Overview:

A foreign account is an account that does not belong to you. Amazon IAM (Identity Access Management) helps to control your Amazon resources securely. IAM can be used to make sure that all foreign accounts are given the same privilege as non-foreign accounts, this way there is no room for attack.

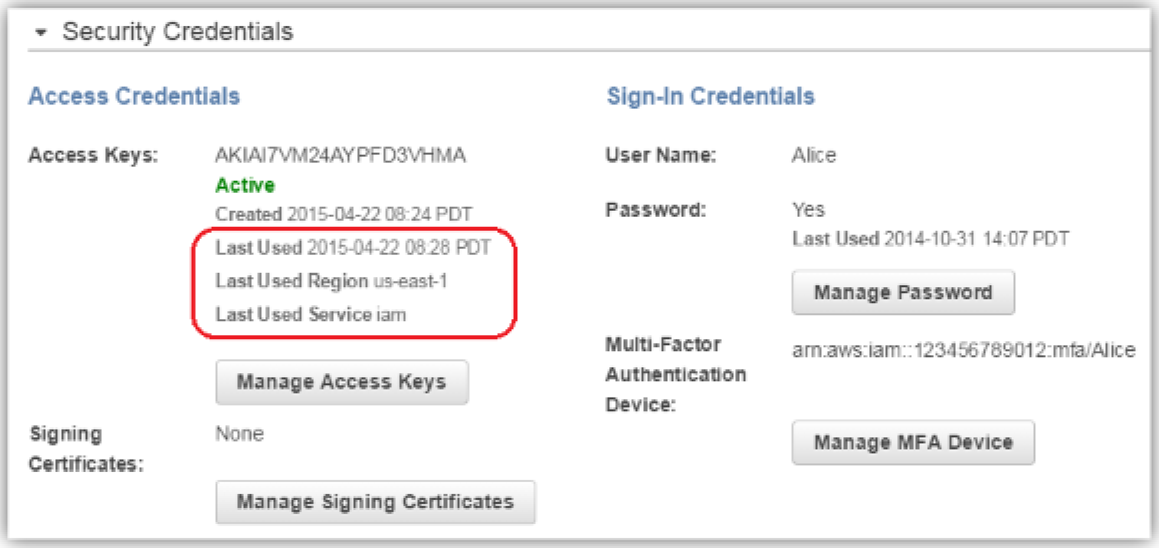
If an employee sends a request to their manager to enable additional features to their account, but the manager gives the employee full access instead of enabling a specific feature. Anyone will access to this account can take full advantage and use the additional features to go against the specific user and whatever account that user has access to.

Discovery:

There are many ways to know if a foreign IAM account has been hacked.

1. Keeping an eye on the activity logs of users:
    - To make sure that the user is only using the application which they have been given permissions to
    - There is no activity occurring out the normal order

2. Identify the last time an access key was used:
    - Login to the IAM console on AWS
    - Click on Users in the navigation pane
    - Click on an individual user name
    - Go to the Security Credentials Section (the pane at the bottom of the page which contains information the user's access keys, MFA and passwords.



Security Credentials

Access Credentials

Access Keys: AKIAI7VM24AYPFD3VHMA
Active
Created 2015-04-22 08:24 PDT
Last Used 2015-04-22 08:28 PDT
Last Used Region us-east-1
Last Used Service iam

Signing Certificates: None

Sign-In Credentials

User Name: Alice

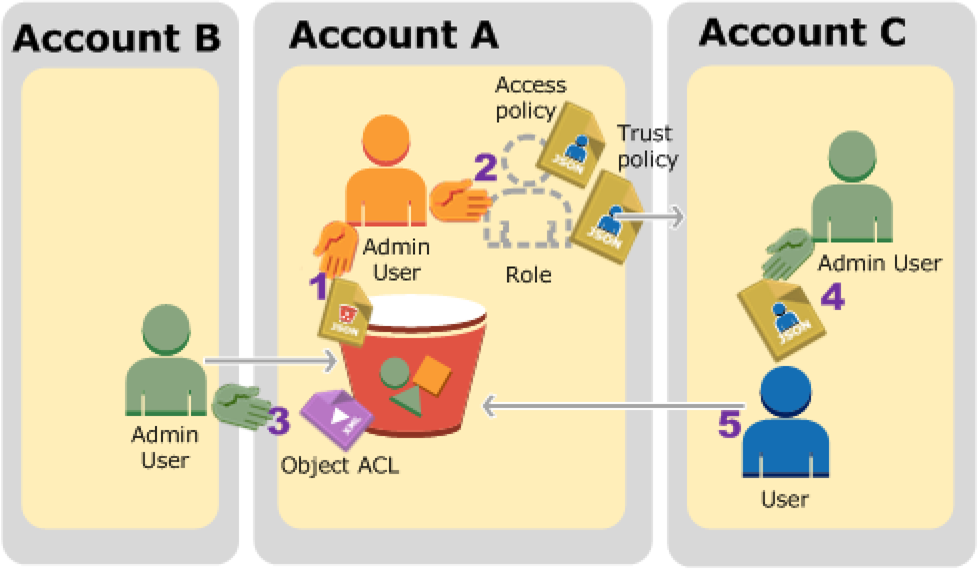
Password: Yes
Last Used 2014-10-31 14:07 PDT

Multi-Factor Authentication Device: arn:aws:iam::123456789012:mfa/Alice

For more information about identification of access key use go to:
https://aws.amazon.com/blogs/security/new-in-iam-quickly-identify-when-an-access-key-was-last-used/

Remediation:

Change permissions to limit the amount of access to each account. Go through all the accounts to make sure that no account has privileges to all features, unless a super manager.



Prevention:

Do not allow full access to any accounts especially accounts that contain a lot of sensitive data.

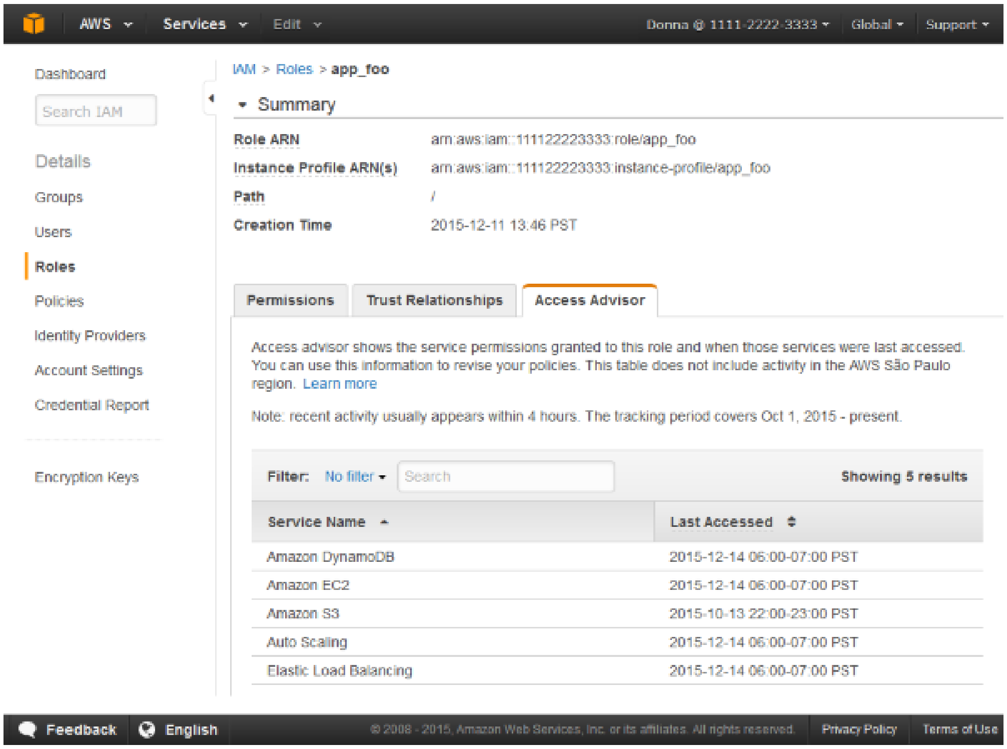
Granting Least Privilege

While creating the policies in Amazon IAM, follow the security rule of *granting lease privilege* (granting only the necessarily privilege for carrying out a task). It is recommended to start off an account with minimal permissions and over time grant the user additional permissions depending on the tasks at hand.

To determine which users need which permissions, one can use Access Advisor Tab. This tab can be used to identify permissions of users which can later be used to refine IAM policies to better adhere to the policy of granting least privilege.

To access Access Advisor Tab:

1. Sign into the IAM console on Amazon
2. Choose Users, Groups, Roles, or Policies under the Navigation Pane
3. Click on the Access Advisor Tab to view:
    - Service Name
    - Policies Granting Permissions
    - Last Access - Last time a user accessed the service
    - Access by Members - which employees and groups can access the service
    - Access by Entities - who has used the policy to access specified services



IAM > Roles > app_foo

Summary

Role ARN	arn:aws:iam::111122223333:role/app_foo
Instance Profile ARN(s)	arn:aws:iam::111122223333:instance-profile/app_foo
Path	/
Creation Time	2015-12-11 13:46 PST

Permissions | Trust Relationships | Access Advisor

Access advisor shows the service permissions granted to this role and when those services were last accessed. You can use this information to revise your policies. This table does not include activity in the AWS São Paulo region. Learn more

Note: recent activity usually appears within 4 hours. The tracking period covers Oct 1, 2015 - present.

Filter: No filter ▾ Search   Showing 5 results

Service Name ▲	Last Accessed ⇕
Amazon DynamoDB	2015-12-14 06:00-07:00 PST
Amazon EC2	2015-12-14 06:00-07:00 PST
Amazon S3	2015-10-13 22:00-23:00 PST
Auto Scaling	2015-12-14 06:00-07:00 PST
Elastic Load Balancing	2015-12-14 06:00-07:00 PST

For more information about IAM best practices:
http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#use-groups-for-permissions

For more information about Accessing Data on the Service:
http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_access-advisor.html#access_policies_access-advisor-viewing