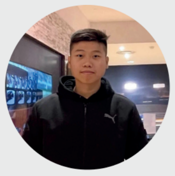
IAM BEST PRACTICES FOR OPTIMAL AWS SECURITY

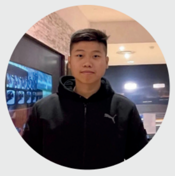
Swipe to know ⟫



Aiden Tran
@aidentran

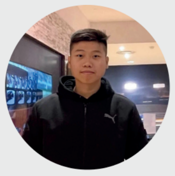
SINGLE-USER ACCOUNTS

“Assign each user a unique AWS user account. This ensures clear activity logs and individual accountability.”



REQUIRED MFA IMPLEMENTATION

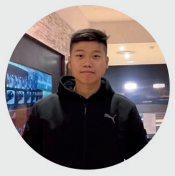
“Enforce Multi-Factor Authentication to significantly reduce the risk of unauthorized access.”



Aiden Tran
@aidentran

ROOT ACCOUNT USE CAUTION

“Use the root account only for initial setup to avoid exposing full administrative privileges.”

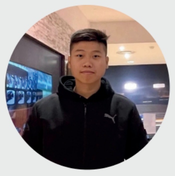


ROLES OVER PERMISSIONS

“Utilize roles for assigning permissions to AWS services, ensuring that rights are governed by current needs without overexposure.”

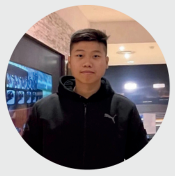
PROGRAMMATIC ACCESS

“Use access keys exclusively for programmatic access (CLI/SDK) to secure your automated operations.“



GROUP-BASED PERMISSIONS

“ Manage permissions efficiently by grouping users and assigning rights at the group level to streamline access management.”



Aiden Tran
@aidentran

NEVER SHARING

“Never share your IAM users and Access Keys. Ensure that each credential is used by one entity only, thereby enhancing security measures.”