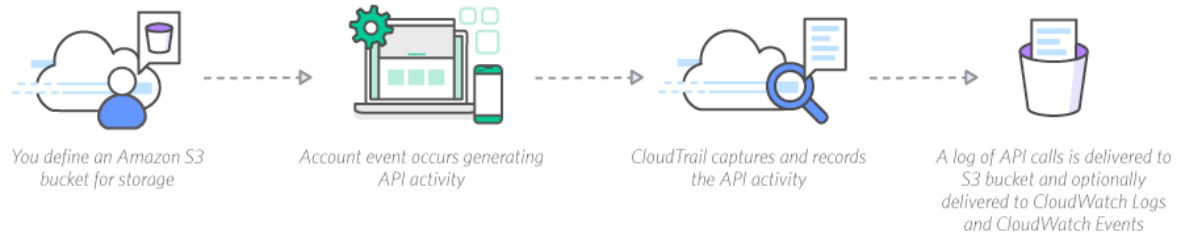


Overview:

If an attacker adds an IAM user they could give this new user all privileges. With these privileges in the new account the hacker could sign in and exfiltrate both the company and consumer data.

Creating IAM should be done through automated process - privileged operation. Want to be able to prevent regular users from adding other users.

Discovery:



It is important to keep track of all ongoing activity logs of users to make sure that they are only using the applications that they have been given permission to.

AWS has logging features that can determine what actions users are taking as well as the resources they are using.

What Do Log Files Show?

The log files show:

- Time and date of actions
- Source IP for an action
- Actions that failed due to inadequate permissions, and more.

AWS CloudTrail

AWS IAM, Identity and Access Management, is integrated with CloudTrail logs. CloudTrail “logs AWS API calls and related events made by or on behalf of an AWS account.”

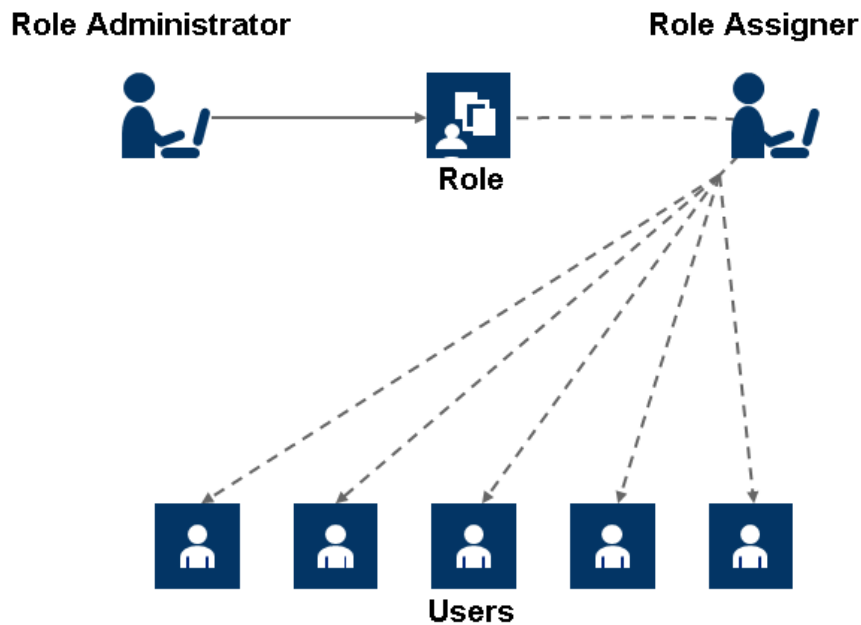
If a user adds an IAM user the action will be saved in the CloudTrail logs.

More Information: <https://aws.amazon.com/cloudtrail/> and <http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html#cloudtrail-integration-iam-information>

Taken directly from <http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

Remediation:

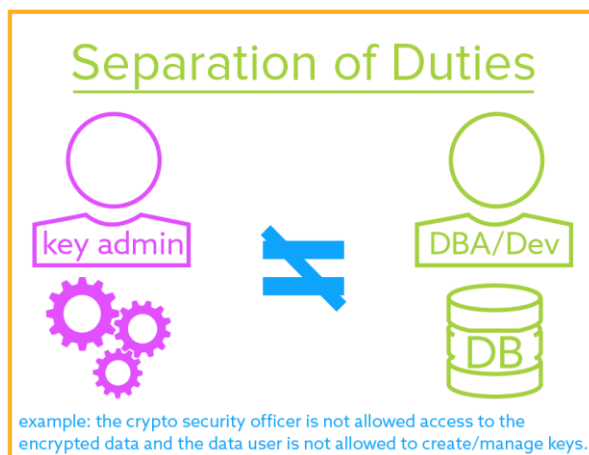
To remediate an AWS role or group attack on AWS, it is important to limit the access on who can change and/or create roles and groups on AWS. Another important thing to consider is separation of duties, the act of requiring multiple people to complete a task. Separation by sharing a task is a great internal control that will help prevent attacks on AWS IAM users.



Prevention:

By default, AWS IAM is secure. When an IAM user is created, they have no access to any services. Users are given access only when permissions are explicitly set.

The best way to secure this is to Grant least privilege.



In the creation of IAM policies it is important to grant least privilege. Granting least privilege consists of granting only the permissions required to perform a task. It is important to determine what specifically the user will be doing and create policies that will allow them to perform **only** the necessary things in those tasks.

It is more secure to start by granting just the minimum permissions for each user and granting additional permission when necessary.

It is vital to be able to properly determine what it required for each task. Such as, what actions services support, and what permissions will be required by those actions.

Useful Tool:

Access Advisor tab:

Available in the IAM console summary page. The tab includes information about which services are used by a *user, group, role or policy*. This information can be used to identify what permissions will be necessary and what may be unnecessary. This allows you to keep IAM policies to the least privilege policy.

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Users > kex496

Users: kex496

User ARNarn:aws:iam::326305413413:user/kex496

Path/

Creation time2016-10-21 22:11 EDT

Permissions

Groups (0)

Security credentials

Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015 [Learn more](#)

Filter: No filterSearch

Showing 73 results

Service Name	Policies Granting Permissions	Last Accessed
Amazon S3	AdministratorAccess	Today
Amazon EC2	AdministratorAccess	148 days ago
Amazon RDS	AdministratorAccess	Not accessed in the tracking period