**19SFC162- CLOUD SECURITY MODULE 4 NOTES**

**1. Draw the architecture of Identity and Access Management in the cloud and explain its essential features**

**Key components of identity and access management**

To create a secure cloud environment, you need to account for the following components of identity and access management:

* [User identity, authentication, and authorization service](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#useridentityauthenticationandauthorizationservice). Enables applications deployed to the cloud to externalize the authentication of users to a range of different identity providers
* [Multifactor authentication](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#multifactorauthentication). Combats identity theft by adding an additional level of authentication for application users
* [Directory services](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#directoryservices). Hosts the user profiles and associated credentials that are used to access applications
* [Reporting](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#reporting). Provides a user-centric view of access to resources or a resource-centric view of access by users
* [Audit and compliance](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#auditandcompliance). Validates implemented controls against an organization's security policy, industry compliance, and risk policies and to report deviations
* [User access management](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-identity-access-management#useraccessmanagementforadministratorsoperatorsanddevelopers). Enables cloud providers to manage user identities in cloud-based platforms, applications, and services

User identity, authentication, and authorization service

Authentication, or the identity service, enables applications deployed to the cloud to authenticate users at an application level, based on a range of identity providers.

For example, the identity service recognizes a subset or combination of the following identity providers:

* Cloud directory (hosted in the same cloud as the application)
* Social identity provider (such as Google, LinkedIn, Facebook, Twitter, or GitHub)
* Enterprise-hosted identity provider
* Cloud-hosted identity provider

With the proliferation of Software as a Service (SaaS) and API delivery models, API keys have emerged as another source of identities to accommodate.

IBM Cloud App ID helps you to easily add authentication to your web and mobile applications with few lines of code, and to secure your cloud-native applications and services on IBM Cloud. IBM Cloud App ID also helps you to manage user-specific data that you can use to build personalized application experiences.

IBM Cloud App ID is designed to make it simple for developers to quickly get authentication and authorization working, abstracting away complex security functions. You can use these key features of IBM Cloud App ID to integrate authentication into your application:

* Simple on-boarding wizard to create a working sample application with Google and Facebook authentication or by using email and password.
* Highly scalable cloud directory to store user records in the cloud.
* Quickly integrate authentication into your application by using client SDKs for iOS and Android, REST APIs, server SDKs for node.js and Swift, and a customizable login UI widget. For other languages such as Python, you can use the IBM Cloud App ID REST APIs.
* Secures cloud-native applications and services from unauthorized access by using authentication filters.
* Built with open standards (OAUTH2, OIDC).
* Store user data, like application preferences or information from public social profiles, and use it in your applications.
* Support engagement for both anonymous and authenticated users. If users start anonymously and later authenticate, applications can continue to use the information previously stored for them.

To read more about IBM Cloud App ID and to learn how to use it for your application user authentication scenarios, visit the [getting started](https://cloud.ibm.com/docs/services/appid?topic=appid-getting-started#gettingstarted&cm_mmc=IBMBluemixGarageMethod-_-MethodSite-_-10-19-15::12-31-18-_-ibm-cloud-app-id-getting-started#gettingstarted) page.

Multifactor authentication—or additional authentication controls—is used to combat increasing levels of identity theft. Examples of multifactor authentication include single-use passwords, certificates, and tokens.

To maintain the user experience while also improving login security, risk-based authentication controls are typically used. **Multifactor authentication**

These controls change the level of required authentication based on a user's location, past activity, operation being performed, preferences, or other factors.

Multifactor authentication is available as a built-in service in IBM Cloud infrastructure offerings.

For IBM Cloud environments, you can implement multifactor authentication into your environments indirectly through SAML. The third-party identity provider implements multifactor authentication on your behalf.

Directory services

Directory services support the identity service by hosting the user profiles and associated credentials that are used to access applications. Directory services can be used to host a range of information, for example:

* User identities and group or role membership
* Resource and service descriptions and locations
* Access policies

Directory services typically use a directory access protocol, for example, a lightweight directory access protocol (LDAP) and can be shared across components in an application, across applications, or across organizations.

**Cloud directory services**

Cloud directory services securely manage user profiles and their associated credentials and password policy inside a cloud environment. A directory service within a cloud means that applications hosted on the cloud do not need to use their own user repository.

The Cloud Directory service in [IBM Cloud App ID](https://cloud.ibm.com/docs/services/appid?topic=appid-cloud-directory#cd&cm_mmc=IBMBluemixGarageMethod-_-MethodSite-_-10-19-15::12-31-18-_-appid-config-clouddir#cd) lets users:

* Populate the registry with user information
* Have default or branded user interface for sign-up, sign-in, change or reset password
* Create customizable emails
* Use secured API for management

You can populate the registry with user information in several ways:

* Cloud directory admin interface. Add users on the Cloud Directory identity provider page.
* Bulk user load. Use Cloud Directory management APIs to bulk import users.
* Self-registry. Enable users to sign up on the Cloud Directory sign-in page.

**Reporting**

Reporting can provide a user-centric view of access to resources, or a resource-centric view of access by users. The reports often address:

* Which users have access to each resource
* Which access is being exploited by each user, and under what conditions
* Which users have changes access rights

Details about the reporting capabilities of IBM Cloud are described in the [Monitoring and intelligence](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-monitoring-and-intelligence) article.

**Audit and compliance**

Audit and compliance is an increasingly critical service within the identity and access management framework, both for the cloud provider and the cloud consumer. These processes are required for the auditor or risk officer to validate implemented controls against an organization's security policy, industry compliance, and risk policies and to report deviations.

Compliance standard such as HIPAA, PCI/DSS, and NERC are mandatory for specific industries, and an automated report helps organizations efficiently demonstrate compliance to these standards. However, cloud consumers must understand how the cloud provider fits within their overall workload compliance assessment.

**Auditing and compliance in IBM Cloud**

Audit logs are created for all successful and unsuccessful authentication attempts by application developers. Audit logs are created also for privileged access to Linux systems that host the containers where IBM Cloud applications run.

For all IBM Cloud deployments, IBM uses the IBM Security QRadar tools to consolidate Linux logs to monitor privileged access on Linux systems. IBM Cloud also uses IBM security information and event management (SIEM) to monitor successful and unsuccessful login attempts of application developers.

IBM Cloud auditing resources

* Refer to the [IBM Cloud documentation](https://cloud.ibm.com/docs/overview?topic=overview-security#security&cm_mmc=IBMBluemixGarageMethod-_-MethodSite-_-10-19-15::12-31-18-_-bmx-security#security) for more details on auditing, compliance, and other security related items.
* IBM Cloud is audited by a third-party security firm and meets all the requirements for ISO 27001. IBM Cloud works with independent auditors and third-party organizations to meet the industry's most stringent guidelines to provide reports and information for customer's own compliance needs. Learn more about the long list of [compliance standards that IBM Cloud meets](https://www.ibm.com/cloud/compliance#iso27001).

Read [Security policy, governance, risk, and compliance](https://www.ibm.com/cloud/garage/architectures/securityArchitecture/security-policy-governance-risk-compliance) for specific information about compliance.

**Enabling user and service access management**

The user and service management capability enables cloud providers to manage user and service identities in cloud-based platforms, applications, and services. With efficient user management, cloud-deployed applications can provision and de-provision customer, partner, and vendor user profiles with minimal human interaction. This streamlines access control based on the role, organization, and access policies defined by the owner.

**User access management for administrators, operators, and developers**

As outlined above, user accounts of administrators and developers give access to sensitive information, so potential attackers can manipulate applications.

To mitigate this risk, customers require maximum control over the whole lifecycle of these users. In particular, cloud owners want to control:

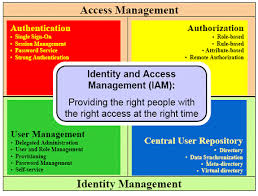
* Provisioning of users into the cloud. Customers want to control whom can access which resources in which role. In IBM Cloud, you can invite single or multiple users to your account and specify roles on resources for these invited users.
* Password policies. Customers must be able to control the usage of special characters, minimum password lengths, and similar settings.
* Multifactor authentication. Many companies want to use multifactor authentication like time-based, one-time-passwords (TOTP). One widely used implementation of TOTP is the "Google Authenticator" app for smartphones.
* De-provisioning access. When a user leaves the company or switches his or her role, you must be able to immediately revoke the user's permissions.

To meet these requirements, many customers use an internal solution like an enterprise-owned SAML identity provider. The SAML identity provider is accessible only through the enterprise network, so attackers are prevented from accessing the login screen. Often, SAML identity providers already support multifactor authentication. Use multifactor authentication capabilities inside the SAML identity provider. Some customers even use external service providers that manage their enterprise user accounts.

**2. Characterize 8 Hours Identity and Access Management functions with respect to cloud security**

* **Access management:** Access management refers to the processes and technologies used to control and monitor network access. Access management features, such as authentication, authorization, trust and security auditing, are part and parcel of the top ID management systems for both on-premises and cloud-based systems.
* **Active Directory (AD):** Microsoft developed AD as a user-identity directory service for Windows domain networks. Though proprietary, AD is included in the Windows Server operating system and is thus widely deployed.
* **Biometric authentication:** A security process for authenticating users that relies upon the user’s unique characteristics. Biometric authentication technologies include fingerprint sensors, iris and retina scanning, and facial recognition.
* **Context-aware network access control:** Context-aware network access control is a policy-based method of granting access to network resources according to the current context of the user seeking access. For example, a user attempting to authenticate from an IP address that hasn’t been whitelisted would be blocked.
* **Credential:** An identifier employed by the user to gain access to a network such as the user’s password, public key infrastructure (PKI) certificate, or biometric information (fingerprint, iris scan).
* **De-provisioning:** The process of removing an identity from an ID repository and terminating access privileges.
* **Digital identity:** The ID itself, including the description of the user and his/her/its access privileges. (“Its” because an endpoint, such as a laptop or smartphone, can have its own digital identity.)
* **Entitlement:** The set of attributes that specify the access rights and privileges of an authenticated security principal.
* **Identity as a Service (IDaaS):** Cloud-based IDaaS offers identity and access management functionality to an organization’s systems that reside on-premises and/or in the cloud.
* **Identity lifecycle management:** Similar to access lifecycle management, the term refers to the entire set of processes and technologies for maintaining and updating digital identities. Identity lifecycle management includes identity synchronization, provisioning, de-provisioning, and the ongoing management of user attributes, credentials and entitlements.
* **Identity synchronization:** The process of ensuring that multiple identity stores—say, the result of an acquisition—contain consistent data for a given digital ID.
* **Lightweight Directory Access Protocol (LDAP):** LDAP is open standards-based protocol for managing and accessing a distributed directory service, such as Microsoft’s AD
* **Multi-factor authentication (MFA):** MFA is when more than just a single factor, such as a user name and password, is required for authentication to a network or system. At least one additional step is also required, such as receiving a code sent via SMS to a smartphone, inserting a smart card or USB stick, or satisfying a biometric authentication requirement, such as a fingerprint scan.
* **Password reset:** In this context, it’s a feature of an ID management system that allows users to re-establish their own passwords, relieving the administrators of the job and cutting support calls. The reset application is often accessed by the user through a browser. The application asks for a secret word or a set of questions to verify the user’s identity.
* **Privileged account management:**  This term refers to managing and auditing accounts and data access based on the privileges of the user. In general terms, because of his or her job or function, a privileged user has been granted administrative access to systems. A privileged user, for example, would be able set up and delete user accounts and roles.Provisioning: The process of creating identities, defining their access privileges and adding them to an ID repository.
* **Risk-based authentication (RBA):** Risk-based authentication dynamically adjusts authentication requirements based on the user’s situation at the moment authentication is attempted. For example, when users attempt to authenticate from a geographic location or IP address not previously associated with them, those users may face additional authentication requirements.
* **Security principal:** A digital identity with one or more credentials that can be authenticated and authorized to interact with the network.
* **Single sign-on (SSO):** A type of access control for multiple related but separate systems. With a single username and password, a user can access a system or systems without using different credentials.
* **User behavior analytics (UBA):** UBA technologies examine patterns of user behavior and automatically apply algorithms and analysis to detect important anomalies that may indicate potential security threats. UBA differs from other security technologies, which focus on tracking devices or security events. UBA is also sometimes grouped with entity behavior analytics and known as UEBA.

**3.Illustrate the Identity and Access Management (IAM) Model with its core diagram**



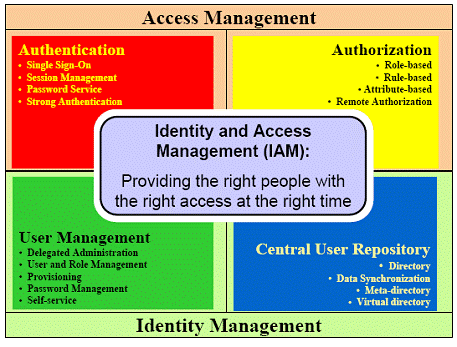
Identity and Access Management (IAM)

**Why have enterprises started to implement IAM?**

IAM has emerged as a critical foundation for realizing the business benefits in terms of cost savings, management control, operational efficiency and business growth of enterprises.  Enterprises need to manage access to information and applications scattered across internal and external application systems.  Moreover, they must provide this access for a growing number of identities, both inside and outside the organization, without compromising security or exposing sensitive information.  In addition, they shall have to ensure the correctness of data in order for the IAM Framework to function properly.

**What is an IAM Framework?**

An IAM Framework can be divided into four major areas: Authentication, [Authorization](http://en.wikipedia.org/wiki/Authorization), User Management and Central User Repository.  The IAM components are grouped under these four areas.  The ultimate goal of the IAM Framework is ‘*to provide the right people with the right access at the right time‘* (see the diagram below ‘What is Identity & Access Management?’).



What is an IAM Framework?

* **Authentication**

Authentication is the area through which a user provides sufficient credentials to gain initial access to an application system or a particular resource.  Once a user is authenticated, a session is created and referred during the interaction between the user and the application system until the user logs off or the session is terminated by other means (e.g. timeout).   
It usually comes with a password service module when the user ID /password authentication method is used.  By centrally maintaining the session of a user, it provides Single-Sign-On service so that the user needs not logon again on accessing another application system or resource governed under the same IAM Framework.

* **Authorization**

Authorization is the area that determines whether a user is permitted to access a particular resource.  Authorization is performed by checking the resource access request, typically in the form of an URL in web-based application, against authorization policies that are stored in an IAM policy store.  
Authorization is the core area that implements role-based access control.  Moreover, the authorization model could provide complex access controls based on data or information or policies including user attributes, user roles /groups, actions taken, access channels, time, resources requested, external data and business rules.

* **User Management**

This area comprises of user management, password management, role/ group management and user /group provisioning. It defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges.  One of its components is user life cycle management that enables an enterprise to manage the lifespan of a user account, from the initial stage of provisioning to the final stage of de-provisioning.  
Some of the user management functions should be centralized while others should be delegated to end users. Delegated administration allows an enterprise to directly distribute workload to user departmental units.  Delegation can also improve the accuracy of system data by assigning the responsibility of updates to persons closest to the situation and information.  
Self-service is another key concept within user management.  Through self-profile management service an enterprise benefits from timely update and accurate maintenance of identity data.  Another popular self-service function is self-password reset, which significantly alleviates the help desk workload to handle password reset requests.  
User management requires an integrated workflow capability to approve some user actions such as user account provisioning and de-provisioning.

* **Central User Repository**

Central User Repository stores and delivers identity information to other services, and provides service to verify credentials submitted from clients.  The Central User Repository presents an aggregate or logical view of identities of an enterprise.    
Directory services adopting LDAPv3 standards have become the dominant technology for Central User Repository. Both meta-directory and virtual directory can be used to manage disparate identity data from different user repositories of applications and systems.  A meta-directory typically provides an aggregate set of identity data by merging data from different identity sources into a meta-set.  It usually comes with a 2-way data synchronization service to keep the data in synchronization with other identity sources.  A virtual directory delivers a unified LDAP view of consolidated identity information, and multiple databases containing different sets of users are combined in real time behind the scene.

**How an organization can benefit from implementing IAM?**

Business value improves when an organization is able to appropriately protect its information assets.  IAM provides the kind of reliability and accessibility to user access control that is imperative to most e-business sites these days.  
IAM can enable new users, employees or contractors to gain necessary information from applications so that they can be productive and at the same time allow the organization to keep a check on the access rights as their roles require.  
The key benefits of implementing IAM are as follows:

* Facilitating the identification of loop holes in control points by phased approach of providing access controls,
* Enhancing business value by improving security,
* Improving compliance with various industry regulations and creating opportunities for new business initiatives,
* Reducing overall effort of IT administration,
* Improving the productivity of employees and other members,
* More effective customer support,
* Streamlining IT management in large organizations for enhancing overall ROI for business,
* Providing scalable approach that enables IT expansion in growing organizations.

**4.Examine the core concepts of Identity Federation in Identity and Access Management(IAM)**

Federated identity management is an arrangement that can be made between two or more trust domains, to allow users of these trust domains to access applications and services using the same digital identity. An identity such as this is known as federated identity and the use of such a solution pattern is known as identity federation.

Federated identity management is built upon the basis of trust between two or more domains. For example, a trust domain can be a partner organization, a business unit, a subsidiary, etc.

In any digital organization today, identity and access management (IAM) is a specialized function that is delegated to a service provider known as the identity broker. An identity broker is a service provider that specializes in brokering access control between multiple service providers (also referred to as relying parties). Federated identity management is an arrangement that is made between two or more such identity brokers across organizations.

An identity broker could be known by more specific names depending on the role it plays in federated identity management. These names are not quite standardized across the industry, although used in common parlance and you may find people using these names interchangeably. Therefore it is important to specify these names with the relevant context whenever they are used and depending on the arrangement, an identity broker may play more than one role.

These roles include:

1. Identity Provider
2. Resident Identity Provider
3. Federated Identity Provider
4. Federation Provider
5. Resident Authorization Server

An identity provider is an identity broker that is responsible for asserting digital identities with claims for service providers to consume.

A resident identity provider is defined with respect to a digital identity, and is the identity provider responsible for asserting the digital identities within its trust domain. Sometimes this is also referred to as local identity provider or incumbent identity provider.

A federated identity provider is defined with respect to a trust domain, and is responsible to assert digital identities that belong to another particular trust domain. A trust relationship is established between the two identity providers.

The term federation provider is often used to denote an identity broker that specializes in mediating IAM operations between multiple service providers and multiple identity providers, based on trust relationships.

A resident authorization server is defined with respect to a service provider, and is where the logical representation of the application or service provider resides. It is responsible for authenticating and authorizing the application or service provider for the requested access.

**Identity federation provides the following benefits:**

1. Users are required to remember only one set of credentials which provides a seamless user experience.
2. Single sign-on is supported in most implementations.
3. Avoids administrative overhead by delegating account and password management responsibilities to the resident identity provider, instead of having multiple identity silos to be managed.
4. Simplifies data management and storage costs.
5. Avoids privacy and compliance burdens.

Following are some examples of federated identity management use cases:

1. Provide access to users from supplier, distributor, and partner networks.
2. Provide access to new users outside the traditional organization perimeter after mergers and acquisitions.
3. Provide access to users from commercial identity providers like banks, for example, Third Party Payment Providers (TPPs) in PSD2.
4. Provide access to citizens using national identity provider, for example, DigiD, Emirates ID, etc.
5. Provide access to users who own a public organization ID, for example, ORCID ID.
6. Social Login (sign-up/sign-in/connect), for example, Facebook, Google, LinkedIn, etc.
7. As a temporary arrangement for supporting transitioning between IAM systems.

**Inbound and Outbound Identity Federation**

Identity Federation is broadly categorized into two areas:

1. Inbound Identity Federation
2. Outbound Identity Federation

In an identity federation flow, an identity broker which receives an assertion from another identity broker is known as inbound identity federation. In other words, inbound identity federation allows you to provide access to your applications and services to identities that are outside your organization’s traditional boundary/trust domain.

Similarly, an identity provider which produces an assertion to be consumed by another identity broker is known as outbound identity federation. Outbound identity federation allows identities that you manage to access applications and services that are outside your traditional organization boundary/trust domain.

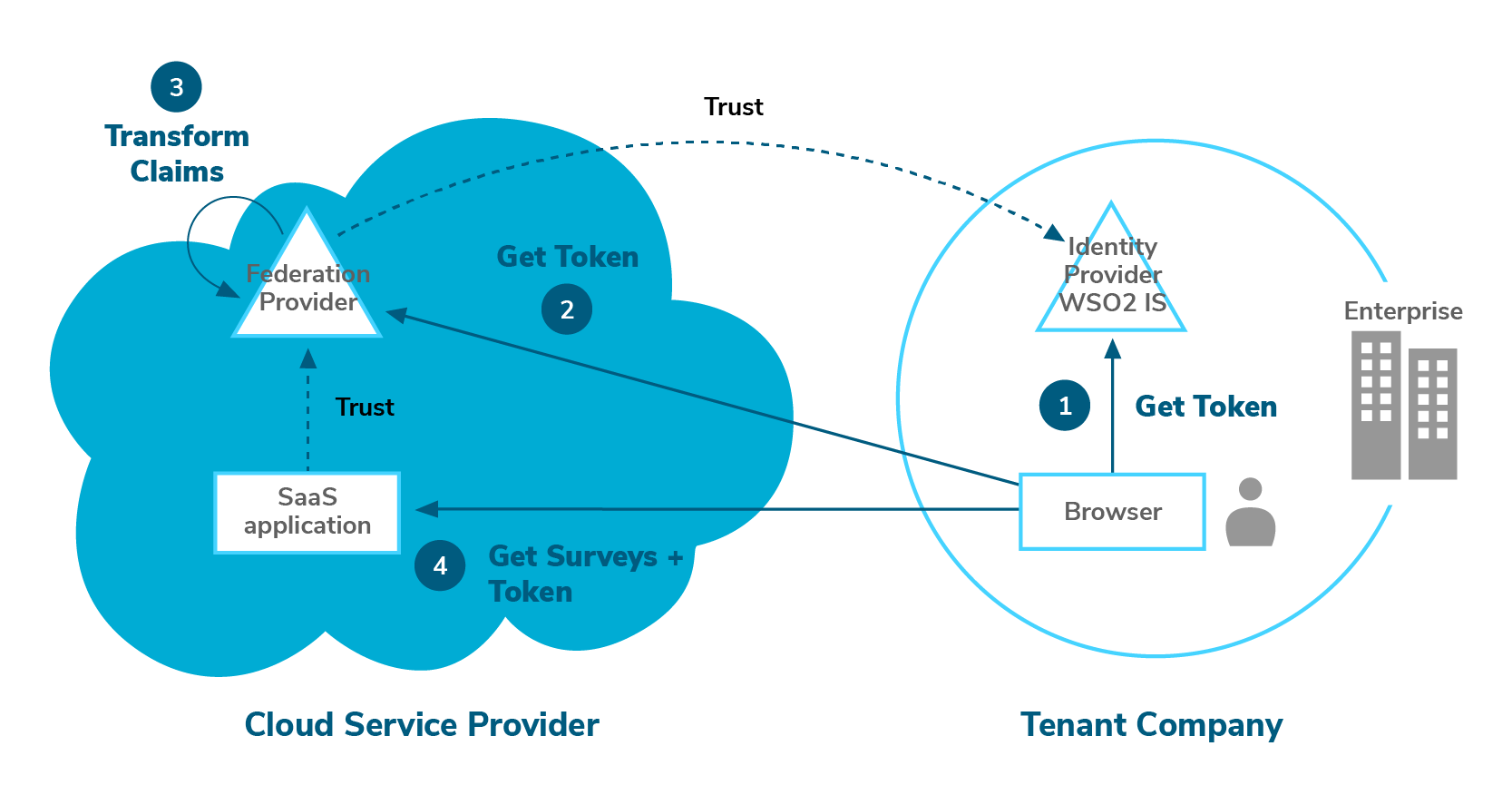


Figure 1: Identity Federation between the Enterprise and SaaS Application

Figure 1 illustrates an identity federation arrangement between an enterprise and a SaaS application. The SaaS application is hosted in Azure cloud and its authentication is delegated to a federation provider. The enterprise is a tenant in the SaaS application and the federation provider. The enterprise identity provider (ADFS) is configured as a federated identity provider in the respective tenant of the federation provider in Azure cloud. Thus, a trust is established between the cloud tenant’s federation provider and the enterprise identity provider. Therefore the users in the enterprise identity provider will be able to login to the respective tenant of the SaaS application using their identities in the enterprise identity provider.

The flow described is with respect to authentication. However, in order for users to gain complete access they need to pass authorization as well. Authorization may or may not be part of this federation arrangement.

**Identity Federation vs. Single Sign-On**

Most federated identity management solutions are implemented in a way in which users are not required to prove their identity more than once per logged-in session. Single sign-on is not synonymous with identity federation. However, it is a by-product of the way identity federation is implemented.

On the other hand, not all single sign-on implementations can be categorized as identity federation. For example, Integrated Windows Authentication (IWA) based on kerberos network authentication protocol, is an example of a single sign-on implementation across applications and services, but not considered an example of identity federation because it is limited to a particular network.

**Bring Your Own Identity**

The phrase bring your own identity (BYOID) became popular following the trend of using social identities to gain access to applications and services. Although BYOID is commonly used in the context of social identities, the concept applies to any federated digital identity issued by the government, non-government organizations or enterprises.

Use cases 3, 4, 5, and 6 are all examples of BYOID, and are commonly found in Customer IAM (CIAM). They can be further divided as BYOID for sign-up, sign-in, and to connect. Although technically all these 3 use cases follow the same kind of flow, there are subtle differences in the objectives of these use cases.

The objective of “BYOID for sign-up” is to improve the user experience of the self sign-up process by retrieving a part of or complete profile information that is necessary to create an account for the user in the intermediary identity broker, using an identity managed by a third party.

The objectives of “BYOID for sign-in” is to make the login flow as smooth as possible to the end-user with minimal prompts for additional input as possible. BYOID for sign-in doesn’t necessarily have to have a local account provisioned in the intermediary identity brokers.

The objective of “BYOID to connect” is simply to enrich/fill the local user profile with additional/missing information.

**Federated Account Linking**

One of the key features of a federation provider is linking digital identifiers of a single identity in multiple federated identity providers to a digital identifier in the resident identity provider. This is known as federated account linking.

Without federated account linking, a federation provider will simply only mediate between a service provider and a federated identity provider. This mode of federation is commonly seen in non-critical applications and services such as public forums, downloading marketing material, etc.

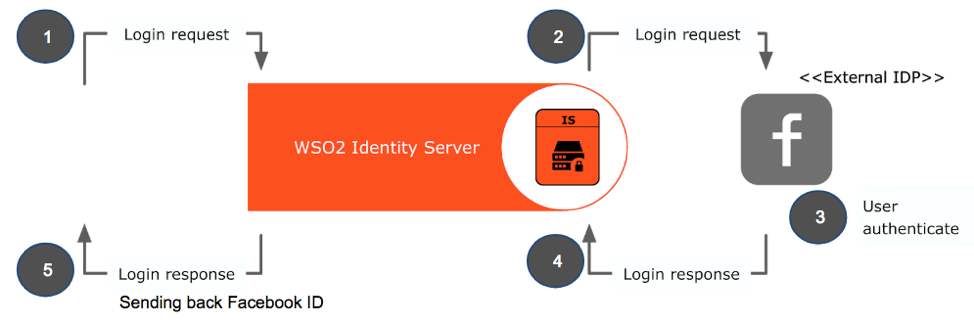


Figure 2: Federated login without account linking

However with federated account linking, in addition to mediating, the federation provider may also provide features such as account management, password management, and entitlements management.

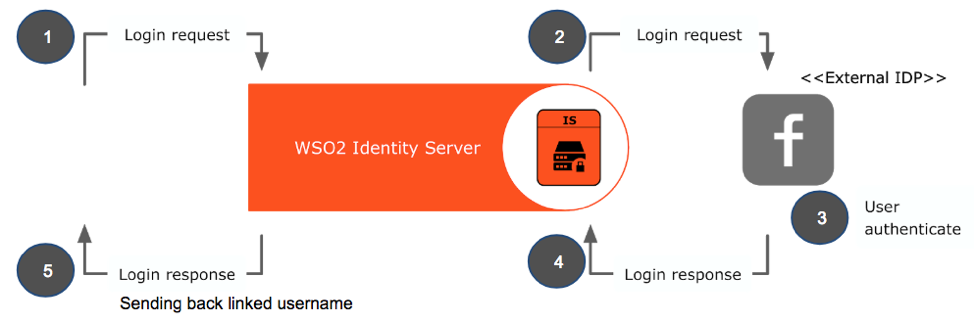


Figure 3: Federated login with account linking

**Just-In-Time Account Provisioning**

Just-In-Time account provisioning technique is used to setup an account for the user in an intermediary identity broker on the fly. Just-in-Time account provisioning is a key part of just-in-time account linking.

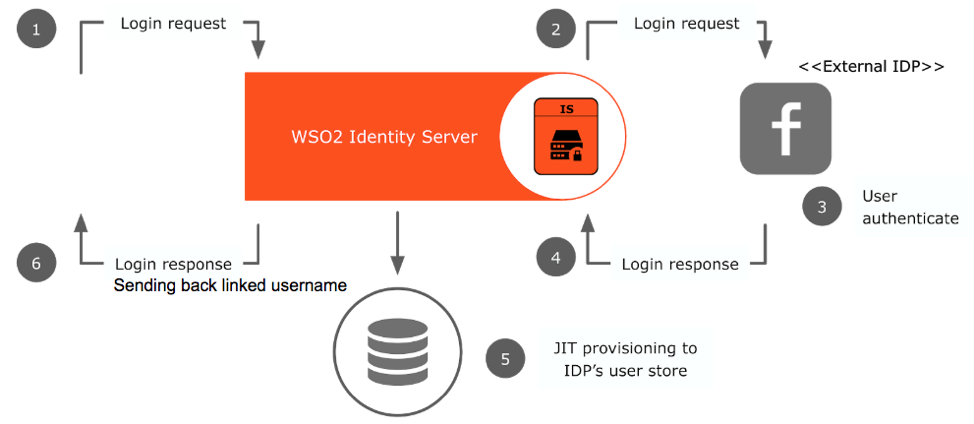


Figure 4: Federated login with just-in-time account provisioning

**Just-In-Time Password Provisioning**

Just-In-Time Password provisioning is an optional step of just-in-time account provisioning. The need for this type of provisioning generally depends on the combined account and password policies of the organization and the applications the user will be accessing. If you decide to provision a new password for the local account, it is also optional to allow the user to continue signing in using the federated identity.

**Home Realm Discovery**

Federating with a single identity provider is not sufficient for today’s enterprise needs. Typically there are multiple federated identity providers (realms) that are configured, due to the need of supporting multiple partners or multiple social login options. In such cases choosing the resident identity provider (home realm) for the particular user who is trying to access the application or service becomes a challenge, especially in terms of user experience.

Home Realm Discovery (HRD) is the process of identifying the resident identity provider of a particular user in order to authenticate the user and assert the user's identity with claims. HRD was originally a Microsoft term but the concept applies to all modern identity federations. There are no standards around how HRD should be implemented, each vendor has their own style and as such, it’s hard to support portability.

HRD methods can be automatic or involve manual user interaction. Following are some commonly used methods for HRD:

1. Present a list of options to the user to choose from.
2. Identifier first login — Prompt the user to enter his/her identifier and resolve the identity provider based on the identifier. For example, if identifier is johann@gmail.com, we would know that the identity provider for Johann is Google, initiate an authentication request to Google, and ideally the identifier would be pre-filled in the Google login form so that the user does not have to re-enter his identifier.
3. Selective home realm discovery — Limit the identity providers that are used for a specific service provider. This can be useful in situations where there are multiple federated identity providers that you trust, but have service providers that will only be used and access by users in a specific subset of identity provider.
4. Use HTTP query parameters added by the service provider.
5. Use the IP address of the user’s device. For example, intranet users must login using local accounts in AD, whereas Internet users must login from upstream identity provider with multi-factor authentication for additional security.
6. Use headers added via an intercepting proxy server.
7. Use cookies to remember the realm the user previously selected on the device. If cookies are not found fallback to manual methods.
8. The federated identity provider can itself be a federation provider who will in-turn federate with other identity providers. In those kind of situations prompting the user to provide information for HRD at each intermediary federation provider, could be considered poor user experience. Therefore in those situations, it may be required to collect all possible information from the user upfront to be routed to the correct resident identity provider.

**5.Classify various Identity Provisioning Recommendations in Cloud security**

**6.Investigate the key features that differentiates the Authentication for SaaS and Paas customers**

**SaaS:** this particular model is focused on managing access to applications. For example, policy controls may dictate that a sales person can only download particular information from sales CRM applications. For example, they are only permitted to download certain leads, within certain geographies or during local office working hours. In effect, the security officer needs to focus on establishing controls regarding users' access to applications.

**PaaS:** the primary focus of this model is on protecting data. This is especially important in the case of storage as a service. An important element to consider within PaaS is the ability to plan against the possibility of an outage from a Cloud provider. The security operation needs to consider providing for the ability to load balance across providers to ensure fail over of services in the event of an outage. Another key consideration should be the ability to encrypt the data whilst stored on a third-party platform and to be aware of the regulatory issues that may apply to data availability in different geographies.

For CSOs focused on PaaS

Challenge #1: **Protect private information before sending it to the Cloud**

There are already many existing laws and policies in place which disallow the sending of private data onto third-party systems. A Cloud Service Provider is another example of a third-party system, and organizations must apply the same rules in this case. It's already clear that organizations are concerned at the prospect of private data going to the Cloud. The Cloud Service Providers themselves recommend that if private data is sent onto their systems, it must be encrypted, removed, or redacted. The question then arises "How can the private data be automatically encrypted, removed, or redacted before sending it up to the Cloud Service Provider". It is known that encryption, in particular, is a CPU-intensive process which threatens to add significant latency to the process.

Any solution implemented should broker the connection to the Cloud Service and automatically encrypt any information an organization doesn't want to share via a third party. For example, this could include private or sensitive employee or customer data such as home addresses or social security numbers, or patient data in a medical context. CSOs should look to provide for on-the-fly data protection by detecting private or sensitive data within the message being sent up to the Cloud Service Provider, and encrypting it such that only the originating organization can decrypt it later. Depending on the policy, the private data could also be removed or redacted from the originating data, but then re-inserted when the data is requested back from the Cloud Service Provider.

For CSOs Focused on SaaS

Challenge #2: **Don't replicate your organization in the Cloud**

Large organizations using Cloud services face a dilemma. If they potentially have thousands of employees using Cloud services, must they create thousands of mirrored users on the Cloud platform? The ability to circumvent this requirement by providing single sign-on between on-premises systems and Cloud negates this requirement.

Users with multiple passwords are also a potential security threat and a drain on IT Help Desk resources. The risks and costs associated with multiple passwords are particularly relevant for any large organization making its first foray into Cloud Computing and leveraging applications or SaaS. For example, if an organization has 10,000 employees, it is very costly to have the IT department assign new passwords to access Cloud Services for each individual user. For example, when the user forgets their password for the SaaS service, and resets it, they now have an extra password to take care of.

By leveraging single sign-on capabilities an organization can enable a user to access both the user's desktops and any Cloud Services via a single password. In addition to preventing security issues, there are significant costs savings to this approach. For example, single sign-on users are less likely to lose passwords reducing the assistance required by IT helpdesks. Single sign-on is also helpful for the provisioning and de-provisioning of passwords. [Editor's note: Also read [Role management software—how to make it work for you](http://www.csoonline.com/article/447619/role-management-software-making-it-work-for-you).] If a new user joins or leaves the organization there is only a single password to activate or deactivate vs. having multiple passwords to deal with. In a nutshell, the danger of not having a single sign-on for the Cloud is increased exposure to security risks and the potential for increased IT Help Desk costs, as well the danger of dangling accounts after users leave the organizations, which are open to rogue usage.

For CSOs focused on PaaS

Challenge #3: **Keep an Audit Trail**

Usage of Cloud Services is on a paid-for basis, which means that the finance department will want to keep a record of how the service is being used. The Cloud Service Providers themselves provide this information, but in the case of a dispute it is important to have an independent audit trail. Audit trails provide valuable information about how an organization's employees are interacting with specific Cloud services, legitimately or otherwise!

The end-user organization could consider a Cloud Service Broker (CSB) solution as a means to create an independent audit trail of its cloud service consumption. Once armed with his/her own records of cloud service activity the CSO can confidently address any concerns over billing or to verify employee activity. A CSB should provide reporting tools to allow organizations to actively monitor how services are being used. There are multiple reasons why an organisation may want a record of Cloud activity, which leads us to discuss the issue of Governance.

**7.Identify the various concepts that builds up the Authentication for IaaS customers**

**8.Draw and explain briefly the Enterprise Architecture with IDaaS**

**1.What is Identity as a Service?**

Identity as a Service refers to the *identity and access management service* which serve through the cloud by subscribing into it. It can be purchased as a subscription-based managed service. It has [**virtualized hardware**](https://data-flair.training/blogs/hardware-virtualization-in-cloud-computing/) and it can be accessed without any complexities. The service provider can host an application by charging some amount and provide access to the clients as per their demand.

They provide the service in a secure manner as the data is secured and work can share with anyone else. It relies so much on the active directory and lightweight directory access protocol for their IAM services.

In addition, there are far more things like devices and objects which configures their identity in different ways. These identities are creating and storing in the databases, which can find in the network with the help of network identity.

**2. Associated Problems with IdaaS**

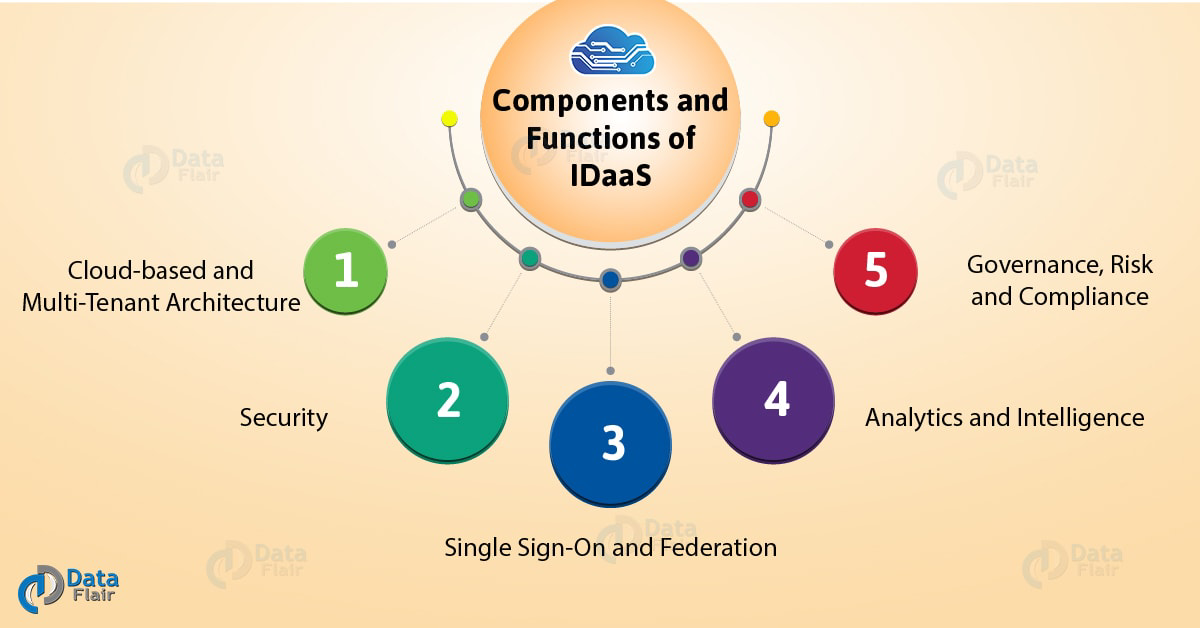
Employees are facing several login problems such as remembering the username and password to access the data. If the employee resigns, the data stored on the computer must be completely erased. This can be done with the help of IdaaS, which also used for electronic transactions.

**3. What is Single Sign-On (SSO)?**

Single Sign-on is an authentication process, with a user can access multiple applications. This requires only one set of log-in information. With the help of LAN, the client can access multiple resources. Through SSO, a user doesn’t have to log in again and again. The mechanism of SSO varies from application to application. Single Sign-On can use with other authentication techniques which can be either smart cards or OTP tokens.

**4. Components and Functions of IDaaS**

Here, we are going to talk about several components and functions of Identity as a Service, let’s discuss them one by one:



*Identity as a Service (IDaas) – Components and Functions*

**i. Cloud-based and multi-tenant architecture**

A multitenant architecture provides lots of benefit such as the vendor can issue updates, [**security fixtures**](https://data-flair.training/blogs/cloud-security/), and improves performance. It also modifies the capability to manage access provision and governance effectively.

**ii. Security (management and architecture)**

The most important need of IDaaS is identity and access management. IDaaS in [**Cloud computing offer features**](https://data-flair.training/blogs/features-of-cloud-computing/) like multi-factor authentication, digital access cards, and biometrics. These features help to easily retrieve the information in a secure manner.

**ii. Single Sign-On and Federation**

SSO enhance the experience of the end user while maintaining security and availability of the network to users as intended. The user can use the safest password combination without working hard to remember, which is used to access services on regular basis. It also benefits in another way, as it helps to manage secure authentication for third-party cloud services.

**iii. Analytics and intelligence**

Analytics and intelligence capabilities are used to report the use of access privileges in the context of multifaceted relationships. This relationship is between users, their roles and responsibilities, job function, and data usage. This information allows the organization to identify anomalies for former employee’s awesome specific type of workforce segment.

**iv. Governance, risk, and compliance**

The governance, risk and compliance are supported by modifying the automation and intelligence capabilities of an Identity as a Service system. This IDaaS function helps an organization to define and automate the application specific processes, which will get familiar with the access and usage patterns.

**5. How SSO Works?**

After the introduction, let’s talk about working of Single Sign-On:

* With the help of username and password, the user log-in to the cloud.
* By the authentication server, a ticket will return.
* The ticket sends to the intranet server.
* Now, a ticket is further forwarded to the authentication server by the intranet.
* Security credentials of the user are sent back to the intranet server.

**6. Advantages of SSO**

It’s time to list down all the benefits of SSO in Identity as a Service:

* Manages local and remote applications along with the desktop flow.
* Removes re-authentication and improves productivity.
* The database is user-friendly and flexible which benefits in many ways.
* Serves detailed user access reporting.

**7. Disadvantages of IDaaS**

There are several disadvantages to Identity as a Service. Provisioning identity on the website, with software like active directory domain services, are often full of prices. The team should pay hosting fees; monitor the extra turf on premises for network security; established continue servers; purchase, upgrade, and install software; keep a copy data regularly; VPNs and many more. With IDaaS, prices drop to the subscription fee and therefore the administration work. That’s it.

ROI for Identity as a Service includes an enhanced version of cybersecurity. Besides savings, it includes improvement in cybersecurity and saved time with quicker logins and fewer word resets. The improved security will keep corporations from facing a hack or breach that may topple their business.

**8. Applications of Identity as a Service**

There are numerous technologies which comprise IDaaS. Accommodative multi-factor authentication is one such used. This is often a feature wherever users submit multiple factors to realize entry to the network. Thus increasing security over single-factor authentication, and dynamically access will grant, depending on what quantity risk users present.

**9.Investigate the various IDaaS Security Recommendations**

We live and work in an increasingly evolving digital environment. Enterprises continue to embrace the power of digital transformation for more efficient communications, business processes, and profitability. Cloud and mobile apps proliferate wildly. Yet the growing cloud adoption rate and the subsequent enterprise IT environment changes it requires challenges traditional IAM solutions.

Bluntly put, traditional identity management solutions don’t possess the capabilities or the infrastructure to support cloud or mobile platforms or applications. Instead, enterprises must select an IDaaS solution which provides the Zero-Trust security necessary to properly protect the cloud.

How can your business pick the right IDaaS solution for your enterprise? What factors should you consider as you plan to bring your identity and access management to the cloud? We read “[Top Six Considerations When Choosing an Identity as a Service (](https://solutionsreview.com/identity-management/idaptive-top-six-considerations-when-choosing-an-identity-as-a-service-idaas-solution-for-zero-trust-security/)IDaaS) Solution for Zero Trust Security,” a white paper by IDaaS provider Idaptive. Here’s just some of what we learned:

**What is Zero-Trust?**

According to [Idaptive](https://solutionsreview.com/identity-management/idaptive-top-six-considerations-when-choosing-an-identity-as-a-service-idaas-solution-for-zero-trust-security/), Zero-Trust Security involves enterprise user authentication through capabilities such as single sign-on (SSO), multi-factor authentication (MFA), and enterprise mobility management (EMM. Additionally, a Zero-Trust security applies context-aware policy to help ensure the legitimacy of users’ authentication.

Zero-Trust also ties into the Principle of Least Privilege, a key aspect of next-generation identity and access management. The Principle of Least Privilege mandates users only have the permissions they *absolutely need* to perform their general job duties and nothing more. This ensures stolen or abused user credentials can only cause a contained amount of damage.

If users need permissions for temporary projects, they can receive them on a limited-time basis, and even then the Principle of Least Privilege applies!

**Never Neglect Single Sign-On**

According to the National Institute of Standards and Technology, the average user undergoes 23 authentication events per day.

That’s quite a few! No wonder so many employees neglect password security best practices; trying to keep track of so many passwords for so many logins must prove a daunting task!

Indeed, credentials reuse and weak passwords continue to plague enterprises’ identity management policies. Furthermore, mobile and remote workers run into their own login issues, as logging in with a password on a mobile device is an exercise in frustration.

While some of these password issues stem from entrenched employee password creation practices, Single Sign-On can help solve many of them!

A major capability in IAM, Single Sign-On (SSO) allows users to log into an app hosted on any environment using a single or federated identity; for enterprise logins, this can be their Active Directory ID.

SSO removes the necessity of complex or weak passwords for users’ logins. Furthermore, it facilitates the user experience and streamlines business processes, as it reduces overall login time. Therefore, your IDaaS solution should provide SSO capabilities which unify all of your business applications, regardless of their IT environment (cloud or on-premises).

Ideally, your IDaaS-provided Single Sign-On should allow authenticated users one-click cloud access and Zero Sign-On for mobile devices. Identity Federation may also contribute positively to your cloud identity security policies.

**App Access Lifecycle Management**

Lifecycle management concerns itself with how your users enter, progress, and exit your enterprise over the course of their careers; their access permissions must adapt to their evolving job descriptions, granting them access to the resources they need to complete their functions.

Your ideal IDaaS solution should allow your enterprise to easily and automatically provision employees with the proper permissions during the onboarding process; additionally, IDaaS should also help with deprovisioning employees’ credentials during the offboarding process.

The automation achieved through an [IDaaS solution](https://solutionsreview.com/identity-management/idaptive-top-six-considerations-when-choosing-an-identity-as-a-service-idaas-solution-for-zero-trust-security/) relieves some of the burdens on your IT security team, ultimately saving you time and resources. Provisioning properly when the employee first becomes onboarded saves your helpdesk time normally spent on fixing permissions issues.

IDaaS can help provision and deprovision identities to cloud-based applications as well as on-premises applications.

**More Time to Focus on What Really Matters**

The first benefit of a comprehensive IAM platform is the power you gain from managing your IT environment from a single pane of glass. You no longer have to suffer through piecemeal processes that are inefficient and prone to human error, and you can gift your end users with a single set of credentials to access everything they need. Everybody earns more time to work on what truly matters. However, this [increase in productivity](https://jumpcloud.com/resources/jumpcloud-increases-productivity-5-ways/) doesn’t mean a decrease in security. In fact it’s just the opposite, which brings us to the next benefit.

**Stronger Security**

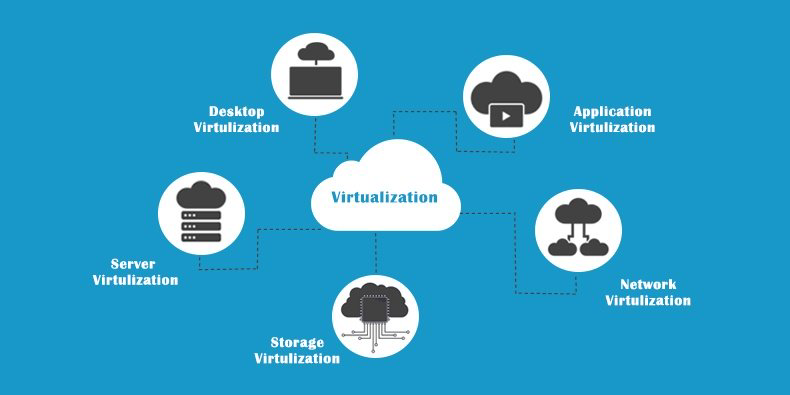
With a modern IDaaS solution, you’ll be able to tightly control access and centrally increase security through features such as password complexity management, 2FA, and SSH keys among others. With identities being the number one attack vector, identity security features such as these are instrumental to your game plan for protecting your environment. Securing identities is just one way a more comprehensive IDaaS solution can help protect your IT environment, though. It can also help you fortify systems, WiFi, and data, making it easier to implement a [Zero Trust Security approach](https://jumpcloud.com/resources/zero-trust-security/) across your entire IT environment.

**Freedom of Choice**

The last benefit we will discuss in this article is the ability to choose the IT resources that make the most sense for you and your users. After all, no two IT environments look the same, so it doesn’t make sense to conform all IT organizations into leveraging the same set of IT resources. When a company gets to use the best tools for their situation, the upside is an increase in agility and speed which in turn often leads to having a more competitive position in your market.

**10.Classify the different characteristics of Hardware Virtualization, Software Virtualization, Memory Virtualization in cloud security**

The Different Types of Virtualization in Cloud Computing – Explained



Although virtualization, as a form of technology has existed since the 1960s, only recently with the advent of [**cloud computing**](https://redswitches.com/enterprise-solutions/private-cloud/) has it become a staple in the vocabulary of those involved in the IT industry. By offloading hardware requirements and utility costs, it can rapidly transform a company’s infrastructure and improve its efficiency by itself. Virtualization in cloud computing allows you to run multiple applications and operating systems on the same server, thereby providing for efficient resource utilization and reducing costs.

**What Is Virtualization?**

Virtualization is the process of creating a virtual environment on an existing server to run your desired program, without interfering with any of the other services provided by the server or host platform to other users. The Virtual environment can be a single instance or a combination of many such as operating systems, Network or Application servers, computing environments, storage devices and other such environments. The concept of virtualization will be easily understood after going through the different types if virtualization later in this article.

**What Are The Benefits Of Virtualization?**

Numerous benefits are provided by virtualization which includes, reduction in costs, efficient utilization of resources, better accessibility and minimization of risk among others.

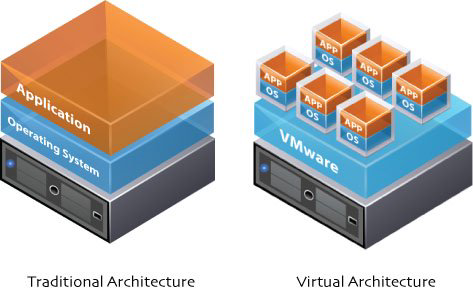
**Benefits for Companies**

1. Removal of special hardware and utility requirements
2. Effective management of resources
3. Increased employee productivity as a result of better accessibility
4. Reduced risk of data loss, as data is backed up across multiple storage locations

**Benefits for Data Centers**

1. Maximization of server capabilities, thereby reducing maintenance and operation costs
2. Smaller footprint as a result of lower hardware, energy and manpower requirements

**How Does Virtualization Work?**



Access to the virtual machine and the host machine or server is facilitated by a software known as Hypervisor. Hypervisor acts as a link between the hardware and the virtual environment and distributes the hardware resources such as CPU usage, memory allotment between the different virtual environments.

**Also Read** - [**Bare Metal Server Vs. Virtualization - What Do We Know ?**](https://www.redswitches.com/blog/bare-metal-server-vs.-virtualization-what-do-we-know)

What types of virtualization are there?

Virtualization can take many forms depending on the type of application use and hardware utilization. The main types are listed below:

**Hardware Virtualization**

Hardware virtualization also known as hardware-assisted virtualization or server virtualization runs on the concept that an individual independent segment of hardware or a physical server, may be made up of multiple smaller hardware segments or servers, essentially consolidating multiple physical servers into [**virtual servers**](https://redswitches.com/blog/small-businesses-reduce-operating-cost-using-vps/) that run on a single primary physical server. Each small server can host a virtual machine, but the entire cluster of servers is treated as a single device by any process requesting the hardware. The hardware resource allotment is done by the hypervisor. The main advantages include increased processing power as a result of maximized hardware utilization and application uptime.

**Subtypes:**

* Full Virtualization – Guest software does not require any modifications since the underlying hardware is fully simulated.
* Emulation Virtualization – The virtual machine simulates the hardware and becomes independent of it. The guest operating system does not require any modifications.
* Paravirtualization – the hardware is not simulated and the guest software run their own isolated domains.

**Software Virtualization**

Software Virtualization involves the creation of an operation of multiple virtual environments on the host machine. It creates a computer system complete with hardware that lets the guest operating system to run. For example, it lets you run Android OS on a host machine natively using a Microsoft Windows OS, utilizing the same hardware as the host machine does.

**Subtypes:**

* Operating System Virtualization – hosting multiple OS on the native OS
* Application Virtualization – hosting individual applications in a virtual environment separate from the native OS
* Service Virtualization – hosting specific processes and services related to a particular application

**Memory Virtualization**

Physical memory across different servers is aggregated into a single virtualized memory pool. It provides the benefit of an enlarged contiguous working memory. You may already be familiar with this, as some OS such as Microsoft Windows OS allows a portion of your storage disk to serve as an extension of your RAM.

**Subtypes:**

* Application-level control – Applications access the memory pool directly
* Operating system level control – Access to the memory pool is provided through an operating system

**Storage Virtualization**

Multiple physical storage devices are grouped together, which then appear as a single storage device. This provides various advantages such as homogenization of storage across storage devices of multiple capacity and speeds, reduced downtime, load balancing and better optimization of performance and speed. Partitioning your hard drive into multiple partitions is an example of this virtualization.

**Subtypes:**

* Block Virtualization – Multiple storage devices are consolidated into one
* File Virtualization – Storage system grants access to files that are stored over multiple hosts

**Data Virtualization**

It lets you easily manipulate data, as the data is presented as an abstract layer completely independent of data structure and database systems. Decreases data input and formatting errors.

**Network Virtualization**

In network virtualization, multiple sub-networks can be created on the same physical network, which may or may not is authorized to communicate with each other. This enables restriction of file movement across networks and enhances security, and allows better monitoring and identification of data usage which lets the network administrator’s scale up the network appropriately. It also increases reliability as a disruption in one network doesn’t affect other networks, and the diagnosis is easier.

Subtypes:

* Internal network: Enables a single system to function like a network
* External network: Consolidation of multiple networks into a single one, or segregation of a single network into multiple ones

**Desktop Virtualization**

This is perhaps the most common form of virtualization for any regular IT employee. The user’s desktop is stored on a remote server, allowing the user to access his desktop from any device or location. Employees can work conveniently from the comfort of their home. Since the data transfer takes place over secure protocols, any risk of data theft is minimized.

**Which Technology to use?**

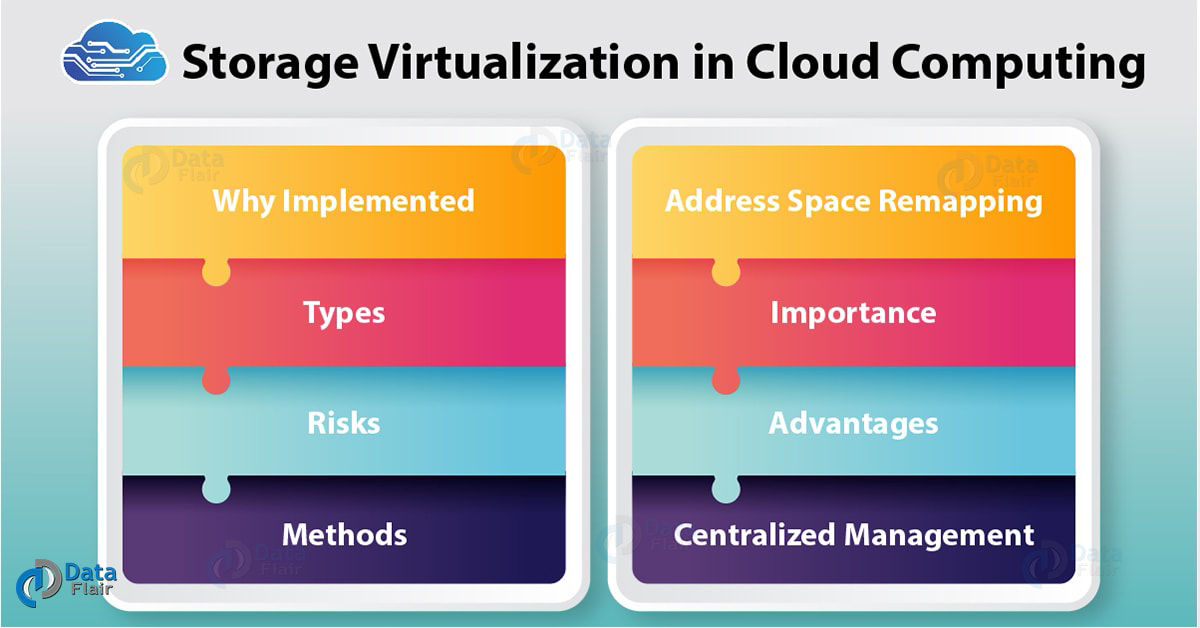
Virtualization is possible through a wide range of Technologies which are available to use and are also OpenSource. We prefer using XEN or KVM since they provide the best virtualization experience and performance.

* [**XEN**](https://www.xenproject.org/)
* [**KVM**](https://www.linux-kvm.org/page/Main_Page)
* [**OpenVZ**](https://openvz.org/Main_Page)

**11. Identify the key features involved in implementation of Storage Virtualization**

**Storage Virtualization in Cloud Computing – Types & Benefits**

After [**Linux Virtualization**](https://data-flair.training/blogs/linux-virtualization/), we are going to learn the Storage Virtualization. Here, we will discuss types, risk, methods, benefits, importance, implementation etc. Storage virtualization in Cloud Computing is nothing but the sharing of physical storage into multiple storage devices which further appears to be a single storage device.



*Storage Virtualization in Cloud Computing*

1. What is Storage Virtualization in Cloud Computing?

Storage [**virtualization in Cloud Computing**](https://data-flair.training/blogs/virtualization-in-cloud-computing/) is nothing but the sharing of physical storage into multiple storage devices which further appears to be a single storage device. It can be also called as a group of an available storage device which simply manages from a central console. This virtualization provides numerous benefits such as easy backup, achieving, and recovery of the data.

This whole process requires very less time and works in an efficient manner. Storage virtualization in [**Cloud Computing**](https://data-flair.training/blogs/learn-cloud-computing-tutorial/) does not show the actual complexity of the Storage Area Network (SAN). This virtualization is applicable to all levels of SAN.

2. Why Storage Virtualization should be implemented?

Following are the reasons shows why we storage virtualization in Cloud Computing implements:

* If this virtualization implements in IT environment it will improve the management of the [**storage**](https://data-flair.training/blogs/cloud-storage-tutorial/). As each and everything will properly store and manage there won’t be any congestion and the task will perform quickly.
* There will be very less downtime as the storage availability is better. All these problems eliminate with the help of an automated management system.
* Storage virtualization will provide better storage utilization as storing most information in a particular place can cause loss of data, congestion, and any other problems. So, properly dividing storage and storing data can be useful.

3. Types of Storage Virtualization

Here, we are going to list down all the storage virtualization in Cloud Computing;

* Hardware Assisted Virtualization
* Kernel Level Virtualization
* Hypervisor Virtualization
* Para-Virtualization
* Full Virtualization

i. Hardware Assisted Virtualization

This type of virtualization requires hardware support. It is similar to full Para-virtualization. Here, the unmodified OS can run as [**hardware**](https://data-flair.training/blogs/hardware-virtualization-in-cloud-computing/) support for virtualization and we can also use to handle hardware access requests and protect operations.

ii. Kernel Level Virtualization

It runs a separate version of the Linux Kernel. Kernel level allows running multiple servers in a single host. It uses a device driver to communicate between main Linux Kernel and the virtual machine. This virtualization is a special form of **Server Virtualization**.

iii. Hypervisor Virtualization

A hypervisor is a layer between the **Operating system** and hardware. With the help of hypervisor multiple operating systems can work. Moreover, it [**provides features**](https://data-flair.training/blogs/features-of-cloud-computing/) and necessary services which help OS to work properly.

iv. Para-Virtualization

It is based on hypervisor which handles emulation and trapping of software. Here, the guest operating system is modified before installing it to any further machine. The modified system communicates directly with the hypervisor and improves the performance.

v. Full Virtualization

This virtualization is similar to Para-Virtualization. In this, the hypervisor traps the machine operations which is used by the [**operating system**](https://data-flair.training/blogs/operating-system-virtualization/) to perform the operations. After trapping the operations, it emulates in particular software and the status codes returned.

[**Do you know What is Software Virtualization in Cloud Computing?**](https://data-flair.training/blogs/software-virtualization/)

4. Storage Virtualization Risks

i. Limited Adoption

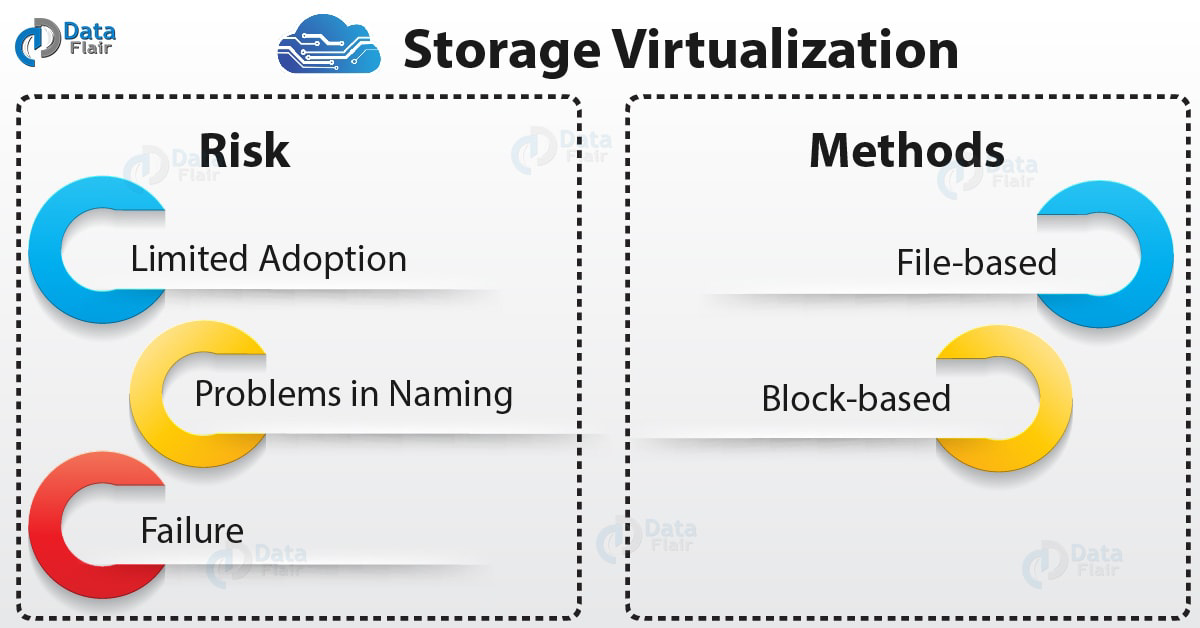
The one-third of the enterprise is reporting in a computer economics survey that they are increasing the funds for storage virtualization. There are some understanding of adoption rates, return of investment and the cost of ownership.

ii. Problems in Naming

**Before very less VMS was used but now there has been a rapid growth of VMS which makes it difficult to distinguish between the important and the important VMS. To make it more future proof building a naming system and sharing with it with all involved parties should be done.**

iii. Failure

The failure occurs due to downtime and data loss. The installation of VMware which hosts crucial services becomes a single point of failure. So to eliminate this threat the protection of virtual machine data should prioritize to the top.



*Storage Virtualization – Risk & Methods*

5. Methods of Storage Virtualization

i. File-based Storage Virtualization

This type of virtualization is used for a specific purpose and can apply to network-attached storage (NAS) system. File-based storage virtualization in Cloud Computing utilizes server message block or network file system protocols and with its help of it breaks the dependency in a normal network attached storage array. This is done between the data being accessed and the location of the physical memory. It also provides a benefit of better handling file migration in the background which improves the performance.

**Recommended reading –** [**Grid Computing Vs Cloud Computing**](https://data-flair.training/blogs/grid-computing-vs-cloud-computing/)

ii. Block-based Virtual Storage

The Block based virtual storage is more widely used than the virtual storage system as the virtual storage system is sometimes used for a specific purpose. The block-based virtual storage system uses logical storage such as drive partition from the physical memory in a storage device. It also abstracts the logical storage such as a hard disk drive or any solid state memory device. This also allows the virtualization management software to get familiar with the capacity of the available device and split them into shared resources to assign.

6. Address Space Remapping

Storage virtualization in Cloud Computing helps to achieve location independence by utilizing the physical location of the data. This system provides the space to the customer to store their data and handles the process of mapping. It is possible that the output of virtualizations can cascade as an input for a higher level of virtualizations. This leads to the fact that it is possible to have multiple layers of virtualizations mapping.

7. Why Storage Virtualization is Important?

i. Performs Tasks

The appliances of storage virtualization are responsible for several tasks such as heterogeneous replication and federation. These devices lineup in front of arrays and create a common interface for the host. This allows the administrator to mix and match the protocols and array which are behind the appliances

ii. WAN Management

It does not send multiple copies of the similar data over WAN. The WAN accelerator use to cache the data and send it LAN speed without changing the performance of WAN.

iii. Disaster Recovery

Storage virtualization in Cloud Computing can increase disk utilization and is flexible. This ameliorates disaster recovery and the continuity of the business.

[**Follow this link to know about Risk and Security Issues in Cloud**](https://data-flair.training/blogs/cloud-security/)

iv. Storage Tiering

Storage tiering is a technique which monitors and selects the most commonly used data and put it on its highest performing storage pool. The least used data is put in the weakest performance storage pool.



*Storage Virtualization – Advantages and Importance*

8. Advantages of Storage Virtualization

Let’s discuss some benefits of Storage Virtualization in Cloud Computing:

**i. Easy Retrieval and Upload of Data**

In storage virtualization, the data quickly retrieve from virtual storage. It is as easy as accessing a file on the local computer. The data store very easily with the help of some application and an internet connection which is an easy task.

**ii. Better Management**

The data can be migrated based upon the utilization such as the data which is frequently used can be stored on a high-performance storage system. However, the data which is rarely used can be placed on a bit slower system. This is an example of a battery management system and the customer won’t face any issue regarding storage.

**iii. Security**

In storage virtualization, the data stores in different place and secure with maximum security. If any disaster takes place the data can be retrieved from some other place and it won’t affect the customer. The security has the ability to meet the real utilization necessities rather than providing additional storage.

9. How Storage Virtualization Apply?

Following are the different ways for storage applies to the virtualization:

* Host-Based
* Network-Based
* Array-Based

i. Host-Based Storage Virtualization

Here, all the virtualizations and management is done at the host level with the help of software and physical storage, it can be any device or array. The host is made up of multiple hosts which present virtual drives of a set to the guest machines. Doesn’t matter whether they are VMs in an enterprise or PCs.

[**Let’s explore the Pros and Cons of Cloud Computing**](https://data-flair.training/blogs/advantages-and-disadvantages-of-cloud-computing/)

ii.  Network-Based Storage Virtualization

Network-based storage virtualization is the most common form which are using nowadays. Devices such as a smart switch or purpose-built server connect to all the storage device in a fibre channel storage network and present the storage as a virtual pool.

iii. Array-Based Storage Virtualization

Here the storage array provides different types of storage which are physical and used as storage tiers. The software is available which handles the amount of storage tier made up of solid-state drives hard drives.



10. Centralized Management

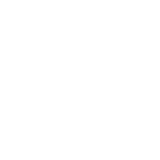
Centralized [**management**](https://data-flair.training/blogs/cloud-management/) system provides various benefits such as it allows managing, allocating, and viewing storage from a single interface. Moreover, the downtime is minimized as centralized management system provides maximum availability.

**12. Examine how Data Virtualization is vital for any enterprise in establishing a data center environment**

**What is Data Virtualization?**

Data virtualization software acts as a bridge across multiple, diverse data sources, bringing critical decision-making data together in one virtual place to fuel analytics.

Data virtualization provides a modern data layer that enables users to access, combine, transform, and deliver datasets with breakthrough speed and cost-effectiveness. Data virtualization technology gives users fast access to data housed throughout the enterprise—including in traditional databases, big data sources, and cloud and IoT systems—at a fraction of physical warehousing and extract/transform/load (ETL) time and cost.



With data virtualization, users can apply a range of analytics—including visualized, predictive, and streaming analytics—on fresh, up-to-the-minute data updates. Through integrated governance and security, data virtualization users are assured their data is consistent, high quality, and protected. Additionally, data virtualization allows for more business-friendly data, transforming native IT structures and syntax into easy-to-understand, IT-curated data services that are easy to find and use via a self-service business directory.

Data virtualization supports multiple lines of business, hundreds of projects, and thousands of users that can increase from project to enterprise scale.

**What does data virtualization do for users?**

With data virtualization, users get data that is not just up-to-date, but up-to-the-minute, easy to find, easy to use, and easy to understand. Data is available wherever and whenever you need it. Data virtualization can provide users with any dataset they might need, even from new, unique assets. This gives users data they can trust and more time for analyzing as opposed to chasing it.

Data virtualization gives users a full range of capabilities for applying multiple analytics tools. Data is available in all structures and formats, allowing for many types of analytics users and skill levels. As a result, users can respond urgently to every request, retain better data security, put their data in the cloud, and meet governance and compliance requirements.

Common data sources virtualized through data virtualization software

* Packaged apps
* RDBMS
* Excel & flat files
* Data warehouses
* Data lakes
* Big data
* XML docs
* Cloud data
* Web services
* IoT data

Common systems used with data virtualization

* Oracle
* SQL Server
* Teradata
* Netezza
* DB2
* Hive
* Impala
* Sharepoint
* Excel
* Flat files
* Amazon Redshift
* Google Big Query
* Spark
* Drill
* REST
* OData

**Top 4 capabilities that a data virtualization system should have**

**Four components are needed to meet urgent business needs with data virtualization**

**Agile design and development:** You need to be able to introspect available data, discover hidden relationships, model individual views/services, validate views/services, and modify as required. These capabilities automate difficult work, improve time to solution, and increase object reuse.

**High-performance runtime:** The application invokes a request, the optimized query executes a single statement, and the result is delivered in proper form. This capability allows for up-to-the-minute data, optimized performance, and less replication.

**Use of caching when appropriate:** Caching essential data, the application invokes a request, an optimized query (leveraging cached data) executes, and data is delivered in the proper form. This capability boosts performance, avoids network constraints, and allows 24x7 availability.

**Business directory/catalog to make data easy to find:** This capability includes features for search and data categorization, browsing all available data, selecting from a directory of views, and collaborating with IT to improve data quality and usefulness. This capability empowers business users with more data, improves IT/business user effectiveness, and enables data virtualization to be more widely adopted.

**What are some data virtualization use cases?**

* Analytics use cases
  + Physical data integration prototyping
  + Data access/semantic layer for analytics
  + Logical data warehouse
  + Data preparation
  + Regulatory constraints on moving data
* Operational use cases
  + Abstract data access layer/virtual operational data store (ODS)
  + Registry-style master data management
  + Legacy system migration
  + Application data access
  + Regulatory constraints on moving data
* Emerging use cases
  + Cloud data sharing
  + Edge data access in IoT integration
  + Data hub enablement
  + Data and content integration
  + Regulatory constraints on moving data

**The Benefits of Data Virtualization**

Business value acceleration: Analytics applications can be applied sooner and greater value can be attained faster as changes occur

Business insight improvement: More complete, up-to-the-minute, easy to access and understand data, requiring less effort than ETL

Development cost avoidance: Reusable data services and interactive development and validation improves quality and avoids rework for new projects

Data management infrastructure cost reduction: Lower infrastructure costs, and fewer licenses to buy and depreciate, result in lower support and maintenance costs

**How do various industry sectors use data virtualization?**

* Communications & Technology
  + Differentiating market research services
  + Increasing revenue per customer
  + Building a virtual customer data lake
  + Enabling leading-edge innovation
  + Creating a real-time ODS for billing and marketing
  + Optimizing customer care
  + Managing customer entitlements
  + Improving customer insights
* Energy
  + Optimizing upstream energy production
  + Improving well maintenance and repair
  + Analyzing offshore platform data
  + Optimizing cross-refinery processes
  + Providing SAP master data quality
* Financial Services
  + Managing fixed-risk income
  + Improving trade reconciliation
  + Accelerating new client onboarding
  + Addressing mortgage data complexity
  + Enriching cash management clients
  + Empowering data democracy
* Government
  + Protecting the environment
* Healthcare
  + Driving new product innovation
  + Accelerating M&A synergies
  + Providing more efficient claims analysis
  + Improving patient care
* Manufacturing
  + Optimizing a global supply chain
  + Optimizing factories and logistics
  + Differentiating via digitization
  + Improving IT asset utilization

Getting Started with Data Virtualization

The highest value implementation of data virtualization is a high-speed, virtualized data layer. Such a layer allows for robust management and governance, while also delivering self-service access to critical data, organizing it for scale, and making it available in a cost-effective manner to applications and analytics systems.

However, most data virtualization implementations start small and expand. A common way of starting is with a small and focused team charged with one or more projects. A small team can be versatile while also accepting some uncertainty. (Teams must be agile to move fast and complete several iterations of data projects.)

The next step is to deliver project datasets as the data layer is being built. This step addresses several data challenges including evolving requirements, multiple sources, mixed data types, up-to-the-minute data, data outside of the data warehouse, data too large to physically integrate, and data outside the firewall.

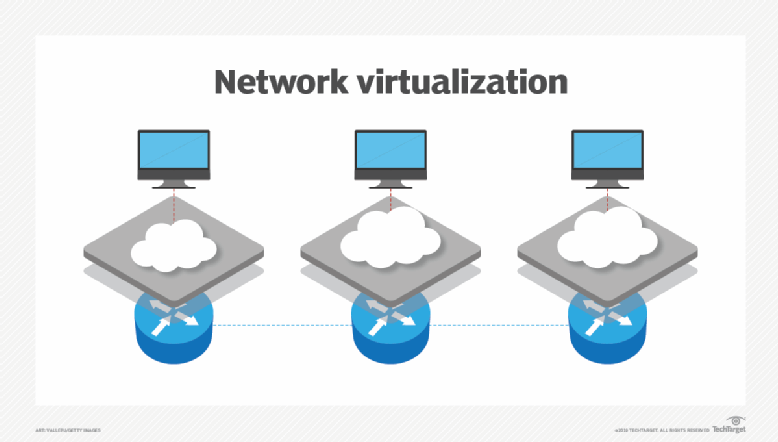
Teams also need to prioritize their data virtualization projects based on business value and ease of data virtualization implementation. The greater the business value and implementation ease, the higher the project’s priority. Data virtualization, and the people who implement it, also need to evolve to reuse various data services in the application layer, business layer, and source layer.

**13.Categorize Network Virtualization with its key features in cloud security**

Network virtualization is a method of combining the available resources in a network to consolidate multiple physical networks, divide a network into segments or create software networks between virtual machines (VMs). IT managers that use network virtualization can administrate their environment as a single software-based network. Network virtualization is intended to optimize network speed, reliability, flexibility, scalability and security. It is said to be especially useful in networks that experience sudden, large and unforeseen surges in usage.

Network virtualization works by combining the available resources in a network and splitting up the available [bandwidth](https://searchnetworking.techtarget.com/definition/bandwidth) into [channels](https://searchdatacenter.techtarget.com/definition/channel), each of which is independent from the others and each of which can be assigned (or reassigned) to a particular server or device in real time. Each channel is independently secured. Every subscriber has shared access to all the resources on the network from a single computer.

Network virtualization is intended to improve productivity, efficiency and job satisfaction of the administrator by performing many of these tasks automatically, thereby disguising the true complexity of the network. Files, images, programs and folders can be centrally managed from a single physical site. Storage media such as hard drives and tape drives can be easily added or reassigned. Storage space can be shared or reallocated among the servers.



Types of network virtualization

Virtual networks exist in two forms; internal and external. Both of these terms refer to inside or outside the server. Eternal virtualization will use tools such as switches, adapters or a network to combine one or more networks into virtual units. Internal virtualization refers to using network-like functionality in software [containers](https://searchitoperations.techtarget.com/definition/container-containerization-or-container-based-virtualization) on a single network server. Internal software allows VMs to exchange data on a host without using an external network.

Advantages and disadvantages

The use of network virtualization does have its upsides and downsides, including:

Advantages:

* More productive IT environments (i.e., efficient scaling).
* Improved security and recovery times.
* Faster in application delivery.
* More efficient networks.
* Reduced overall costs.

Disadvantages:

* Increased upfront costs (investing in virtualization software).
* Need to license software.
* There may be a learning curve if IT managers are not experienced.
* Not every application and server will work in a virtualized environment.
* Availability can be an issue if an organization can’t connect to their virtualized data.

SDN vs. network virtualization

Network virtualization shares common elements with software-defined networking ([SDN](https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN)) which can create confusion for some. For example, both share the goal of improving the agility of network resources to VMs and consolidating or segmenting networks.

**14.Illustrate various Virtualization Security Recommendations with examples**

Virtualization is the process of running multiple virtual instances of a device on a single physical hardware resource. Security virtualization is the process, procedure and policy that ensures that the virtualized hardware infrastructure is secure and protected.

**Problems Security Virtualization Addresses**

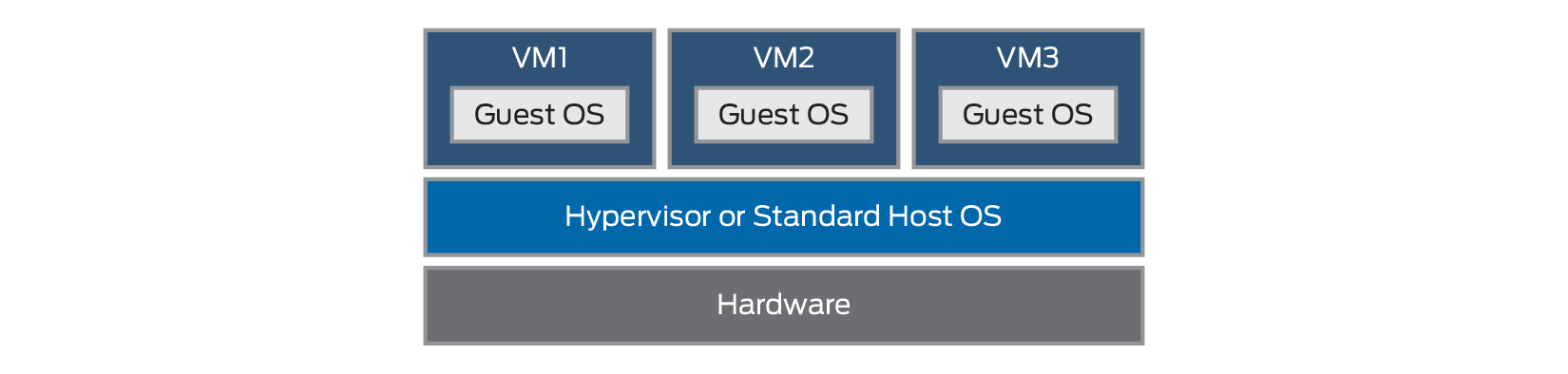
Virtualization centralizes administrative tasks while improving scalability and workloads, and leads to the consolidation of network infrastructure, lower OPEX, and ease of management. However, virtualization also introduces security challenges that physical security systems cannot adequately protect against:

* File sharing between hosts and guests is not secure.
* Isolation between components such as guest OSs and applications, hypervisors, hardware are weakened.
* Multiple servers are consolidated which increases the risk that a compromise may spread from applications on the same host.
* For intrusion prevention systems (IPS), malware targeted for physical and virtual machines causes infection via the virtual network. Other security threats include unauthorized access, denial of service, and exploits.

Many organizations do not realize that using their existing legacy security solutions can expose them to these types of attacks and data loss.

**What Can You Do with Security Virtualization?**

Security virtualization acts as a barrier to secure perimeter access to a network. It provides dedicated security services and assured traffic isolation within the cloud, along with customizable firewall controls as an additional managed service. Enterprises and service providers can leverage their virtualization investment to create a granular security perimeter, giving dedicated security resources within a cloud construct to tenants and service subscribers.



**How Does Security Virtualization Work?**

A virtualization system consists of a host operating system, a hypervisor, and a guest operating system.

The host is the underlying hardware of the virtualization system that provides computing resources (physical interface cards, CPUs, memory, management ports, operating system, third-party software, hypervisor). All this enables the host to contain one or more Virtual Machines (or partitions) and share physical resources with them.

The host is the underlying hardware of the virtualization system that provides computing resources (physical interface cards, CPUs, memory, management ports, operating system, third-party software, hypervisor). All this enables the host to contain one or more Virtual Machines (or partitions) and share physical resources with them.

**PREPARED BY**

**SRINIVASAN.L,Sr.AP,ISE?NHCE**