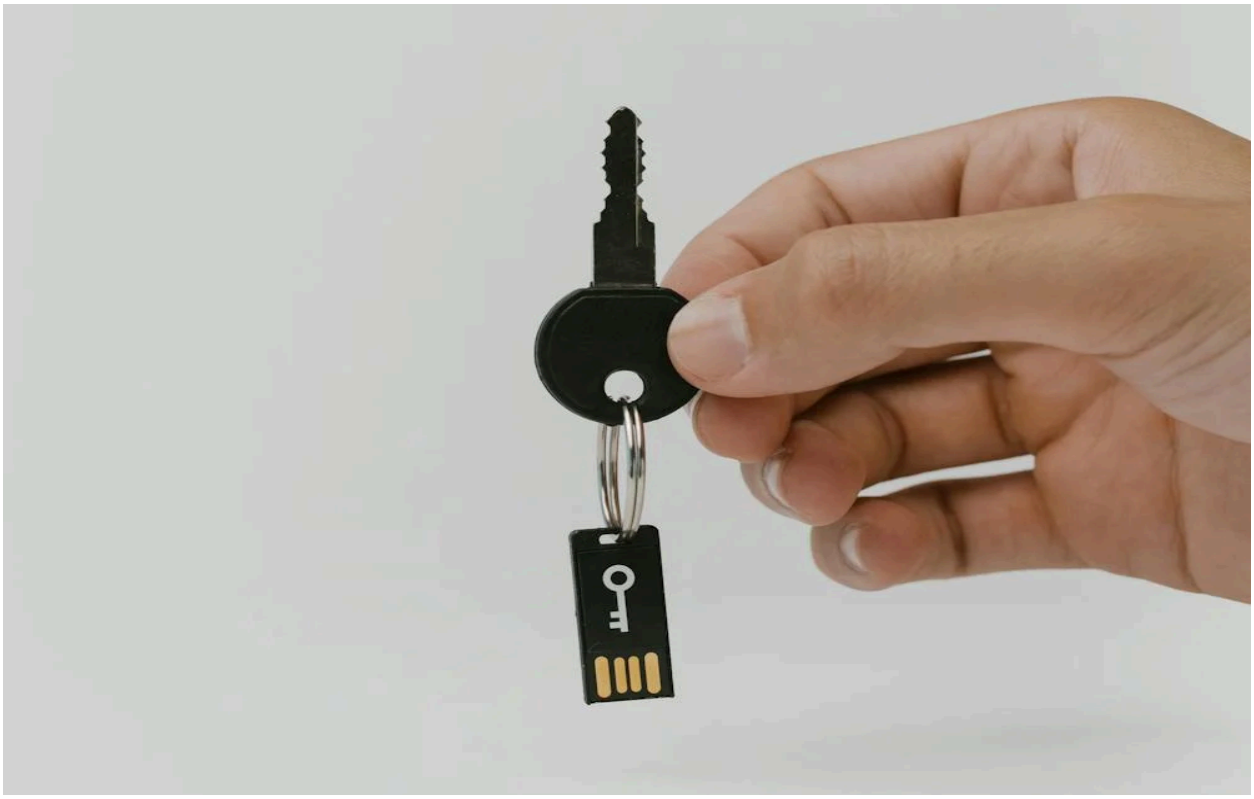
AWS IAM Identity Center: Discover How an Identity Strategy Can Help Your Company



As if dominating the ecommerce industry wasn't enough, Amazon is also the largest cloud provider in the world. Amazon Web Services (AWS) offers two services: AWS Identity and Access Management (IAM) and AWS IAM Identity Center. The Identity Center is built on top of AWS IAM and is a recommended service for managing user access to AWS resources. The use of the Identity Center enables an integrated experience for assigning, defining, and customizing access.[4] It allows you to:

- Assign your workforce users (workforce identities) consistent access to multiple AWS accounts and applications
- Assign users access to AWS managed and customer managed applications
- Create new workforce users or connect existing users
- Centrally manage their access across all AWS accounts and applications [4]

What is AWS IAM Identity Center?

The AWS IAM Identity Center is a specialized platform for managing user access to AWS accounts and applications. Here, you can easily create or connect users and have centralized control over their access across all their accounts and applications. The multi-account

permissions feature is brilliant for managing multiple accounts as it lets you grant access to users at the user or group level. You can also assign access to both AWS-managed and customer-managed applications using application assignments.[4]

The Identity Center has a portal where users can find and access their assigned accounts, cloud applications, and custom applications. If you need to customize user or group access, you can specify permission levels, which can involve using existing permissions or creating a custom permission set.[1]

Put simply, the Identity Center is a hub where you can:

- Create and manage user accounts
- Specify who has access to specific services and resources
- Manage permissions

The Importance of IAM for Your Company

Today, it's tougher than ever to keep your company secure from cyberthreats. Even with traditional security measures, such as multi-factor authentication, patching, and training, cybercriminals slip through the cracks due to ineffective IAM practices.

Improper identity management is dangerous to your company — it opens the door for cybercriminals to hijack identities, access sensitive information, and falsely approach vendors, partners, and customers. This can increase risks, harm your reputation, and compromise operational efficiency. Effective identity management can be tricky, but don't worry, Cybersecurity Connection is here to help.

PAM (Privileged Access Management) falls under the umbrella of IAM which focuses on overseeing privileged accounts within an organization. A powerful PAM strategy helps protect your organization against threats by monitoring, detecting, and auditing unauthorized access to critical resources. While AWS IAM doesn't have its own PAM features, it can still support PAM by allowing temporary elevated privileges and by working with third-party vendors.

Like all cybersecurity solutions, identity center practices should be holistic and work seamlessly throughout your entire company to ensure the best result. Integrated practices provide the visibility to discover, onboard, manage, and audit any user or device by role, function, persona, time, or location, making your job less demanding and more efficient.[5]

Benefits and Features of IAM Identity Center

The Identity Center is like a handyman's tool belt. It keeps necessary tools in one area for you to easily access when you need to. Just like a tool belt, the Identity Center improves efficiency and lessens your workload. It simplifies access management by:

- Automatically managing permissions
- Centrally managing multiple accounts and applications
- Strengthening your company's security posture[3]

Here are some key features of AWS IAM Identity Center:

Manage access to multiple AWS accounts with ease

The Identity Center assures consistent access management across multiple AWS accounts, identifies users' access permissions, and enables single sign-on authentication for your team. You can use IAM Identity Center with your current identity source or set up a new directory to control workforce access to specific parts or the entire AWS environment.[2]

Built-in integrations

It integrates seamlessly with applications such as Amazon SageMaker Studio, AWS Systems Manager Change Manager, Salesforce, Box, and Microsoft 365 to avoid having to connect your identity source to each application individually.[3]

Effortlessly maintain access to applications

When user and group information is available from your identity source through IAM Identity Center, it makes management and auditing much simpler. This can be achieved while maintaining existing access configurations for AWS accounts.[2]

Boost control and visibility of user access to data

This feature gives data owners the permission to authorize and log access by user. It allows the transfer of user identity context from your intelligence tool to the AWS data services you use, while also using your chosen identity source and other AWS access management configurations.[2]

Integrate your existing identity source to simplify processes

Connect your existing identity source to provide single sign-on access and a seamless experience across AWS services. You can use your preferred identity source and IAM Identity Center along with your existing IAM roles and policies.[2]

Manage instances

The Identity Center supports two instances: organization and account instances. An organization instance is best practice and the only one which allows you to manage access to accounts. It's deployed in the AWS Organizations management account and provides a single point to manage user access across the AWS environment.

Account instances are secured to the account in which they're enabled. It's primarily used to support isolated deployments of select AWS managed applications.[4]

How Cybersecurity Connection can Help Your Company with Identity Strategy

If you need help setting up AWS Identity Center, allow Cybersecurity Connection to be your guide. Our engineering services help you choose and implement the best cybersecurity tools for your company and offer training on the use and maintenance of the tools.

We'll begin by conducting an assessment of your current processes, whether you already use an identity tool or are starting from scratch without any processes in place. This assessment will involve looking at your compliance requirements and your organization's needs. Once we have all the information we need, we'll provide a professional recommendation on whether the Identity Center is an effective option for your company.

If our team determines that using AWS Identity Center would benefit your business, we'll work with you to create a plan for implementing the solution and provide training to designated users responsible for managing it.

Don't settle when it comes to the well-being of your company. To improve your security posture and enhance your operational excellence, visit CybersecurityConnection.com.

References

1. Bell, C., & Morgan, S. (n.d.). *AWS IAM vs. AWS IAM Identity Center: Choosing the Right Service*. JumpCloud. Retrieved June 20, 2024, from https://jumpcloud.com/blog/aws-iam-vs-aws-sso

2. (n.d.). *AWS IAM Identity Center*. Amazon. Retrieved June 20, 2024, from https://aws.amazon.com/iam/identity-center/

3. (n.d.). *AWS IAM Identity Center Features*. Amazon. Retrieved June 20, 2024, from https://aws.amazon.com/iam/identity-center/features/

4. (n.d.). *What is IAM Identity Center?* Amazon. Retrieved June 19, 2024, from https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html

5. Pelton, C. (n.d.). *The Importance of Identity Management in Security*. CIO. Retrieved June 20, 2024, from https://www.cio.com/article/1247542/the-importance-of-identity-management-in-security.html