Book start

content *text*

Term

Definition 1

This is a definition.

Definition 2: Context

This is a definition.

> This is a quote.

Another Term

Definition 3

This is a definition.

Definition 4: Context

This is a definition.

> This is a quote.

AWS IAM

Definitions

Definition 5: Definition 1AWS

The native IAM platform in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. (link)
5. (link)
6. (link)
7. (link)
8. (link)

Quotes

> AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

(AWS, 11/2020, p. 1)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

((link) , p. 1) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

Bibliography

1. (link)

See Also

label = ”aws-iam” false title

AWS IAM Policy

Definitions

Definition 6: Definition 1AWS

An access policy in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)
7. (link)

Quotes

> Policies and Permissions in IAMYou manage access in AWS by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, if a policy allows the GetUser action, then a user with that policy can get user information from the AWS Management Console, the AWS CLI, or the AWS API. When you create an IAM user, you can choose to allow console or programmatic access. If console access is allowed, the IAM user can sign in to the console using a user name and password. Or if programmatic access is allowed, the user can use access keys to work with the CLI or API..

(AWS, 11/2020, p. 351)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

((link) , p. 351) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

Bibliography

1. (link)

See Also

label = ”aws-iam-policy” false title

AWS IAM Temporary Security Credentials

Definitions

Definition 7: Definition 1AWS

A temporary identity in AWS.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)
7. (link)

Quotes

> Temporary security credentials in IAMYou can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences: • Temporary security credentials are short-term, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them. • Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so.These differences lead to the following advantages for using temporary credentials: • You do not have to distribute or embed long-term AWS security credentials with an application. • You can provide access to your AWS resources to users without having to define an AWS identity for them. Temporary credentials are the basis for roles and identity federation. • The temporary security credentials have a limited lifetime, so you do not have to rotate them or explicitly revoke them when they're no longer needed. After temporary security credentials expire, they cannot be reused. You can specify how long the credentials are

> valid, up to a maximum limit.

(AWS, 11/2020, p. 301)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

((link) , p. 301) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

Bibliography

1. (link)

See Also

label = ”aws-iam-temporary-security-credentials” false title

AWS IAM Group

Definitions

Definition 8: Definition 1AWS

A security group in AWS. It contains *AWS IAM Users* and may be granted permissions via policies. It has a flat structure, i.e. AWS IAM does not support group nesting.

Related Terms

1. ARN
2. AWS
3. AWS Account
4. AWS IAM
5. (link)
6. Group

Quotes

> IAM GroupsAn IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. If a new user joins your organization and needs administrator privileges, you can assign the appropriate permissions by adding the user to that group. Similarly, if a person changes jobs in your organization, instead of editing that user's permissions, you can remove him or her from the old groups and add him or her to the appropriate new groups.Note that a group is not truly an "identity" in IAM because it cannot be identified as a Principal in a permission policy. It is simply a way to attach policies to multiple users at one time.Following are some important characteristics of groups:- A group can contain many users, and a user can belong to multiple groups.- Groups can't be nested; they can contain only users, not other groups.- There's no default group that automatically includes all users in the AWS account. If you want to have a group like that, you need to create it and assign each new user to it.- The number and size of IAM resources in an AWS account are limited. For more information, see IAM and STS quotas.

(AWS, 11/2020, p. 160)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

((link) , p. 160) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html
)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-group”

AWS Account Root User

Definitions

Definition 9: Definition 1AWS

The root user of an AWS account, with unlimited privileges on the account and its resources.

Related Terms

1. AWS
2. Root User

Quotes

> AWS account root userWhen 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 in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account.

(AWS, 11/2020, p. 72)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html)

((link) , p. 72) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html)

Bibliography

1. (link)

See Also

label = ”aws-account-root-user” false title

AWS ACL

Alternate Forms

1. AWS Access Control List

Definitions

Definition 10: Definition 1AWS

An ACL implementation specific to AWS whose scope is limited to granting access to identities outside the AWS Account that contains the resource. Contrary to other AWS policy types, AWS ACL is not following the AWS JSON policy format.

Related Terms

1. (link) `Generic Form`
2. AWS
3. AWS Account
4. AWS IAM
5. (link)

Quotes

> Access control lists (ACLs)Access control lists (ACLs) are service policies that allow you to control which principals in another account can access a resource. ACLs cannot be used to control access for a principal within the same account. ACLs are similar to resource-based policies, although they are the only policy type that does not use the JSON policy document format. Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs.

(AWS, 11/2020, p. 353)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

((link) , p. 353) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html)

Bibliography

1. (link)

See Also

false title label in (”aws-access-control-list” , ”aws-acl”)

AWS IAM Role

Definitions

Definition 11: Definition 1AWS

A temporary on-demand business role in AWS. Once an identity is granted permission to assume a role, the identity may assume that role by demanding it. It then inherits all of the access permissions linked to it.

Related Terms

1. AWS
2. AWS Account
3. (link)
4. AWS IAM
5. (link)
6. (link)

Quotes

> IAM RolesAn IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard longterm credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account. Or you might want to allow a mobile app to use AWS resources, but not want to embed AWS keys within the app (where they can be difficult to rotate and where users can potentially extract them). Sometimes you want to give AWS access to users who already have identities defined outside of AWS, such as in your corporate directory. Or, you might want to grant access to your account to third parties so that they can perform an audit on your resources.For these scenarios, you can delegate access to AWS resources using an IAM role.

(AWS, 11/2020, p. 167)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)

((link) , p. 167) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-role”

AWS IAM User

Definitions

Definition 12: Definition 1AWS

An identity in AWS. It is mapped to either a person or an application. It has 3 identifiers: a friendly name, an ARN and a unique ID. It is linked to a single *AWS Account* . It may be a member of *AWS IAM Groups* . It may be granted direct permissions or indirect permissions via *AWS IAM Group* membership.

The *AWS Account Root User* is not considered as an *AWS IAM User* .

Related Terms

1. ARN
2. AWS
3. AWS Account
4. (link)
5. AWS IAM
6. (link)

Quotes

> IAM UserAn AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user in AWS consists of a name and credentials.

(AWS, 11/2020, p. 74)
(Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

((link) , p. 74) (Online: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

Bibliography

1. (link)

See Also

false title label = ”aws-iam-user”

Mutual Authentication

Definitions

Definition 13: Definition 1

A communication scheme where both communicating entities are authenticated to each other.

Mutual authentication requires more than two unilateral authentications in opposite directions, because of the relationship between these two opposite processes.

Mutual authentication protects against unauthorized access by mitigating man-in-the-middle attacks. In certain circumstances, it may mitigate DoS attacks as well.

When communication takes place between a server and a client, authentication of the client by the server may be incorrectly perceived as the only important security aspect. But without authentication of the server by the client, the server itself may be spoofed leading the way to multiple attacks.

Related Terms

1. (link)
2. Unilateral Authentication

Quotes

> SRP-8REQUIREMENT: The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel. (5.3.3.2 #7)SUPPLEMENTAL GUIDANCE: Mutually authenticated protected channels employ approved cryptography to encrypt communications between (sic)Supervised remote identity proofing stations/kiosks are required to employ mutual authentication where both the station/kiosk and server authenticate to each other. This is most often accomplished through the use of mutual TLS. Upon successful mutual authentication, an encrypted communication channel is established between the workstation/kiosk and the server which protects the data exchanged between them.ASSESSMENT OBJECTIVE: Confirm the CSP's supervised remote identity proofing stations or kiosks communicate with the identity service via mutually authenticated protected channels.POTENTIAL ASSESSMENT METHODS AND OBJECTS: Examine: one or both the of the following: system documentation, such as remote identity proofing station specifications; or an actual supervised remote identity proofing station (kiosk) employed by the CSP.

(Fenton, 2020, p. 58-59)

((link) , p. 58-59)

> 3.2.2.4 Authentication and Data Integrity between ABAC ComponentsThe authorization service requires strong mutual authentication between ABAC components (e.g., PEP, PDP) when authorization service components exchange sensitive information. For each exchange, proof of origin, data integrity, and timeliness should be considered. For example, when the authorization service needs to obtain attributes from an authoritative attribute service, mutual authentication should be used, followed by mechanisms for validating message integrity and message origin. Authentication protocols based on strong methods (e.g., X.509 authentication) should be used to provide the level of assurance needed by both parties involved in the attribute exchange.

(NIST SP 800-162, 2014, p. 28)

((link) , p. 28)

> RADIUS(…)- Mutual authentication support: Man-in-the-middle attacks are possible with one-way authentication. Mutual authentication eliminates this risk by authenticating the RADIUS server and the client. The client initially passes its identification to the server, which responds with its identification so that both the server and the client are assured of mutual reliability. The same happens with the AP and the server.

(EC-Council, 2010, § 5-35)

((link) , § 5-35)

> DHCP Services(…)RFC 3118 appends authentication to DHCP and permits a client to confirm whether a specific DHCP server can be relied on and whether a request for DHCP information originates from a client that is certified to use the network. This mutual authentication in DHCP presents the additional security advantage of helping to protect DHCP clients and servers from DoS attacks and unauthorized access. RFC 3118 describes a method that can present both individual certification and message confirmation. This helps a DHCP client verify the uniqueness of the DHCP server it chooses in an unsecured network environment. This operation is very helpful for both a standard company Ethernet network and an Internet service provider (ISP).

(EC-Council, 2010, § 5-38-39)

((link) , § 5-38-39)

> 11.4.2 Mutual AuthenticationThe basic mechanisms for message freshness or principal-liveness introduced so far achieve so-called ”unilateral authentication” which means that only one of the two protocol participants is authenticated. In mutual authentication, both communicating entities are authenticated to each other.ISO and IEC have standardized a number of mechanisms for mutual authentication. A signature based mechanism named ”ISO Public Key Three-Pass Mutual Authentication Protocol” [148] is specified in prot 11.1. We choose to specify this mechanism in order to expose a common misunderstanding on mutual authentication.One might want to consider that mutual authentication is simply twice unilateral authentication; that is, mutual authentication could be achieved by applying one of the basic unilateral authentication protocols in §11.4.1 twice in the opposite directions. However, this is not generally true!A subtle relationship between mutual authentication and unilateral authentication was not clearly understood in an early stage of the ISO/IEC standardization process for prot 11.1. (…)

(Mao, 2003, § 11.4.2)

((link) , § 11.4.2)

> mutual authenticationAuthentication of both ends of a communication session.OverviewTraditional network authentication systems have centered around having the server authenticate the credentials of the client. They ignore authentication of the server by the client since it is assumed that the server is always a trusted entity. However, it is sometimes possible to spoof the identity of a server, especially in an Internet scenario in which information is sent over an insecure public communication system and is subject to eavesdropping, interception, and hijacking. Although simple consumer transactions such as users buying goods online may suffice with one-way authentication of clients by e-commerce servers, more costly business-to-business (B2B) and financial industry transactions need both ends of a communication channel to be authenticated before establishing a session and per- forming a transaction. Mutual authentication is the general term for any scheme by which both parties authenticate the other prior to sending sensitive information to each other.One protocol that was developed for mutual authentication is Kerberos, a popular authentication protocol developed by the Massachusetts Institute of Technology (MIT) and used by Active Directory directory service in Microsoft Windows 2000 and Windows Server 2003. Other mutual authentication protocols include the following: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) Extensible Authentication Protocol/Transport Layer Security (EAP/TLS) Symmetric-Key Three-Pass Mutual Authentication Protocol defined in the ISO 9798 standardSee Also:

> authentication, Kerberos

(Tulloch, 2003, p. 199)

((link) , p. 199)

Bibliography

1. (link)
2. (link)
3. (link)
4. (link)
5. (link)

See Also

false title label = ”mutual-authentication”

Stability of Access Decision Factors

Definitions

Definition 14: Definition 1

The average period during which access decision factors are only subject to slight disturbance, prolonging the validity of previously defined access permissions. A disturbance of access decision factors beyond some threshold triggers the requirement to adapt access permissions. Distinct access control methods (e.g. ACL, RBAC, ABAC, PBAC) are varyingly efficient in the way they enable modifications of access permissions.

Related Terms

1. ABAC
2. (link)
3. (link)
4. (link)
5. PBAC
6. RBAC

Quotes

> 3.1 Stability of Access Decision Factors – When the basis for access decisions is relatively stable, use of mechanisms such as ACLs lends itself more readily. Administrative processes typically required to maintain these lists are time-intensive and not particularly well suited to situations where significant changes and updates are required frequently. On the other hand, use of a flexible Attribute Management enterprise service where attributes can be easily managed, may be more responsive and thus, more operationally effective.

(Farroha and Farroha, 2012, p. 3)

((link) , p. 3)

Bibliography

1. (link)

See Also

false title label = ”stability-of-access-decision-factors”

RA

e-Identity

RP

Registration Authority

Credential Service Provider

IAM Management

Control Party

Identity Provider

Book end