed for the task or resource you want to access.

d. Assume Role:

Once the role is selected, follow the prompts to assume the role. This will generate temporary security credentials that can be used to access AWS resources within the defined permissions of the assumed role.

By default, the temporary security credentials obtained by assuming a role through STS are valid for one hour. However, the validity period can be customized based on the specific requirements of the access scenario. This flexibility allows organizations to balance security and usability according to their needs.

Advantages of STS Over Normal Role & Policy Creation

Using STS for role assumption offers several advantages over traditional methods of IAM role and policy creation:

Enhanced Security: STS minimizes the exposure of long-term credentials by providing temporary credentials that expire automatically.

Least Privilege Access: Role assumption through STS allows for fine-grained control over permissions, ensuring that users have access only to the resources necessary for their tasks.

Reduced Credential Management Overhead: Since temporary credentials are short-lived and automatically expire, there is less need for manual credential rotation and management.

Support for Federated Identity: STS enables federated access, allowing users from external identity providers to access AWS resources without the need for IAM users or roles.

Auditability and Compliance: Role assumption events are logged, providing visibility into who accessed which resources and when, facilitating compliance with regulatory requirements and security best practices.