

IAM Security Tools

AWS Certified Security Specialty SCS-C02



In this section, we will cover the security tools available in IAM (Identity and Access Management) in AWS. These tools help us manage the security of our accounts and users effectively.

Credential Report

We can generate an IAM Credential Report, which is at the account level. This report will include all users in your account and the status of their credentials.

To create this report, go to "Credential Report" in the sidebar and download the report, which will generate a CSV file.



The report provides important information such as:

- When the user was created
- Whether the password is active
- When the password was last used and changed
- When the next password rotation is expected
- "if password rotation is enabled"
- Multi-Factor Authentication (MFA) is enabled
- Access keys have been created or not

This report is extremely useful if we want to review users who have not changed their passwords or have not used their accounts. It can be a great tool to identify which users need our attention from a security perspective.

Access Advisor:

It will show us the services accessed by the user and when they were accessed.

The screenshot shows the AWS IAM console interface. In the left-hand navigation menu, the 'Users' link is highlighted with a green box. The main content area is titled 'Summary' for user 'Albert'. Below the summary, there are tabs for 'Permissions', 'Groups (1)', 'Security credentials', and 'Access Advisor', with the 'Access Advisor' tab selected and highlighted by a green box. The 'Access Advisor' section displays a table of services accessed by the user. The table has three columns: 'Service Name', 'Policies Granting Permissions', and 'Last Accessed'. The 'Last Accessed' column is highlighted with a green box. The table shows four services: AWS Identity and Access Management, Amazon S3, Amazon EC2, and Elastic Load Balancing, all accessed 144, 145, 162, and 314 days ago respectively. A filter bar at the top of the table shows 'No filter' and a search box. The text 'Showing 73 results' is visible in the top right corner of the table area.

Service Name	Policies Granting Permissions	Last Accessed
AWS Identity and Access Management	AdministratorAccess	144 days ago
Amazon S3	AdministratorAccess	145 days ago
Amazon EC2	AdministratorAccess	162 days ago
Elastic Load Balancing	AdministratorAccess	314 days ago

Using the Access Advisor, you can assess whether the user has the appropriate permissions. Based on this access data, it may become clear that the user only needs access to specific services rather than all of them. This interface provides the ability to drill down further to precisely define permissions.

The Access Advisor is very useful for managing user access permissions in detail on AWS we can use this information to revise our policies.