Root User Policies for Wharton Computing AWS Linked Accounts

Last Modified on 11/22/2024 3:21 pm EST

Secure the *root user email address*

When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources within that account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password you used to create the account.

Using an email address managed by the Infrastructure and Services team

Use a group email address for root user credentials

- Use an alias address for each account that forwards notifications to a mailing list *aws-org-accounts@wharton.upenn.edu*.
- Only Infrastructure and Services team members are members of the list.
- Only Infrastructure and Services team members are owners of the list.

Secure root user password

- Passwords are stored in a dedicated shared folder in Dashlane.
- Only Infrastructure and Services team members have access to this folder.
- Only the Infrastructure and Services team and Dashlane administrators can grant access to the folder.

Restrict actions for the root user

- SCP denies all actions except enabling MFA.

Restrict access to account recovery mechanisms

- Use a Hunt Group number to forward AWS to access the account.
- Only Infrastructure and Services team members will receive AWS calls sent to the Hunt Group number.
- Only Infrastructure and Services team members can modify the list of users who will receive the call.

Disable access keys for the root user

- Access keys are disabled, and the root user cannot reactivate them.

Enable MFA for the root user

- MFA is enabled; however, the effective second authentication factor is access to the Hunt Group number.

Monitor access and usage

- Login events are sent to a SNS notification channel.

Configure *Primary contact* information

- Configure the contact information, and phone number, for restoring access to the account.

You can update the primary contact information associated with your account, including your contact's full name, company name, mailing address, telephone number, and website address. You edit the primary account contact differently, depending on whether or not the accounts are standalone, or part of an organization:

- **AWS accounts within an organization** – For member accounts that are part of an AWS organization, a user in the management account or delegated admin account can centrally update any member account in the organization from the AWS Organizations console, or programmatically via the AWS CLI & SDKs. To learn how to do this, see Update AWS account primary contact in your organization.

References

https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-best-practices.html