Standard AWS Account Configurations

In consultation with Cornell IT Security Office and Cornell financial administrators, two "standard" configurations of AWS accounts have been defined, one for general uses and one for research. Each configuration follows AWS, Cornell, and security best practices. Not all best practices can be implemented by policy and configuration. Individual AWS users also need to follow best practices see the Cloudification Services Tech Blog and AWS IAM best practices documentation.

For details of specific AWS resources created in Cornell AWS accounts, see Resources Created and Managed in Cornell AWS Accounts.

Area	Configuration	Link/Description	General Configuration	Research Configuration
Security /Network	• Shared AWS VPC for Cornell AWS Accounts • Cornell Standard VPC	The Cornell Shared AWS VPC provides access to the private Cornell network without the need to manage VPC resources. For needs not met by the Shared VPC offerings, the Cornell Standard VPC is customizable VPC owned and managed by customers.	y	as needed
Security /Network	AWS VPC connected to on-campus network	Private on-campus subnets are connected to AWS VPC subnets using an AWS Direct Connect connection from campus to AWS. See Cornell AWS Direct Connect.	y	as needed
Security /Network	AWS VPC subnets are assigned to managed, private IP spaces	This ensures that Cornell private subnets (on-campus and in AWS) do not overlap and that private subnets are transparently and securely routed to AWS VPC subnets.	y	as needed
Security /Network	private AWS VPC subnets are provisioned with a NAT Gateway	This provides a secure route to the public internet so that AWS EC2 instances can retrieve software updates and remain un-exposed to the public internet. See AWS NAT Gateway documentation.	y	as needed
Security /Network	AWS VPC are provisioned with AWS Internet Gateways	This provides AWS EC2 instances running in public VPC subnets access to the internet and vice versa. (Not application to Shared AWS VPC options.)	y	as needed
Security /Network	Baseline Network ACL configured for all subnets	The baseline NACL allows full access between 10-space and Cornell public IPs, but limits access from the world to ports above 1024 and to 22, 80,443.	y	as needed
Security /Business	AWS account integrated with CloudCheckr and Spot.io	CloudCheckr reports provide suggestions for improving security, reducing costs. It also supports detailed reporting based on AWS labels to e.g., divide account charges to multiple Cornell financial accounts within a single Cornell unit. See CloudCheckr - Cost, Inventory, Security, Utilization reporting As of 02 Apr 2024 we are in the process of giving spot.io access to Cornell AWS accounts. CloudCheckr has been purchased by Spot.	y	y
Business	AWS Cost Explorer access	Each Cornell AWS account has access to the AWS Cost Explorer service to view history and projected costs for that account. Cost Explorer is generally easier to use than CloudCheckr, but it has less flexibility that CloudCheckr and requires AWS account access (something that Cornell financial staff may not want).	y	y
Security	AWS CloudTrail enabled for all activity in all regions	CloudTrail logs all AWS API calls in all regions for auditing purposes. See Cornell Standard AWS CloudTrail Configuration	y	y
Security	AWS Config enabled with Organization-wide Rules	AWS Config is a service that supports assessment, auditing, and evaluation of the configurations of AWS resources. The Cornell Config deployment utilizes Organization-wide Config Rules that check standard configurations and best practices.	y	y
Security	AWS Flow Logs configured	All VPCs are configured to capture flow logs. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html	y	y
Security	access to AWS account by ITSO in cases of security issues		y	y
Security	AWS root account protected with multifactor authentication	root account should not be used for regular administration and the MFA key should be locked in secure location	y	y
Security	no access keys associated with root account		y	y
Security	user access controlled by Cornell AD group membership and integrated with Cornell Shibboleth	See User Access Control for AWS Accounts	y	y
Security	access for users with administrative privileges utilize Cornell Duo for authentication	See User Access Control for AWS Accounts IAM users can be used for service/programmatic access.	y	y

Security	baseline IAM password policy configured	The password policy will enforce complex passwords in the rare instances when an IAM user requires a password.	y	y
Security	Read Only role for AWS resources	This role allows the Cloudification Team to view Cornell AWS accounts while troubleshooting and offering assistance, while ensuring that account owners maintain account integrity.	y	y
Security	Management Role for AWS Resources	This role allows scripted management of these standard account configurations by the AWS Organization master account.	y	y
Security	IAM Access Analyzer enabled in all active regions	The AWS Identity and Access Management Access Analyzer identifies AWS resources that can be accessed by external entities (e.g., other AWS accounts). See Cornell Standard Configuration for AWS IAM Access Analyzer for details.	y	y
Security	Key Security Events Captured by EventBridge Rules	EventBridge Event Rules are configured in all Cornell AWS accounts to capture activity that is or could be an indicator of an account breach or malicious activity. See Cornell Standard Configuration for AWS Security Events for details.	y	y
Security	Regional Restriction feature	Cornell AWS accounts can optionally enable Regional Restriction to have account activity restricted to the four US-based AWS regions.	y	y
Security	Github Actions OIDC Provider	With the Github OIDC provider, Cornell cloud practitioners can use IAM Roles instead of access keys linked to AWS IAM users when a Github Action workflow requires access to a Cornell AWS account. See Github OIDC Provider for Cornell AWS Accounts for details.	y	y