Cloud Vocabulary Taxonomy

Created by **Joshua Wright**
@joswr1ght

ID	TERM	DEFINITION	EXAMPLE
1	AMI	Amazon Machine Image—A template of operating system, application, and data files configured to fulfill a system need.	*Jennifer built the AMI to include only the required packages.*
2	ARN	Amazon Resource Name—A standardized way to refer to AWS resources.	*Instead of using vague project names, Delisha converted all the project documentation to use explicit ARNs for assets.*
3	Account	A relationship with AWS where an email address is registered for access with a payment method.	*My organization has three AWS accounts: DEV, PROD, and TEST.*
4	Action	Refers to any API function.	*Mick called the ApproveSkill action with write access.*
5	Assume Role	A temporary set of credentials issued to grant access to AWS resources consisting of an access key ID, a secret access key, and a security token. Intended for flexibility in delegating access to resources as part of the Security Token Service (STS).	*Meaghan pointed out that the role grants the Assume Role action, which could lead to a confused deputy attack for specified ARNs.*
6	Call	Synonym for action; refers to any API function.	*The backup function does not need access to the Change Password call.*
7	Confused Deputy	A security threat where an entity without access to a privilege can coerce a privileged entity into completing the action on their behalf – often the result of not specifying a resource ID in a policy, or misuse of the AssumeRole privilege.	*Karen tracked the incident to the root cause: an overly broad third-party cross-account access policy allowed external entities to create S3 objects.*
8	Entity	Refers to the users or actors (humans) accessing AWS. Often used interchangeably with identity.	*Lodrina clarified the convention: entities can login, identities receive permissions.*
9	Group	A collection of IAM users, often used for logical organization, or to simplify permission management.	*Developers in the StagingAccess group should not also have access to the s3:CreateBucket action.*
10	IMDS	Instance Metadata Service—A service used for EC2 instances that allow developers to configure and manage the running instance.	*Katie showed us how a vulnerable web application can be coerced to disclose keys through the IMDS service.*
11	laaS	Infrastructure as a Service—A low-level cloud service providing server, storage, and networking services.	*Chris thinks we'll get more flexibility with EC2, the laaS solution, but we take on the burden of OS deployment and management.*
12	Identity	A user account that has varying levels of access rights, often allocated to an individual for access – also known as a user.	*Developers must get approval from their manager to receive an AWS identity for access to cloud systems.*

Cloud Vocabulary Taxonomy

ID	TERM	DEFINITION	EXAMPLE
13	Instance	A copy of an Amazon Machine Image (AMI} running as a virtual server in the AWS Cloud. Often associated with the AWS EC2 product.	*Don't terminate that instance, we need it for forensics.*
14	Operation	Synonym for action; refers to any API function.	*The developer says they need access to the AddUserToGroup operation.*
15	Organization	AWS Organizations is a product that manages multiple AWS accounts for a company/government/institution.	*My employer leverages AWS Organizations to manage the DEV, PROD, and TEST accounts from one central location.*
16	PaaS	Platform as a Service—Mid-level cloud service focusing on application deployment, delegating infrastructure management to AWS.	*Anurag designed the app to deploy on AWS' Elastic Beanstalk (EBS) PaaS solution, eliminating our need to manage server OS components.*
17	Policy	A JSON document that describes the permissions that apply to a user, group or role. Policies can permit or deny access to actions, optionally by resource name.	*Designing policies with the NotAction element is convenient, but risky: when Amazon adds new actions, users will receive the actions automatically.*
18	Principal	The AWS account, role, user, service, entity, or identity that receives permit or deny access to conduct actions.	*Ritu configured the policy to restrict access to explicitly-specified principals.*
19	Region	A location in the world where Amazon has multiple data centers, all within 60 miles (100 km) of each other. A single region is compromised of multiple zones.	*Bryce pointed out that we'd achieve the highest performance by deploying assets in the same region.*
20	Resource	A generic term used by multiple providers for any compute instance, storage object, networking device, or other entity you can create or configure within the platform.	*In our analysis we'll examine Lambda, EC2, S3, and RDS resources for vulnerabilities.*
21	Role	Often used for IAM role; an identity with permission policies that does not have credentials. An IAM role represents a collection of permissions that can be granted to users.	*Jon created a role with the S3 permissions needed to access the files. We'll use the role to grant temporary access to the consultants.*
22	SaaS	Software as a Service—High-level cloud service providing application functionality to end-users.	*Zach completed the transition to the HR Saas solution, eliminating the legacy server platform.*
23	Tenant	Typically associated with Saas deployments, the tenant is the customer that accesses a multi-user system.	*Ron designed the platform to accommodate multiple tenants with isolated data storage.*
24	Zone	One or more data centers within a region with independent resources (power, networking).	*Moses argued that we should distribute backups across different zones to avoid any loss of access following a natural disaster.*