AWS Best Practices

Last Modified on 02/19/2024 4:02 pm EST

AWS is Wharton's preferred cloud vendor. Wharton has AWS Enterprise Support and has integrated account creation for AWS, allowing payment via budget code. For information on obtaining an account see AWS Linked Accounts.

Table of Contents

- Enterprise Support
- Billing
- User Access
- Emergency Account Access
- Security
- Questions?

Enterprise Support

All Wharton faculty and staff with AWS-linked accounts can contact AWS directly for Enterprise Support.

- To open a support case, see Amazon Support's article, Creating support cases and case management.
- Enterprise Support includes:
  - Unlimited 24x7 support
  - Billing assistance
  - Architectural reviews
  - Proactive guidance

If you want more information about Enterprise Support, ask your Wharton Computing Representative to contact Wharton Computing's ESS team on your behalf.

^Top

Billing

- Every linked account must have a budget code associated with it. F&A will charge back costs to that billing code quarterly.
  - Wharton Research has a separate billing mechanism for users who use Research's AWS accounts. Those charges are billed back monthly.
- Users can see the charges in their linked account by using the AWS Cost Explorer.
- Wharton has a more sophisticated tool called CloudHealth that is available on request. To get access to CloudHealth, ask your Wharton Computing Representative to contact Wharton Computing's ESS team on your behalf.
  - To log in, use **[your Pennkey]@upenn.edu** and your Pennkey password
  - If you are interested in an introduction to CloudHealth, ask your Wharton Computing Representative to contact Enterprise Solutions and Services.
  - CloudHealth is the only way to see charges for multiple AWS-linked accounts at one time.
- CloudHealth provides a Cost Anomaly Detector that uses artificial intelligence to detect surprising upward deviations in spending. The detector can be set to send an email alert when anomalous spending crosses a threshold.

  - Users can also set up cost anomaly detection on any single AWS-linked account.
  - To set up cost anomaly detection across multiple linked accounts, or simply to get assistance, ask your Wharton Computing Representative to contact Enterprise Solutions and Services.

^Top

User Access

- By default, each AWS-linked account has two roles, an administrator role and a read-only role. When the account is created, at least one person is assigned to the administrator role.
- Wharton has implemented single sign-on so that account users can log on with their Pennkey and password.

Roles

- Account users can create their roles and request that users be assigned to the roles.

User Authentication

- Wharton strongly recommends that users authenticate with Pennkey whenever possible.
- Pennkey authentication ensures that users who no longer have active Pennkeys cannot access AWS-linked accounts.
- If necessary, linked account users can create IAMusers. This is a less desired configuration as IAM users are not protected by PennKey MFA (Multi-Factor Authentication). Also, IAM user accounts will not expire when the account user is no longer affiliated with Penn.
- Every account has a root credential. This root credential is held byWharton Computing for landing-zone accounts (all accounts created since March 2020). Account owners have the root credentials for accounts created before March 2020. AWS policy is that root credentials should never be used for regular account access and that the service team that manages AWS should hold all root credentials. Also, all root credentials should be protected with MFA.

^Top

Emergency Account Access

- By default, Wharton Computing has no access to linked accounts that are owned by faculty. Access for staff-linked accounts is set by the account owner.

- In an emergency, Wharton Computing can shut down systems that have security breaches.

- Also, if an account has an anomalous cost increase Wharton Computing can shut down systems.

- Wharton Computing's senior leadership has to approve any emergency access to shut down resources in linked accounts.

^Top

Security

- AWS-linked accounts are configured by default to follow AWS best practices for security. They use AWS Config, GuardDuty, and Security Hub to monitor potential threats.

^Top

Questions?

For more information, contact your Wharton Computing Representative.