



Annual General Security Training Science Managed Cloud Environment (SMCE)

Last Updated: 13 June 2022

Computational and Information Sciences and Technology Office (CISTO)

GSFC Code 606





Topics

- Acronyms
- User Agreements and Training Requirements
- Shared Security Model
- Roles and Responsibilities
- Authorization and Access
- ID, Password, and Key Expirations
- Allowable Types of Data
- Configuration Management
- Backups
- Incident Response
- User Agreement Attestation
- Project SysAdmin Training





Acronyms

| | | | |
|-------|---|------|---|
| ACG | A Cloud Guru | IAM | Identity and Access Management |
| AMI | Amazon Machine Image | ISSO | Information Systems Security Officer |
| API | Application Programming Interface | ITAR | International Traffic in Arms Regulations |
| ATC | AWS Training and Certification | MFA | Multi-Factor Authentication |
| AWS | Amazon Web Services | NIST | National Institutes of Standards and Technology |
| CIS | Center for Internet Security | PI | Principal Investigator |
| CUI | Controlled Unclassified Information | RHEL | Red Hat Enterprise Linux |
| CVE | Common Vulnerabilities and Exposures | S3 | Simple Storage Service |
| EC2 | Elastic Compute Cloud | SLES | SUSE Linux Enterprise Server |
| ECR | Elastic Container Registry | SOC | Security Operations Center |
| FISMA | Federal Information Management Security Act | SSM | Systems Manager |



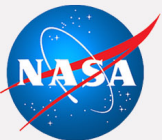


User Agreements and Training Requirements

| SMCE Agreement or Training Module | Who Should Take This | Time Frame |
|---------------------------------------|-----------------------------------|------------|
| User Agreement | All console users | Annually |
| General Security Training | All console users | Annually |
| Elevated Privileges Security Training | Project SysAdmins, CloudAdmins | Annually |

- Training is designed to help users understand current NASA security requirements and how they impact the operation of SMCE
- SMCE Users, PIs, and Project SysAdmins will need to work together with the SMCE CloudAdmin Team to implement good security practices

Security is everyone's responsibility!





Shared Security Responsibility Model

| Layer | SMCE CloudAdmins | Project SysAdmins |
|--------------------------|--|--|
| Application Layer | <ul style="list-style-type: none">Monitor application authentication for security compliance and provide recommendations for remediation | <ul style="list-style-type: none">Install/configure applications in a secure fashionCreate and update passwords to meet NASA guidelines |
| Container Layer | <ul style="list-style-type: none">Implement AWS Elastic Container Registry (ECR) for storage of approved Containers | <ul style="list-style-type: none">Store approved Containers in AWS Elastic Container Registry (ECR)Update Containers to resolve vulnerabilities shown in Inspector v2 |
| O/S Layer | <ul style="list-style-type: none">Monitor EC2 instances for security compliance and provide notifications for required patches | <ul style="list-style-type: none">Use SMCE supplied AMIsRead and understand vulnerabilities from weekly Inspector v2 reportsConfigure secure EC2 instances and implement patches as required |
| Cloud Layer | <ul style="list-style-type: none">Maintain Custom AMIs, and Monitor Password / API key age compliance | <ul style="list-style-type: none">Coordinate with the ISSO to ensure User Agreement is signed create IAM users |
| Physical Layer | <ul style="list-style-type: none">AWS provides secure facilities, hardware, and other capabilities | |

Roles and Responsibilities

Project Teams

SMCE Team

SMCE Management

Project vetting, SMCE funding and financials, operational oversight

SMCE Cloud Administrators

Cloud-layer administration, cloud operations, secure images, setup projects, cloud accounts, security scans, security compliance, etc.

SMCE Cloud Architects

Cloud-layer operational solutions, SMCE services, prototyping, consulting, some training, and more

SMCE Information Systems Security Officer

Maintain and implement security plan, cloud security operations, conduct training, maintain authorization to operate

Project End Users/Service Users

Users of the project's services (NO console access), as defined by the PI, must adhere to the project and/or service requirements

Project Principal Investigator

Responsible for all aspects of the project, including funding, defining the project system administrators, ensuring security requirements are met

Project System Administrators

Defined by the PI, operating system administration, must respond to SMCE Elevated Privileges Security Training

Project Console Users

Defined by the PI, access to AWS console, must adhere to SMCE User Agreement and General Security Training

SMCE Users

Any user of the SMCE, to include Project End/Service Users, PIs, Project Sysadmins, and Project Console Users

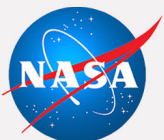


**RESTRICTED
AREA**

**AUTHORIZED
PERSONNEL
ONLY**

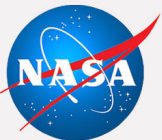
Authorization and Access

- All Project Console Users must request access through their Principal Investigator or Project SysAdmin
- The SMCE Information Systems Security Officer (ISSO) will provide the SMCE User Agreement and appropriate Security Training modules to those who request access
- Initial credentials will be provided to users by their Principal Investigator, Project SysAdmin, or one of the SMCE CloudAdmins after the User Agreement Attestation has been signed and returned to the ISSO
- The use of Multi-Factor Authentication (MFA) is required for AWS Console Access and all applications hosted on the SMCE
 - Applications that are not MFA-compliant must be part of a documented exception



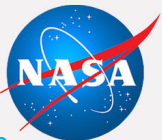
User ID, Password, and Key Expirations

- All passwords (for both AWS Console and Applications) must meet "strong" password guidelines, which requires:
 - A minimum of 12 characters
 - Each of the following character types:
 - Uppercase
 - Lowercase
 - Numbers
 - Special characters (! @ # \$ % ^ & * () <> [] {} | _+ -=)
 - Passwords should be different from your AWS account name or email address
 - Passwords should never be written down
- AWS Console Passwords and API Keys must be changed every 60 days or sooner, or they will be disabled
- API Keys must never be stored in a publicly-available repository
- Applications that are not compliant with these guidelines must be part of a documented exception



Allowable Types of Data

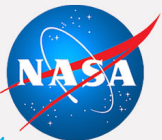
- All data in SMCE has been categorized as a Federal Information Security Management Act (FISMA) “Low”
- SMCE is an approved FISMA Low system, and is appropriate for the storage and processing of public data that is openly available
- Uploading of classified, CUI, ITAR, or other sensitive data to the SMCE is strictly prohibited

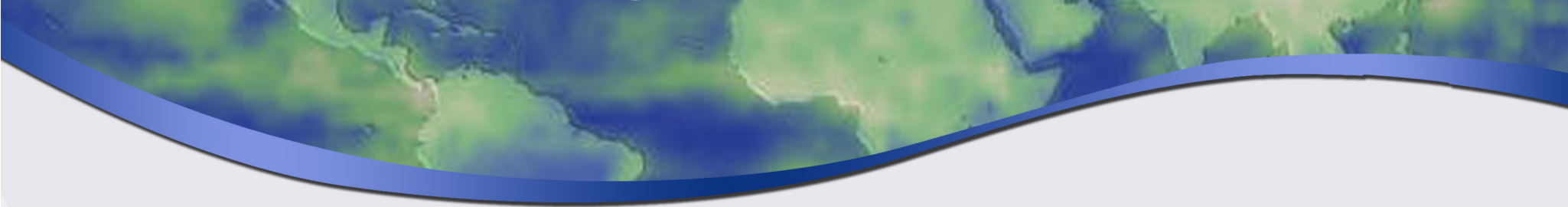




Golden Amazon Machine Images (AMI)

- SMCE System Administrators develop and maintain Golden Amazon Machine Images (AMI)
 - Golden AMIs are maintained by the SMCE team for:
 - Amazon Linux 2
 - CENTOS
 - RHEL
 - Ubuntu
 - SLES
 - Other operating systems (as necessary)
 - These AMIs are hardened images based on security best practices and the Center for Internet Security (CIS) benchmarks
 - They provide a more secure basis and starting point for creating new EC2 instances





Golden Amazon Machine Images (AMI) - Usage



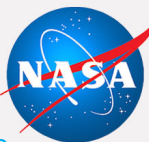
- Use of Golden AMIs is highly encouraged, as deviations may cause security non-compliance issues due to increased need for patching
 - The use of non-Golden AMIs can cause security issues if the underlying Operating System is no longer fully supported by the vendor
 - Keeping the instance patched will become problematic, and may eventually require shutdowns due to non-compliance issues
- The SMCE CloudAdmin team will provide a path for Project SysAdmins to upgrade their Operating Systems which are poorly supported by the vendor, and/or are planned for deprecation in the near future
- Examples of upgrade paths currently available via Golden AMIs are as follows:
 - Ubuntu 18.04 → Ubuntu 20.4 or Ubuntu 22.04
 - CENTOS7 → RHEL8





Systems Manager and Inspector v2

- The AWS Systems Manager agent (SSM) must be installed on all EC2 instances
 - Golden AMIs have Systems Manager pre-installed as part of the base image
 - AWS provides instructions for installing the SSM agent on all AWS-supported OSes at the following URL:
<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>
- With the SSM agent in place, vulnerabilities are continuously updated for each EC2 instance based on:
 - EC2 instance state
 - Installed packages
 - Changes by NIST to the current Common Vulnerabilities and Exposures (CVE) information
- **Note: EC2 instances without the SSM agent will need to be updated or shutdown within 48 Hours**





Backups of Customer Data

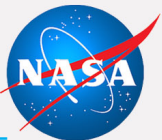
- Backups of customer data and disaster recovery are the responsibility of the PI and Project SysAdmins for each project
- PIs are encouraged to have a backup strategy for customer data stored within their individual project resources to ensure that regular backups are conducted
 - The absence of a backup strategy is suitable if the PI is OK with the potential loss of customer data due to unforeseen system outages
- SMCE CloudAdmins backup copies of Golden Amazon Machine Images (AMI) and any associated scripts used for automation capabilities
 - Golden AMIs and scripts are available for use by Project SysAdmins

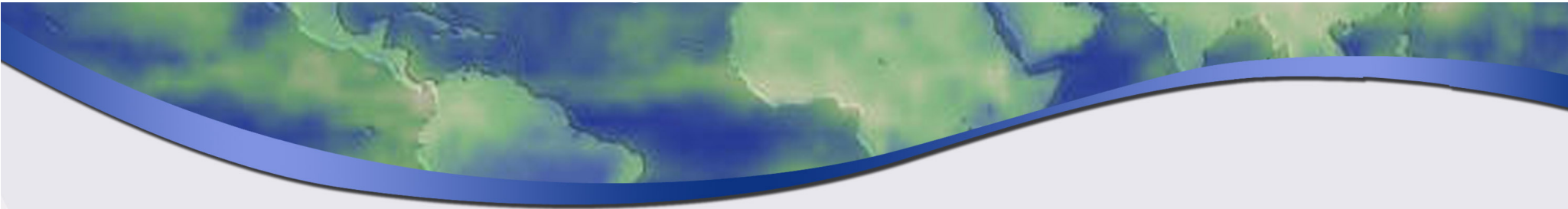


Incident Response



- If a security incident occurs, SMCE users will be required to fully and immediately cooperate with the SMCE ISSO, CloudAdmins, and Management Team
- If you think a security incident has occurred (or is occurring), SMCE users shall:
 - Leave systems as is and not terminate any instances
 - Immediately contact the SMCE ISSO or CloudAdmin team
 - Be available to perform any necessary remediation activities
 - Re-complete the annual SMCE security training and User Agreement attestation
- To assist NASA Security Operations Center (SOC) personnel, SMCE users will need to be available to respond to requests





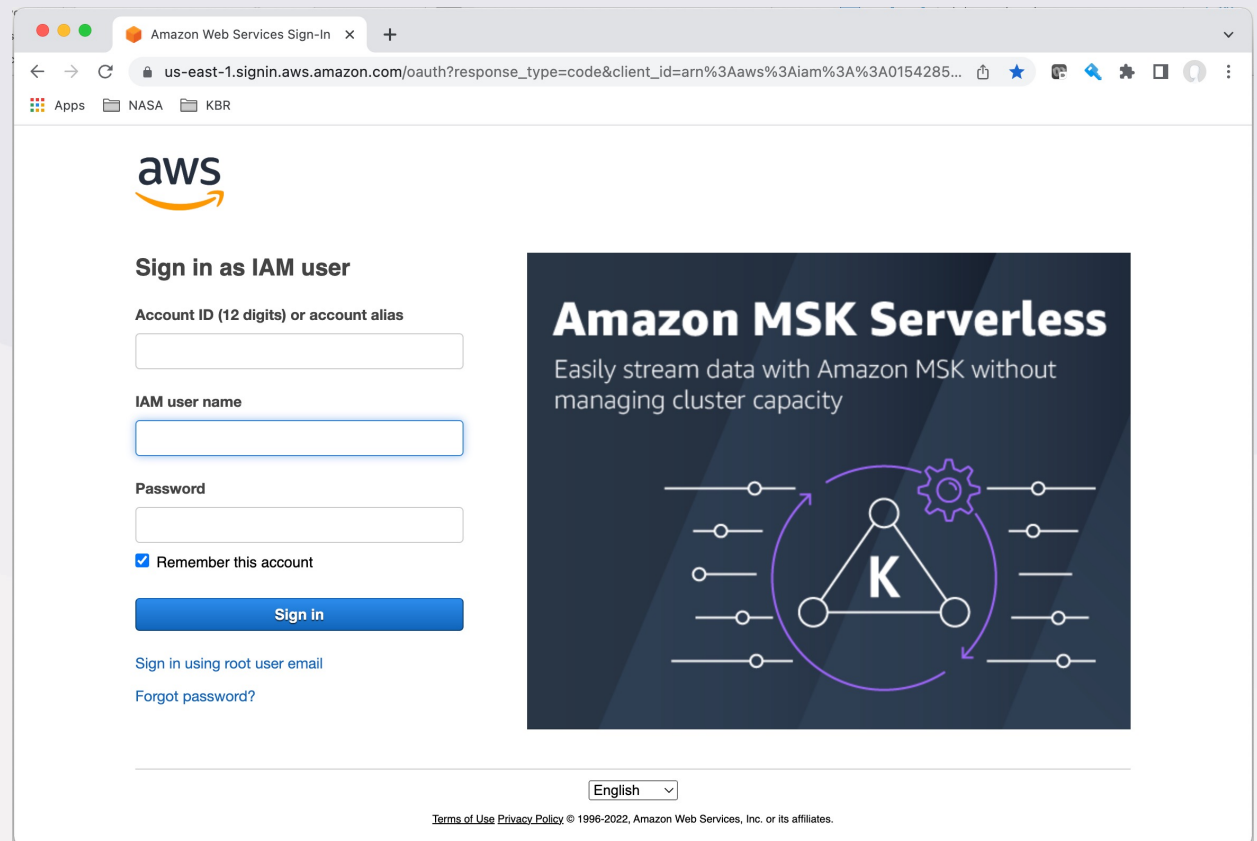
User Agreement Attestation

- The SMCE User Agreement:
 - Describes the security-related responsibilities and expected user behavior for each type of user
 - Promotes good security practices by ensuring the confidentiality, integrity, and availability of all SMCE resources
 - Assures that SMCE users with AWS console access have read and understand the Security training modules and the compliances to which are required for the type of access to be granted
- All SMCE users with AWS console access must attest to the SMCE User Agreement prior to accessing any SMCE resources, and annually thereafter

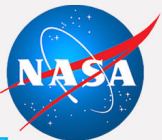


Project Sysadmin Training – Console Login/Password

- Initial login to AWS console will require:
 - Account ID/Project Name (e.g, smce-xxx)
 - IAM username (your assigned IAM username)
 - Password (provided password - must be changed after login)

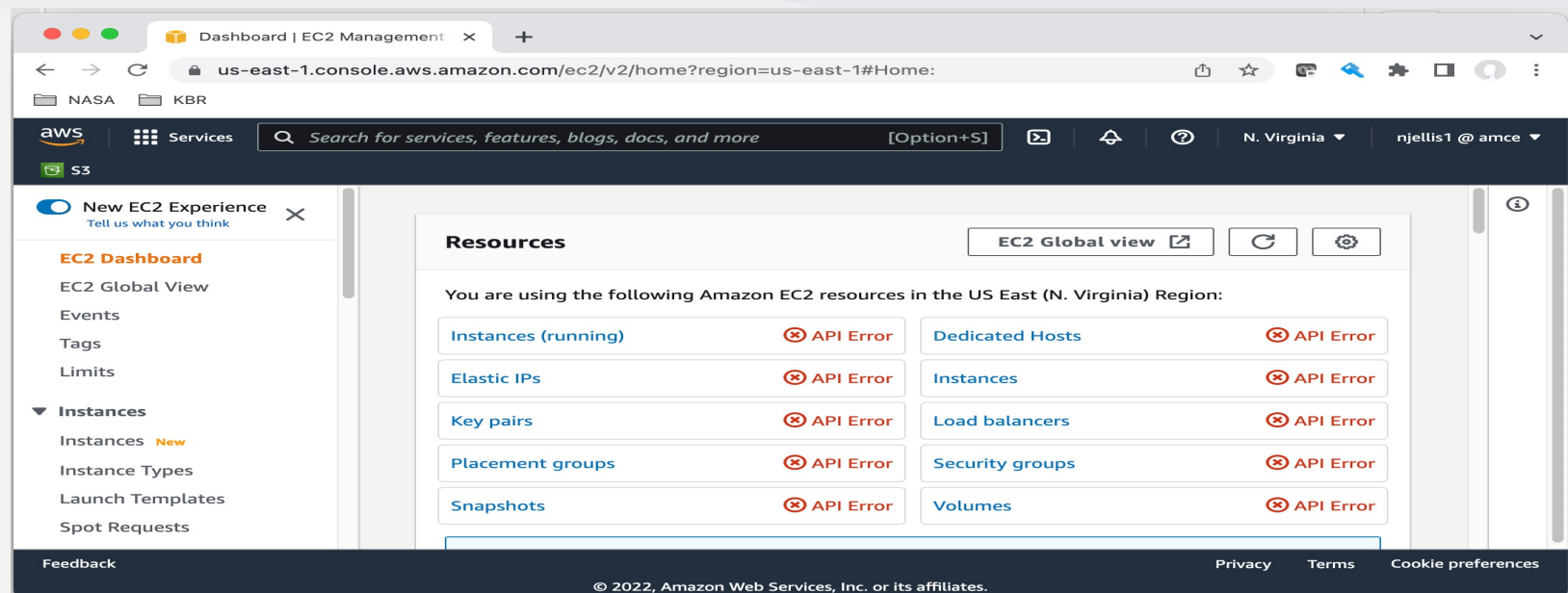


The screenshot shows the AWS IAM console login page in a web browser. The browser's address bar displays the URL: `us-east-1.signin.aws.amazon.com/oauth?response_type=code&client_id=arn%3Aaws%3Aiam%3A%3A0154285...`. The page features the AWS logo at the top left. Below it, the heading "Sign in as IAM user" is followed by three input fields: "Account ID (12 digits) or account alias", "IAM user name", and "Password". A checkbox labeled "Remember this account" is checked. A blue "Sign in" button is positioned below the password field. At the bottom of the login section, there are links for "Sign in using root user email" and "Forgot password?". On the right side of the page, there is a promotional banner for "Amazon MSK Serverless" with the text "Easily stream data with Amazon MSK without managing cluster capacity" and a diagram of a Kinesis cluster. At the very bottom, there is a language selector set to "English" and a small copyright notice: "Terms of Use Privacy Policy © 1996-2022, Amazon Web Services, Inc. or its affiliates."



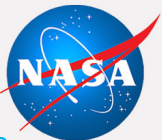
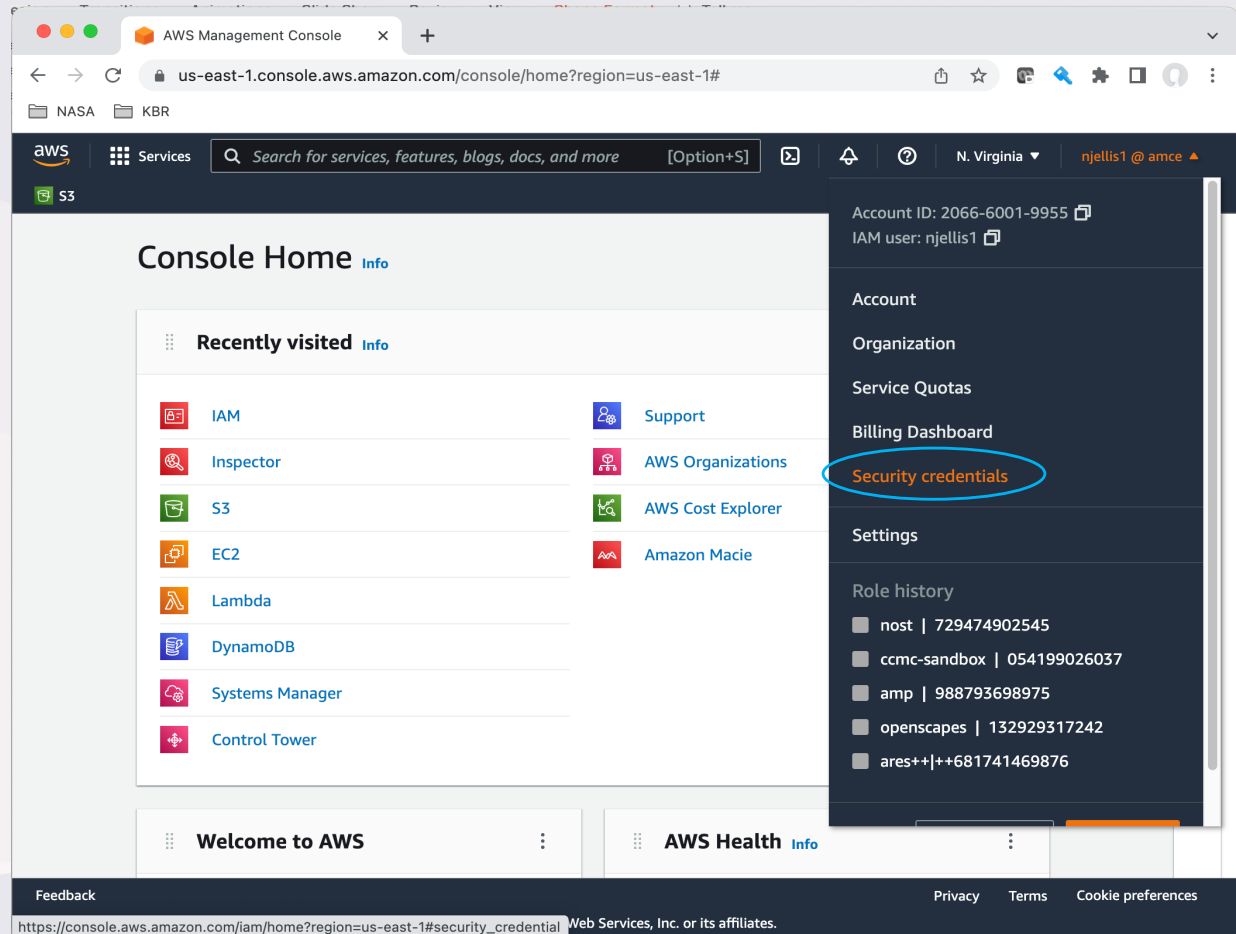
Project SysAdmin Training – Requirement for MFA

- For compliance with our NASA security profile, all users will need to set up Multifactor Authentication (MFA) for logging into the AWS Console
- The preferred application for SMCE is Google authenticator, which can be downloaded and set up on your cellular phone from the Android or iPhone App store
- Note: If you log in with just the normal username and password, you might see messages in the EC2 dashboard like "API Error" (see below) or error messages on the IAM dashboard after you get to the initial AWS console page. **This is expected behavior until MFA is set up.**



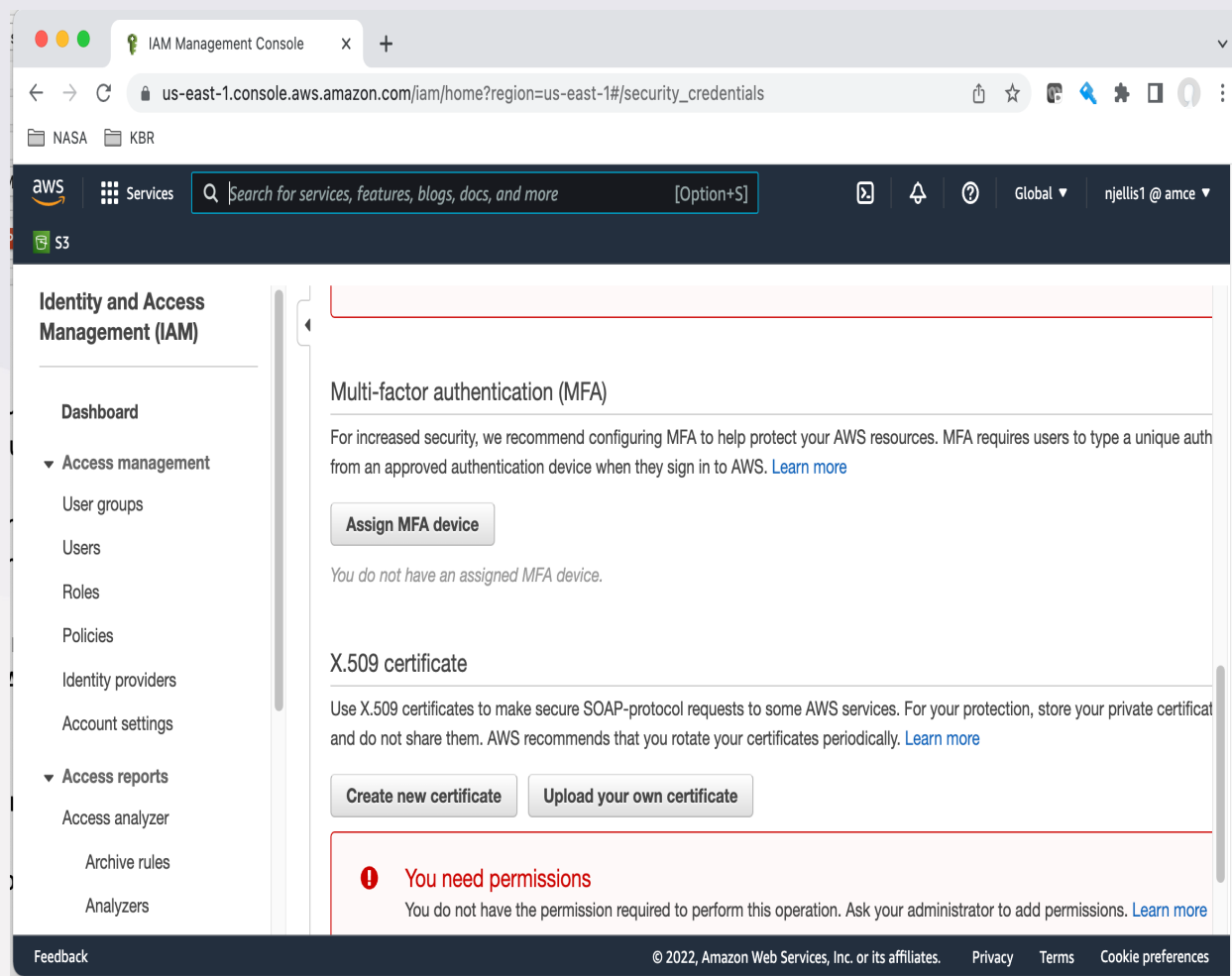
Project Sysadmin Training – Setting up MFA

- From the console page, you'll need to go to the top right corner and click on the part of the menu bar that is in white and says something like <your username@team name>. Then **Click on "Security Credentials"** (circled below in blue) to bring up a new page.
- On your phone, download and install *Google Authenticator* via the [app store if Apple](#) or [play store if Android](#)



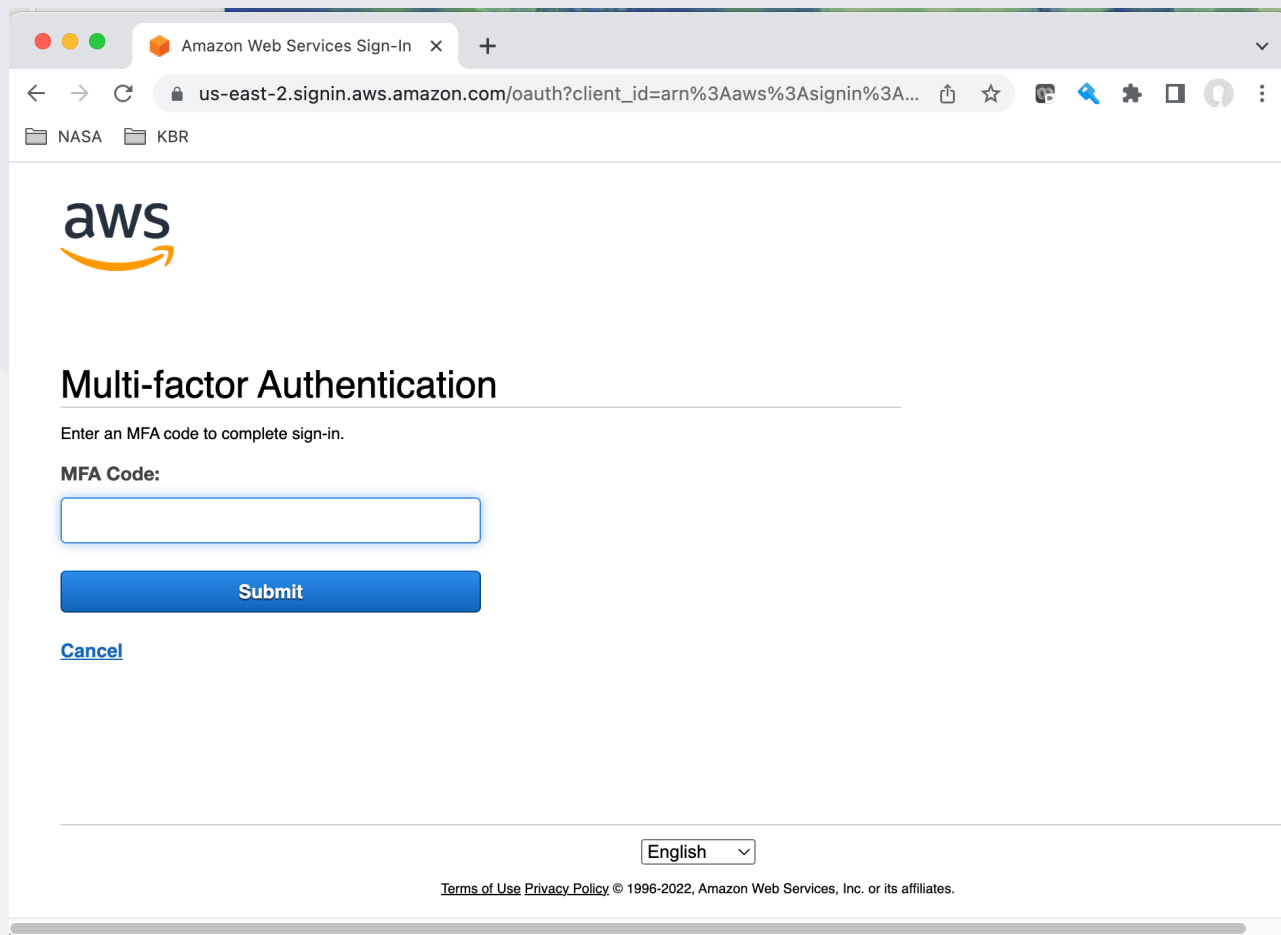
Project Sysadmin Training – Setting up MFA (cont.)

- On the IAM user page, scroll down to the section that says "*Multi-factor authentication (MFA)*" and click "**Assign MFA Device**"
- Using your phone, click to show the QR code and then use the Google Authenticator app to read the QR code shown.
- You'll then need to enter the next two 6-digit codes that appear in Google Authenticator. Enter the first one that appears. Wait until a different code appears and put that in the second box. Then click continue.
- Once completed, log out, and then log back in.



Project Sysadmin Training – Logging in with MFA

- After completing the normal AWS sign-in as previously, you'll now be directed to an MFA screen.
- You'll need to go back to your phone and get the code being shown in the Google Authenticator app. Enter that code into the AWS webpage form that is now asking for it in the **MFA Code** field.
- Click submit. You will now be logged into the AWS console with the necessary privileges enabled for IAM, EC2, and other AWS services.



Amazon Web Services Sign-In x +

us-east-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A...

NASA KBR

aws

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

Submit

[Cancel](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2022, Amazon Web Services, Inc. or its affiliates.





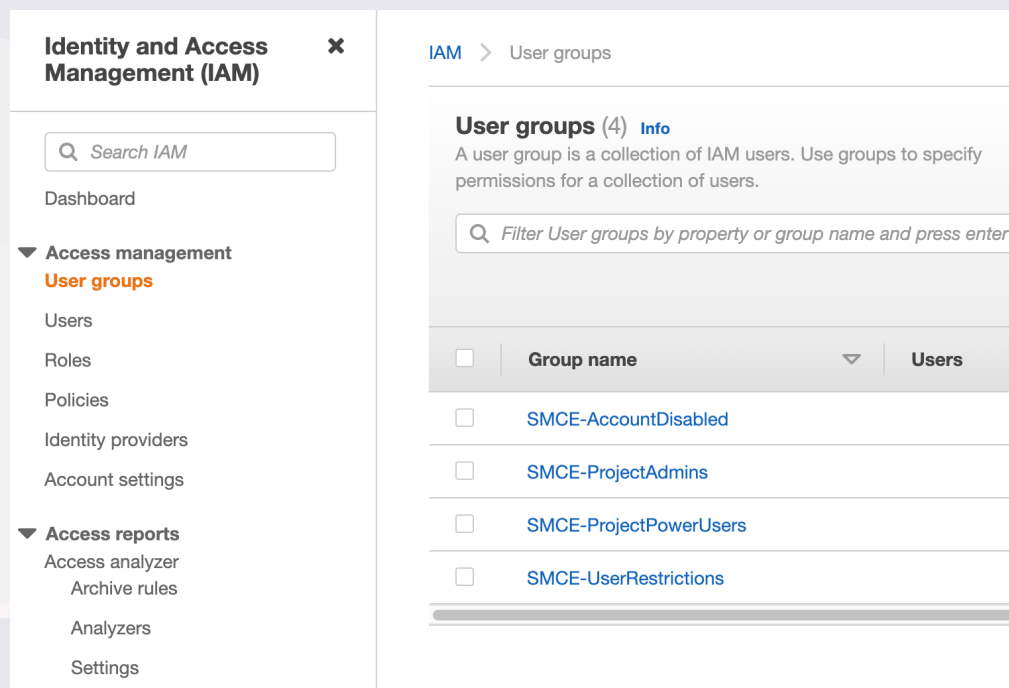
Project Sysadmin Training – Using IAM Groups

- SMCE uses the following four AWS Identity and Access Management (IAM) Groups to enable and restrict access for SMCE users:
 - **SMCE-ProjectAdmins** : Provides system administrator access to allow Project SysAdmins to manage users and EC2 instances
 - **SMCE-ProjectPowerUsers**: Provides limited administrator access to allow console users to manage EC2 instances, but restricts IAM access
 - **SMCE-UserRestrictions**: Ensures that local sysadmins inherit Region and MFA restrictions; Restricts the ability to delete users
 - **SMCE-AccountDisabled**: Disables all access for a given user; Can be used to quickly restrict access on a temporary basis due to non-compliance issues



Project Sysadmin Training – New IAM User Requirements

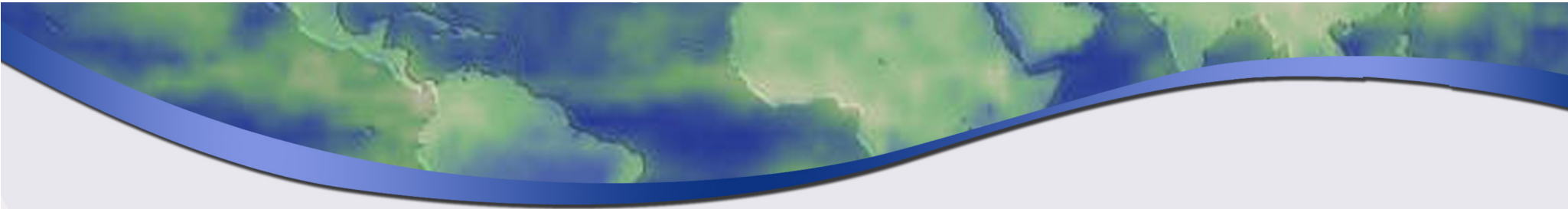
- Need to verify signed User Agreement has been received prior to the creation of any new IAM user by either a PI, Project SysAdmin, or SMCE CloudAdmin
 - Receipt of a signed User Agreement prior to the creation of an IAM user verifies that all SMCE Console Users have read and understand the SMCE Security Training modules.
- All users must enable MFA
- All users must include a custom AWS tag named “email” with the current email address for the user, which will be used for important SMCE security notifications
- Need to ensure membership in one of the 4 standard groups as defined on Slide 20 and shown here:



The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Access management' expanded and 'User groups' selected. The main content area shows the 'User groups' page, which includes a search bar, a filter input, and a table of existing user groups. The table lists four groups: 'SMCE-AccountDisabled', 'SMCE-ProjectAdmins', 'SMCE-ProjectPowerUsers', and 'SMCE-UserRestrictions', each with an associated checkbox.

| <input type="checkbox"/> | Group name | Users |
|--------------------------|------------------------|-------|
| <input type="checkbox"/> | SMCE-AccountDisabled | |
| <input type="checkbox"/> | SMCE-ProjectAdmins | |
| <input type="checkbox"/> | SMCE-ProjectPowerUsers | |
| <input type="checkbox"/> | SMCE-UserRestrictions | |





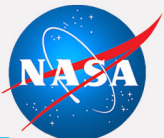
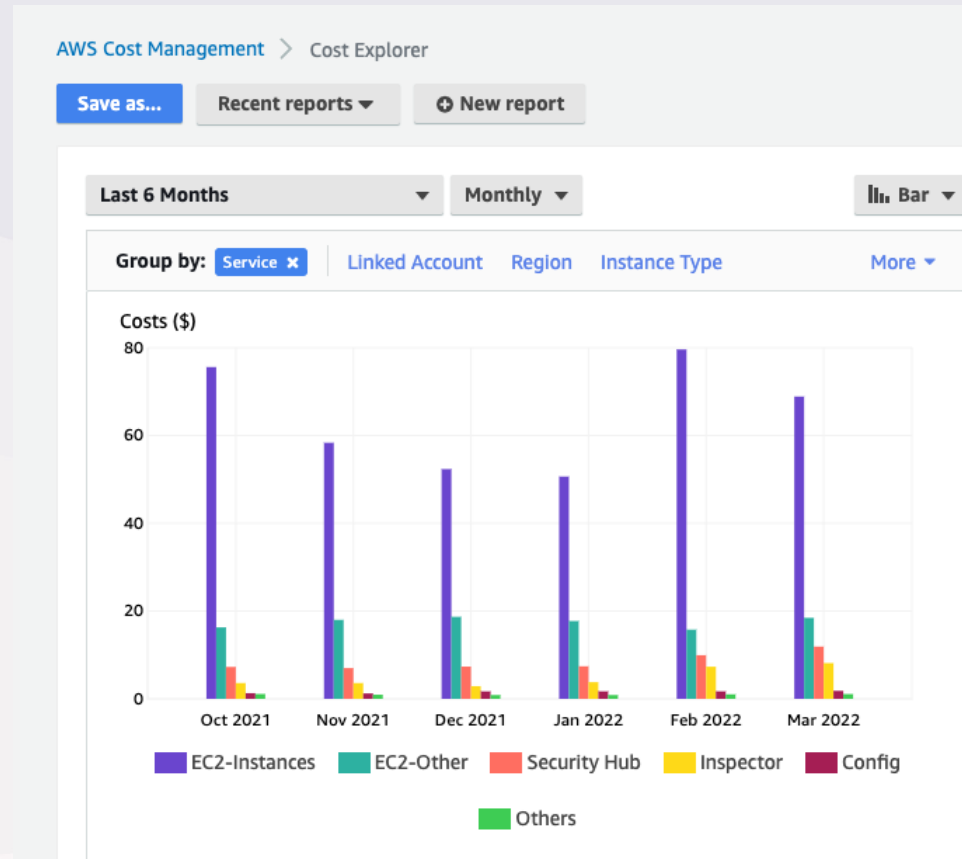
Project SysAdmin Training – Leveraging AWS Roles

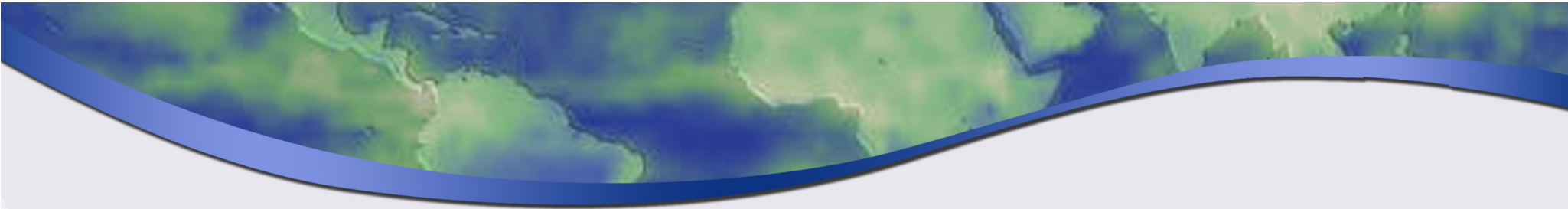
- Most secure approach for enabling access to any type of AWS resources is via the use of Roles, rather than using API Keys
 - For processes that will occur entirely within the AWS Ecosystem, IAM roles can be assigned to EC2 instances and other AWS services to provide required access.
 - Uses the same granular security model throughout IAM, so permissions can be specified narrowly
- Benefits include
 - Key rotation is handled automatically
 - No need for MFA or security exceptions/service accounts for automated processes
- Cannot be used for processes that run outside AWS, like copying data from a local device to an S3 bucket. This will still require a service account (and a documented security exception)



Project Sysadmin Training – AWS Cost Monitoring

- AWS provides several tools to allow PIs and Project SysAdmins to monitor current expenditures in AWS for a particular project
- AWS Cost Explorer allows for display of project costs by service, by month
- AWS Budgets can be used to set up custom budget alerts when a cost threshold has been exceeded
- AWS Cost Calculator can help you predict costs before you deploy a solution:
 - <https://calculator.aws>





Project SysAdmin Training – Data Allowed in SMCE

- Open Data only (publicly accessible, non-proprietary)
- No ITAR
- FISMA Low only
- No CUI
- All AWS commercial services allowed in US regions

