Creating a step-by-step hands-on guide for using AWS Security Token Service (STS) involves demonstrating **how to assume roles, generate temporary security credentials, and access AWS resources securely.** Here's a detailed guide to get you started:

**Title: Hands-On Guide to Using AWS Security Token Service (STS)**

**Introduction:**

AWS Security Token Service (STS) is a critical AWS service that allows you to grant temporary, limited-privilege credentials to users or systems, enhancing security by minimizing long-term access. In this hands-on guide, you will learn how to use AWS STS to assume roles, generate temporary security credentials, and access AWS resources securely.

**Prerequisites:**

**1. An AWS account.**

**2. AWS Command Line Interface (CLI) installed and configured with appropriate IAM user credentials.**

**3. Basic knowledge of AWS Identity and Access Management (IAM).**

**Step 1: Create an IAM Role**

1.1. Sign in to the AWS Management Console.

1.2. Open the IAM console and navigate to "Roles."

1.3. Click "Create role."

1.4. Select "Another AWS account" and enter the Account ID that needs access. Optionally, you can set up a trusted relationship.

1.5. Attach permissions policies as needed.

1.6. Review and create the role.

**Step 2: Assume the IAM Role**

2.1. Open your terminal or command prompt.

2.2. Use the AWS CLI to assume the role:

|  |
| --- |
| aws sts assume-role --role-arn arn:aws:iam::ACCOUNT-ID-WITH-ROLE:role/ROLE-NAME --role-session-name YourSessionName |

Replace `arn:aws:iam::ACCOUNT-ID-WITH-ROLE:role/ROLE-NAME` with the role's ARN and choose a meaningful session name.

2.3. The command will return temporary credentials (Access Key, Secret Access Key, Session Token).

**Step 3: Configure AWS CLI with Temporary Credentials**

3.1. Configure the AWS CLI with the temporary credentials:

|  |
| --- |
| aws configure set aws\_access\_key\_id YOUR\_ACCESS\_KEY  aws configure set aws\_secret\_access\_key YOUR\_SECRET\_KEY  aws configure set aws\_session\_token YOUR\_SESSION\_TOKEN  aws configure set region YOUR\_AWS\_REGION |

Replace `YOUR\_ACCESS\_KEY`, `YOUR\_SECRET\_KEY`, `YOUR\_SESSION\_TOKEN`, and `YOUR\_AWS\_REGION` with the values obtained in step 2.3.

**Step 4: Test Access**

4.1. Run AWS CLI commands to access AWS resources with the assumed role permissions:

|  |
| --- |
| aws s3 ls # Example command to list S3 buckets  aws ec2 describe-instances # Example command to describe EC2 instances |

Ensure that you can perform actions allowed by the IAM role's policies.