

n. 1

- A. Spiegare l'importanza di definire un servizio Network Time Protocol - Fare degli esempi
- B. Descrivere che cosa si intende per autenticazione a multi-fattore – Ambiti di applicazione
- C. The Active Directory structure is comprised of three main components: domains, trees, and forests. Several objects, like users or devices that use the same AD database, can be grouped into a single domain. Domains have a domain name system (DNS) structure. Multiple domains can be combined to form a group known as a tree. The tree structure uses a contiguous namespace to arrange domains in a logical hierarchy. Different domains in a tree share a secure connection and trust each other in a hierarchy. This means the first domain can implicitly trust the third domain in a hierarchy. A collection of multiple trees is called a forest. Admins can allocate specific access rights and communication privileges at all levels. Moreover, a forest also includes directory schemas, shared catalogs, domain configurations, and application information. The global catalog servers provide a list of all the objects in a forest, and the schema defines the class and attributes of an object in a forest. Organizational units (OUs) organize groups, users, and devices. Every domain can contain its own OU.

Handwritten signatures and initials in blue ink, including a star-like symbol, a circle with a letter, and the word 'Aut.' followed by a large signature.

n. 2

- A. In quale contesto viene usato il Simple Network Management Protocol? - Fare un esempio pratico
- B. Quali sono le tecniche di difesa da attacchi informatici?
- C. Active Directory uses a security mechanism known as Kerberos. Once the user enters his or her login details, Kerberos grants a Ticket Granting Ticket (TGT) to the user through a ticket-granting system. The user then presents this ticket to other workstations and servers throughout the same domain (or even on other domains where a trust relationship exists). The servers identify the ticket and understand it's been issued by a trusted domain controller. After authorization, the users get the permissions necessary to complete their intended tasks.

X PD cui [signature]

Genovese

n. 3



A. Quali sono i permessi che possono essere settati ad una risorsa condivisa?

B. Descrivere come organizzare un'infrastruttura di backup efficiente

C. Every domain controller stores the objects for the domain in which it is installed. However, a domain controller designated as a global catalog server stores the objects from all domains in the forest. For each object that is not in the domain for which the global catalog server is authoritative as a domain controller, a limited set of attributes is stored in a partial replica of the domain. Therefore, a global catalog server stores its own full, writable domain replica (all objects and all attributes) plus a partial, read-only replica of every other domain in the forest. The global catalog is built and updated automatically by the AD DS replication system. The object attributes that are replicated to global catalog servers are the attributes that are most likely to be used to search for the object in AD DS. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are defined by default by Microsoft. However, to optimize searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.



n. 4

A. Quali sistemi di *collaboration* conosci e quali sono le principali caratteristiche e peculiarità?

B. Che cos'è il *Lightweight Directory Access Protocol*? Come viene utilizzato ed a quale scopo?

C. Given that increasingly more organizations are shifting their business operations to the cloud, Microsoft has introduced Azure Active Directory (Azure AD), which is their cloud-based version of Windows AD, which can also sync with on-premise AD implementations. Azure AD is said to be the backbone of Office 365 and other Azure products; however, it can also be integrated with other cloud services and platforms. Some of the differences between Windows and Azure AD are as follows.

Communication: Azure AD uses a REST API, whereas Windows AD uses LDAP, as mentioned previously.

Authentication: Windows AD uses Kerberos and NTLM for authentication, whereas Azure AD uses its own built-in web-based authentication protocols.

Structure: Unlike Windows AD, which is organized by OUs, trees, forests, and domains, Azure AD uses a flat structure of users and groups.

Device Management: Unlike Windows AD, Azure AD can be managed via mobile devices. Azure AD does not rely on Group Policy Objects (GPOs) to determine which devices and servers are able to connect to the network.

f R au

Santhi Mani

n. 5

A. Quali vantaggi presenta una infrastruttura in *cloud* rispetto ad una on-premise?

~~Scalability Access Pay as you go~~

B. Quale ruolo svolge un servizio *Proxy*?



C. Swap is disk space used for virtual memory. This is similar to the "page" file that Windows uses for virtual memory. The Installer will create a swap partition for you. If you intend to hibernate (and not just suspend) the system, here are some recommendations for the size of the swap space:

- For less than 1 GB of RAM, the swap space should at least be equal to the amount of RAM and at maximum twice the amount of RAM depending upon the amount of hard disk space available for the system.
- For systems with larger amounts of RAM, your swap space should at least be equal to the memory size.
- Technically a Linux system can operate without swap, although some performance problems may occur even on systems with large amounts of RAM.

* NO lui [Signature]

[Signature]

n. 6

Donik Foxveme

A. A cosa si riferiscono i file di log in ambito database?

B. Sistemi di storage – DAS, NAS, SAN Caratteristiche e differenze.

C. For admin access Fedora postgresql is configured to obtain the host's operating system user name from the kernel and using it as the allowed database user name. Therefore, as soon as someone can authenticate on the host as user *postgres*, that person has administrative privileges on the postgresql server without any additional password prompt. The only one who can do that by default, is root. Root can configure additional users to be able to su to postgres. In any case, in a whatever emergency, if any then the system administrator is able to quickly access postgresql server unhindered and salvage what can still get salvaged.

If local regulations make it necessary to replace these procedures with a dedicated authentication by postgresql itself, one of the other procedures can be configured later. In general, however, it is not advisable to make any changes. Once root is compromised, there are a lot of completely different problems to get tackled.



n. 7

A. Quali sono le componenti fondamentali di un *datacenter*?

B. In quale ambito possiamo utilizzare il linguaggio SQL?

C. UEFI Secure Boot is a platform feature within the UEFI specification that ensures that the system boots by using only the software that's trusted by the hardware manufacturer. Secure Boot provides a verification mechanism where the firmware validates a boot loader before running the loader. This mechanism checks that the code that's run by a system's firmware is trusted. When the system starts, the firmware checks the signature for each piece of boot software, including the firmware drivers and the OS itself. If the signatures are valid, the system boots, and the firmware relinquishes control to the OS.

Secure Boot uses cryptographic checksums and signatures to prevent malicious code from being loaded and run early in the boot process before the OS has loaded. Every program that's loaded by the firmware includes a signature and a checksum and undergoes the same validation by the firmware. Secure Boot stops all untrusted programs from running to prevent any unexpected or unauthorized code from operating in the UEFI-based environment.



n. 8

A. Spiegare il funzionamento di un DNS e il suo ruolo in una rete aziendale.

B. Quali sono i vantaggi forniti da un sistema antivirus centralizzato?

C. The term *load balancing* refers to the efficient distribution of incoming network traffic across a group of back-end servers. The use of load balancing ensures that your infrastructure is highly available, reliable, and that performance is not degraded. Load balancers can typically handle traffic for the HTTP, HTTPS, TCP, and UDP protocols.

Load balancers manage network traffic by routing client requests across all of the servers that can fulfill those requests. This routing maximizes speed and capacity use so that no one particular server becomes overloaded, thereby improving overall performance. In situations where a server might become unavailable or goes down, the load balancer redirects any incoming traffic to other servers that are online. In this way, server downtime is minimized. When a new server is added to the server group, the load balancer automatically redistributes the workload and starts to send requests to that new server.

In Oracle Linux, load balancing of network traffic is primarily handled by two integrated software components: HAProxy and Keepalived. The HAProxy feature provides load balancing and high-availability services to TCP and HTTP, while Keepalived performs load balancing and failover tasks on both active and passive routers. The NGINX feature can also be used in Oracle Linux for load balancing.



A. Descrivere il funzionamento di un servizio di gestione PEC


B. Perché usare le macchine virtuali?

C. Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are the most widely used security protocol today and are primarily used to serve two specific functions:

1. Authentication and verification: The TLS/SSL certificate has information about the authenticity of certain details regarding the identity of a person, business or website, which it will display to visitors on your website when they click on the browser's padlock symbol or trust mark. All that information was validated by the Certificate Authority (CA) which issued the SSL certificate.
2. Data encryption: The TLS/SSL certificate also enables encryption, which means that the sensitive information exchanged via the website cannot be intercepted and read by anyone other than the intended recipient.

In the same way that an identity document or passport may only be issued by the country's government officials, an TLS/SSL certificate is most reliable when issued by a trusted Certificate Authority (CA). The CA has to follow very strict rules and policies about who may or may not receive an TLS/SSL certificate. When you have a valid TLS/SSL certificate from a trusted CA, there is a higher degree of trust by your customers, clients or partners.

f. 10 cuc



n. 10

A. In quale ambito possiamo utilizzare il linguaggio Powershell?

B. Differenze tra Backup full e incrementale.

C. The different types of firewalls will have a shared goal: protect the network and infrastructure from malicious external traffic. However, each type will vary in the process of achieving this aim.

These firewalls can be in the form of software or hardware, and increasingly are cloud-based. There are three common types of firewalls in use by organizations, each with a different way of functioning. Each firewall type has its benefits and drawbacks when protecting a private network. Individual types also vary in terms of complexity and security. The three main types of firewall are:

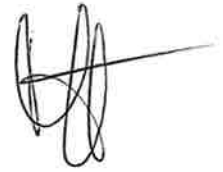
A proxy firewall acts as a sort of 'go-between', preventing a direct connection between a device and network. A device will first connect to the proxy, and then the proxy will make the relevant connection to the network destination. Because it prevents a direct connection, it is one of the most secure types of firewall.

Stateful and stateless inspection firewalls are both often described as 'traditional firewalls'. These firewalls control and filter the flow of network traffic based on pre-set conditions such as source, destination, or port address. These firewalls will allow only trusted traffic to enter and leave a network.

Next generation firewalls (NGFW) are more advanced versions of traditional firewalls. Many next generation firewalls have the added ability to filter traffic based on applications. This helps organizations protect against more advanced threats. They can also act as an anti-virus, blocking specific malware from accessing networks. These systems combine traditional firewalls with an intrusion detection system, which actively monitors the network for malicious activity.



n. **11**



- A. Spiegare il funzionamento di un DHCP, descrivere le sue fasi di configurazione.
- B. Che cosa sono le Access Control List - Fare degli esempi di applicazione
- C. When you use NAT, you assign private IP addresses to hosts on the private side of the router. When those hosts send traffic, the router translates the private addresses to one or more public and valid addresses before routing the traffic. When the router receives traffic that is destined for those hosts, it translates the public addresses back to the appropriate private addresses. NAT, defined in RFC 1631, provides a solution to one of the major problems facing the Internet—IP address depletion. IP address space is limited and obtaining a large block of registered addresses is difficult. Although you can use private IP address (RFC 1918) in your internal network, private IP addresses are not routable through the Internet.



n. 12

A. Cosa s'intende per Disaster Recovery in ambito aziendale?

B. Misure minime di sicurezza informatica: gestione degli accessi e delle password.

C. The router supports:

Port Forwarding: To provide public access to internal servers, the firewall is used in conjunction with NAT and the firewall must be able to forward traffic received on an interface to those servers. Port Forwarding redirects any traffic from the specified entity to a specific host address regardless of the original destination of the traffic.

NAT with IP Masquerade: It is a case where all or a range of addresses are mapped to a single address with source port translation to identify the association. This single address masquerades as the public source address for the private addresses.

[Handwritten signatures]

n. 13

A. Cosa vuol dire Virtualizzare un PC o un Server?

B. Caratteristiche principali di un database management system

C. Below is a list of firewall features:

- **Bandwidth control and monitoring:** Every firewall should have this feature, which is sometimes called traffic shaping. It allows you to control the available bandwidth of your network for sites, applications, and users.
- **Web filtering:** Also known as content filtering, it oversees data packets your computer sends and receives to weed out any compromising, flagged, or forbidden content.
- **Logging:** An effective firewall can log network traffic, giving you updated information about what's happening. It can show you vulnerabilities and provide information about an attack happening on the web.
- **Sandboxing:** Sandboxing takes files or executables and opens them in a test environment. This feature essentially opens and runs files to scan for any malware or suspicious activity to protect the end user.
- **Threat prevention:** A firewall with a threat prevention feature identifies and blocks attacks before they cross into a network, helping companies avoid cyberattacks and their negative implications.
- **Application and identity-based inspection:** Companies are constantly changing their applications, so they can use a firewall with an application and identity-based inspection feature. This lets a company apply specific policies to applications or users within the organization to better control their networks.
- **Scalability:** Using a scalable firewall solution is important as more companies incorporate digital technologies into their business. They grow as organizations evolve and their cybersecurity needs become more complex.



n. 14

A. Quali sono le caratteristiche dei sistemi EDR (Endpoint Detection and Response)?

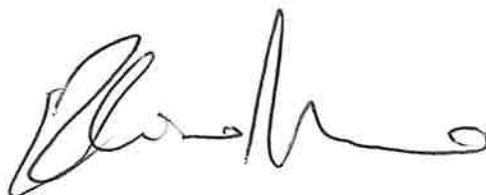
B. Business Continuity (BC) e Disaster Recovery (DR)

C. The most common solutions are IPsec (Internet Protocol Security) VPN, SSL (Secure Sockets Layer) VPN, or a hybrid combination of both.

IPsec is a set of methods for securing Internet-based communications by authenticating and encrypting information as it passes back and forth between two end points.

IPsec is an open standard, meaning that its specification has been published and is available for anyone to use. IPsec VPN functions at a lower network level than SSL VPN and, because of this, is considered more secure.

SSL VPN is based on a different tunneling technology than IPsec and also includes a secure connection that's authenticated and encrypted. It was developed due to increasing popularity of web-based applications and the need for easy and "clientless" secure remote access to them.



n. 15

A. Descrivere alcuni esempi di Misure Minime di Sicurezza definite dall'AgID.

B. Cos'è una VPN e a cosa serve?

C. ESXi Hosts

Industry standard x86 servers that run ESXi on the bare metal. ESXi software provides resources for and runs the virtual machines. You can group a number of similarly configured x86 servers with connections to the same network and storage subsystems. This grouping creates an aggregate set of resources in the virtual environment, called a cluster.

Storage networks and arrays

VMware vSphere uses Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays to meet different data center storage needs. With storage area networks, you can connect and share storage arrays between groups of servers. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

IP networks

Each compute server can have multiple physical network adapters to provide high bandwidth and reliable networking to the entire VMware vSphere data center.

vCenter Server

vCenter Server provides a single point of control to the data center. It provides essential data center services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire data center. It manages the assignment of virtual machines to the ESXi hosts and the assignment of resources to the virtual machines within a given computing server. These assignments are based on the policies that the system administrator sets.



n. 16

- A. Che cos'è un'infrastruttura VDI (Virtual Desktop Infrastructure)?
- B. Il domain controller quale risorsa per proteggere i dati dell'azienda
- C.

Full Backup

A full backup is the most complete type of backup where you clone all the selected data. This includes files, folders, SaaS applications, hard drives and more. The highlight of a full backup is the minimal time it requires to restore data. However, since as everything is backed up in one go, it takes longer to backup compared to other types of backup.

The other common issue with running full backups is that it overloads storage space..

Differential Backup

A differential backup straddles the line between a full and an incremental backup. This type of backup involves backing up data that was created or changed since the last full backup. To put it simply, a full backup is done initially, and then subsequent backups are run to include all the changes made to the files and folders.

It lets you restore data faster than full backup since it requires only two backup components: an initial full backup and the latest differential backup.

Incremental Backup

The first backup in an incremental backup is a full backup. The succeeding backups will only store changes that were made to the previous backup. Businesses have more flexibility in spinning these types of backups as often as they want, with only the most recent changes stored.



n. 17

A. Caratteristiche e differenze tra Application Server e DB Server.

B. Cosa si intende per aggregazione di schede di rete?



C. Denial-of-Service Attack (DoS)

DoS attacks are used to prevent users of an online service from accessing that service's data, apps and other elements. Unlike attacks intended to allow the attacker to gain access, DoS breaches offer little benefit. Many attackers are motivated by the thrill of exploiting a system.

Social Engineering Attacks

Social engineering is the art of exploiting human psychology. Today's cyber attackers are combining social engineering and technology to aid in data breaching. According to the InfoSec Institute, phishing is the most commonly used social engineering attack. These attacks leverage social engineering to trick victims into giving up sensitive information such as passwords or credit card information.

Ransomware

Ransomware poses a significant and growing threat to companies, representing one of the most impactful trends in cyberattacks today, according to Microsoft's Threat Protection Intelligence Team. These threats involve hackers holding data hostage in exchange for money or other demands.

A. Caratteristiche e vantaggi di un file server

B. Come funziona la virtualizzazione?

C. Network Access Control is a tool that defines and implements rules that specify which users and devices can access the network using a set of protocols and policies. In most situations, a NAC system is built to prohibit non-compliant and unauthorized device access to the network. Based on a number of factors, such as system health or role-based variables, NAC enables you to deny or allow network access. NAC helps to identify network access policies based on tasks within the company and enforce them. As an outcome, NAC should be configured so that employees only have access to the data required to complete their job functions.

NAC is a two-stage process: authentication and authorization. If either stage fails, then it blocks and quarantines the device or user. DURING AUTHENTICATION, the NAC system

NAC then approves access based on local access policies after authentication. If the access policies authorize the user or computer, access is granted. If not, Access is refused.

R R Au [Signature]

[Signature]