ASIX Administració de sistemes informàtics
Projectes 2020-2021

Cloud / Alta Disponibilitat

Kubernetes

Kubernetes (K8s) is an open-source system for automating deployment, scaling, and management of containerized applications.

It groups containers that make up an application into logical units for easy management and discovery. Kubernetes builds upon 15 years of experience of running production workloads at Google, combined with best-of-breed ideas and practices from the community.

Designed on the same principles that allows Google to run billions of containers a week, Kubernetes can scale without increasing your ops team.

Kubernetes is open source giving you the freedom to take advantage of on-premises, hybrid, or public cloud infrastructure, letting you effortlessly move workloads to where it matters to you.

https://kubernetes.io/

Kubernetes Documentation:

- ❏ Understand the basics
- ❏ Try kubernetes
- ❏ Setup a cluster
- ❏ Learn how to use kubernetes

Tasques a realitzar:

- Investigar i exposar clarament el funcionament de Kubernetes.
- Implementar exemples bàsics de funcionament per entendre el ecosistema de kubernetes.
- Implementar una estructura d'autenticació d'usuaris similar a la que realitza el servidor Gandhi: ldap, kerberos samba i nfs.

AWS Recursos

Explicar els recursos que proporciona AWS amb exemples. Per realitzar aquest projecte cal estar disposat a realitzar alguna despesa econòmica.

Descriure el funcionament amb explicacions i exemples d'implementació dels recursos / serveis que proporciona AWS. Entre d'altres explicar el funcionament de:

- ❏ EC2
- ❏ RDS
- ❏ S3
- ❏ Serverless
- ❏ IAM templates
- ❏ AMI Roles
- ❏ MFA
- ❏ AWS CLI
- ❏ ECS

EC2 Elastic Cloud Computing

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

RDS Relational Database Service

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.

S3 Simple Storage Service

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and

configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

IAM Identity and Access management

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

ECS Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service. Customers such as Duolingo, Samsung, GE, and Cook Pad use ECS to run their most sensitive and mission critical applications because of its security, reliability, and scalability.

ECS is a great choice to run containers for several reasons. First, you can choose to run your ECS clusters using AWS Fargate, which is serverless compute for containers. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design. Second, ECS is used extensively within Amazon to power services such as Amazon SageMaker, AWS Batch, Amazon Lex, and Amazon.com's recommendation engine, ensuring ECS is tested extensively for security, reliability, and availability.

Integració Continua / DevOps

“DevOps és una nova tendència en el món de la informàtica. És una metodologia que destaca la col·laboració entre desenvolupadors i operacions per reduir el temps de desenvolupament, les proves i el desplegament i sobretot millorar la qualitat del que construïm.”

La Integració continua, es basa en dissenyar, desplegar i configurar un entorn de desenvolupament i gestió de software en un entorn col·laboratiu. Aquest entorn abasta diferents fases del cicle de vida del software:

1. Desenvolupament codi
2. Automatització de proves
3. Automatització de desplegaments.

El/s projecte/s podrien constar en crear un entorn de desenvolupament desplegat en contenidors Docker proporcionant eines adequades (a escollir) per dur a terme la integració continua. Sempre, complementat amb **GitLab** com a nexe comú per al treball grupal, allotjant i compartint el codi, creant versions estables del producte, així com per la construcció de la Release abans de pujar la versió definitiva a producció..

Entre les eines que es poden incloure en el Docker, i serien les que haurien de treballar en el projecte, destacaria:

1. Jenkins: Eina d'automatització open-source, que s'utilitza per crear un pipeline d'automatització per a la majoria de tasques al voltant de la creació, prova i desplegament de creació de programari.
2. ELK Stack (Elasticsearch, Logstash, and Kibana), és la solució d’anàlisi de registre de codi obert més popular. Ajuda a recopilar logs de diferents aplicacions, servidors de serveis, dispositius de xarxa per emmagatzemar-los en una ubicació centralitzada.
3. Nagios: Manté la supervisió d’aplicacions i servidors, i en cas d’error, Nagios enviarà alertes a l’equip automàticament. A continuació, els equips poden prendre mesures ràpidament de manera que es redueixin els temps morts.
4. Docker: Plataforma de contenidors per virtualitzar sistemes operatius i facilitar l’allotjament d’aplicacions i serveis, de manera que diferents contenidors reutilitzen les biblioteques i les utilitats del sistema operatiu. Així, bàsicament, els contenidors comparteixen el nucli del sistema operatiu amb altres contenidors, de manera que cada contenidor s'executa com un procés aïllat al seu espai d'usuari.
5. Gradle, ant, maven: Totes aquestes eines automatitzem la construcció de builds en diversos llenguatges(C, C ++, Python, Java, Groovy, etc.) i plataformes. Es complementen amb Jenkins.
6. Selenium IDE: Eina d’open source per automatització de proves que intenten simular interaccions de les persones en llocs web, d’aquesta manera s’elimina la necessitat de fer un pas manual repetitiu.
7. Postman és una eina que ajuda als desenvolupadors en totes les etapes del cicle de vida de les API.
8. SonarQube, permet als desenvolupadors fer un seguiment de la qualitat del codi, cosa que els ajuda a determinar si un projecte està preparat per a ser implementat en producció.

Webgrafia:
https://www.upgrad.com/blog/devops-projects-for-beginners/

Pacemaker

Implementar un cluster d'alta disponibilitat amb Pacemaker. Implementar almenys les següents característiques:

- Servidor httpd
- Servidor NFS
- Servidor Samba
- Adreça IP flotant.
- DRDB / GFS2
- Active/Active
- Fences / stonith

Pacemaker 2.0
Clusters from Scratch (en-US) [epub] [pdf] [html] [html-single]
Pacemaker Administration (en-US) [epub] [pdf] [html] [html-single]
Pacemaker Development (en-US) [epub] [pdf] [html] [html-single]
Pacemaker Explained (en-US) [epub] [pdf] [html] [html-single]
Pacemaker Remote (en-US) [epub] [pdf] [html] [html-single]
https://clusterlabs.org/pacemaker/doc/

RedHAt Enterprise Linux 7
Clustering

Deployment and administration of clusters

- **High Availability Add-On Overview**
  Overview of the High Availability Add-On for Red Hat Enterprise Linux 7
- **High Availability Add-On Administration**
  Configuring and Managing the High Availability Add-On
- **Load Balancer Administration**
  Load Balancer for Red Hat Enterprise Linux
- **High Availability Add-On Reference**
  Reference Document for the High Availability Add-On for Red Hat Enterprise Linux 7
- Global File System 2

Product Documentation RH7

LPIC3 High Availability Cluster Management
Tecnologies:

Implementar els continguts descrits a LPIC3 304-200 334: High Availability Cluster Management:

- ❏ 334.1 High Availability Concepts and Theory
- ❏ 334.2 Load Balanced Clusters
- ❏ 334.3 Failover Clusters
- ❏ 334.4 High Availability in Enterprise Linux Distributions

Topic 334: High Availability Cluster Management

334.1 High Availability Concepts and Theory
Weight: 5

Description: Candidates should understand the properties and design approaches of high availability clusters.

Key Knowledge Areas:
- Understand the most important cluster architectures
- Understand recovery and cluster reorganization mechanisms
- Design an appropriate cluster architecture for a given purpose
- Application aspects of high availability
- Operational considerations of high availability

Terms and Utilities:
- Active/Passive Cluster, Active/Active Cluster
- Failover Cluster, Load Balanced Cluster
- Shared-Nothing Cluster, Shared-Disk Cluster
- Cluster resources
- Cluster services
- Quorum
- Fencing
- Split brain
- Redundancy
- Mean Time Before Failure (MTBF)
- Mean Time To Repair (MTTR)
- Service Level Agreement (SLA)
- Disaster Recovery
- Replication
- Session handling

334.2 Load Balanced Clusters
Weight: 6

Description: Candidates should know how to install, configure, maintain and troubleshoot LVS. This includes the configuration and use of keepalived and ldirectord. Candidates should further be able to install, configure, maintain and troubleshoot HAProxy.

Key Knowledge Areas:

- Understanding of LVS / IPVS
- Basic knowledge of VRRP
- Configuration of keepalived
- Configuration of ldirectord
- Backend server network configuration
- Understanding of HAProxy
- Configuration of HAProxy

Terms and Utilities:

- ipvsadm
- syncd
- LVS Forwarding (NAT, Direct Routing, Tunneling, Local Node)
- connection scheduling algorithms
- keepalived configuration file
- ldirectord configuration file
- genhash
- HAProxy configuration file
- load balancing algorithms
- ACLs

334.3 Failover Clusters
Weight: 6

Description: Candidates should have experience in the installation, configuration, maintenance and troubleshooting of a Pacemaker cluster. This includes the use of Corosync. The focus is on Pacemaker 1.1 for Corosync 2.x.

Key Knowledge Areas:

- Pacemaker architecture and components (CIB, CRMd, PEngine, LRMd, DC, STONITHd)
- Pacemaker cluster configuration
- Resource classes (OCF, LSB, Systemd, Upstart, Service, STONITH, Nagios)
- Resource rules and constraints (location, order, colocation)
- Advanced resource features (templates, groups, clone resources, multi-state resources)
- Pacemaker management using pcs
- Pacemaker management using crmsh
- Configuration and Management of corosync in conjunction with Pacemaker
- Awareness of other cluster engines (OpenAIS, Heartbeat, CMAN)

Terms and Utilities:

- pcs
- crm

- crm_mon
- crm_verify
- crm_simulate
- crm_shadow
- crm_resource
- crm_attribute
- crm_node
- crm_standby
- cibadmin
- corosync.conf
- authkey
- corosync-cfgtool
- corosync-cmapctl
- corosync-quorumtool
- stonith_admin

334.4 High Availability in Enterprise Linux Distributions
Weight: 1

Description: Candidates should be aware of how enterprise Linux distributions integrate High Availability technologies.

Key Knowledge Areas:
- Basic knowledge of Red Hat Enterprise Linux High Availability Add-On
- Basic knowledge of SUSE Linux Enterprise High Availability Extension

Terms and Utilities:
- Distribution specific configuration tools
- Integration of cluster engines, load balancers, storage technology, cluster filesystems, etc.

LPIC3 High Availability Cluster Storage

Tecnologies:

Implementar els continguts descrits a LPIC3 304-200 334: High Availability Cluster Storaget:

- ❏ 335.1 DRBD / cLVM
- ❏ 335.2 Clustered File Systems

Topic 335: High Availability Cluster Storage

335.1 DRBD / cLVM
Weight: 3

Description: Candidates are expected to have the experience and knowledge to install, configure, maintain and troubleshoot DRBD devices. This includes integration with Pacemaker. DRBD configuration of version 8.4.x is covered. Candidates are further expected to be able to manage LVM configuration within a shared storage cluster.

Key Knowledge Areas:

- Understanding of DRBD resources, states and replication modes
- Configuration of DRBD resources, networking, disks and devices
- Configuration of DRBD automatic recovery and error handling
- Management of DRBD using drbdadm
- Basic knowledge of drbdsetup and drbdmeta
- Integration of DRBD with Pacemaker
- cLVM
- Integration of cLVM with Pacemaker

Terms and Utilities:

- Protocol A, B and C
- Primary, Secondary
- Three-way replication
- drbd kernel module
- drbdadm
- drbdsetup
- drbdmeta
- /etc/drbd.conf
- /proc/drbd
- LVM2
- clvmd
- vgchange, vgs

335.2 Clustered File Systems
Weight: 3

Description: Candidates should know how to install, maintain and troubleshoot installations using GFS2 and OCFS2. This includes integration with Pacemaker as well as awareness of other clustered filesystems available in a Linux environment.

Key Knowledge Areas:

- Understand the principles of cluster file systems
- Create, maintain and troubleshoot GFS2 file systems in a cluster
- Create, maintain and troubleshoot OCFS2 file systems in a cluster
- Integration of GFS2 and OCFS2 with Pacemaker
- Awareness of the O2CB cluster stack
- Awareness of other commonly used clustered file systems

Terms and Utilities:

- Distributed Lock Manager (DLM)
- mkfs.gfs2
- mount.gfs2
- fsck.gfs2
- gfs2_grow
- gfs2_edit
- gfs2_jadd
- mkfs.ocfs2
- mount.ocfs2
- fsck.ocfs2
- tunefs.ocfs2
- mounted.ocfs2
- o2info
- o2image
- CephFS
- GlusterFS
- AFS

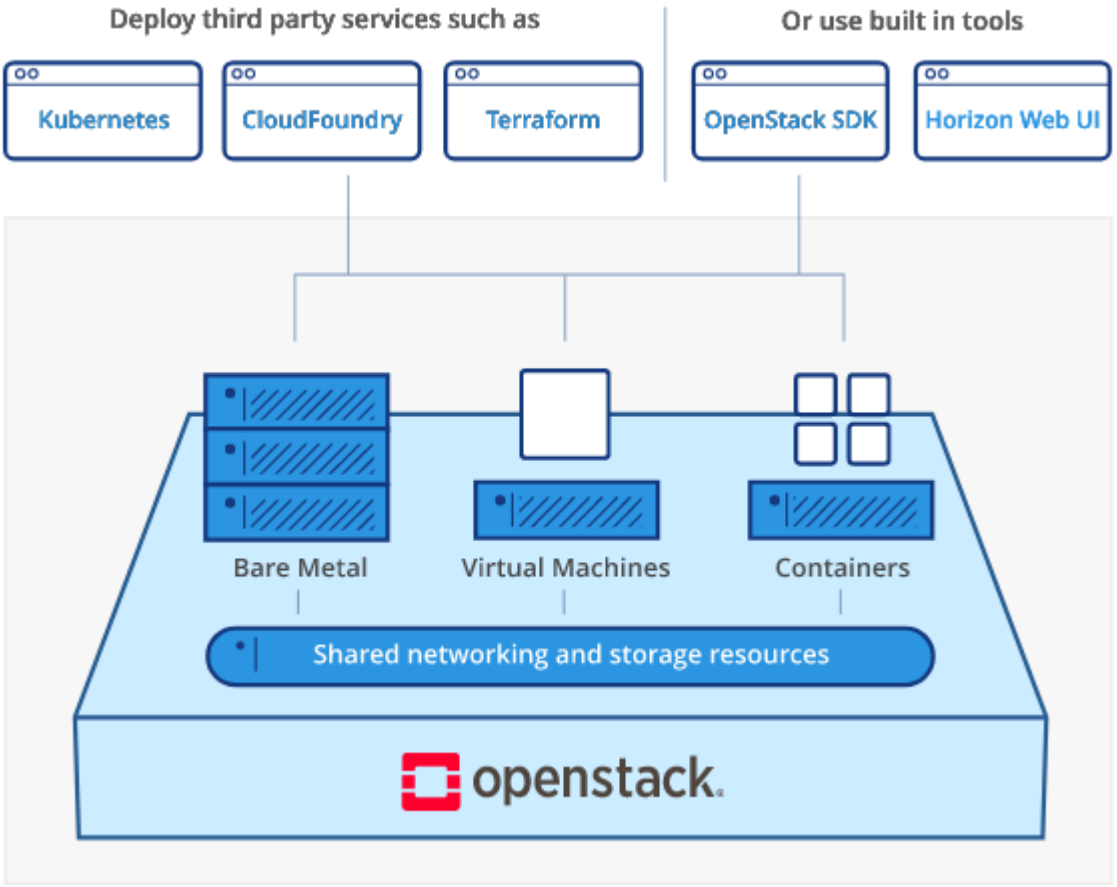
OpenStack

OpenStack is a free open standard cloud computing platform, mostly deployed as infrastructure-as-a-service (IaaS) in both public and private clouds where virtual servers and other resources are made available to users. The software platform consists of interrelated components that control diverse, multi-vendor hardware pools of processing, storage, and networking resources throughout a data center. Users either manage it through a web-based dashboard, through command-line tools, or through RESTful web services.

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed and provisioned through APIs with common authentication mechanisms.

Cloud Infrastructure for Virtual Machines, Bare Metal, and Containers. Openstack controls large pools of compute, storage, and networking resources, all managed through APIs or a dashboard.

Beyond standard infrastructure-as-a-service functionality, additional components provide orchestration, fault management and service management amongst other services to ensure high availability of user applications.



Vagrant / Terraform / Packer

E la bogeria de conceptes i evolució de la informàtica d'avui en dia les eines de virtualització, de virtualització al cloud i de *Infraestructure as Code* són extensament usades. La família d'eines i software de Hashicorp és una de les més usades. Aquest projectes consisteix en explorar la funcionalitat i les prestacions de les eines Vagrant, Terraform, Packer i la seva interrelació amb altres eines i el Cloud, en especial el AWS EC2.

Vagrant

Vagrant is a development environment automation tool. It accomplishes this by leveraging virtual machines with VirtualBox, VMWare, or cloud providers like AWS. It's primarily designed to standardize environments across platforms.
Vagrant makes it easy to create reproducible virtualised environments. Machines are provisioned on top of VirtualBox, VMWare, AWS, or any other provider. Vagrant includes support for configuration management tools like Chef or Ansible.
Vagrant works as a layer on top of virtualisation software aka hypervisor like Oracle Virtual box (or) Vmware workstation.
Vagrant is a minimal form of Infrastructure as Code concept and intended for development infrastructure building/provisioning where Terraform is a full-fledged IaC product from the same company (Hashicorp) is a leader in the IaC market.

Terraform

Is a full-fledged IaC product from the same company (Hashicorp) is a leader in the IaC market.

Terraform is the infrastructure as code tool from HashiCorp. It is a tool for building, changing, and managing infrastructure in a safe, repeatable way. Operators and Infrastructure teams can use Terraform to manage environments with a configuration language called the HashiCorp Configuration Language (HCL) for human-readable, automated deployments

If you are new to infrastructure as code as a concept, it is the process of managing infrastructure in a file or files rather than manually configuring resources in a user interface. A resource in this instance is any piece of infrastructure in a given environment, such as a virtual machine, security group, network interface, etc.

At a high level, Terraform allows operators to use HCL to author files containing definitions of their desired resources on almost any provider (AWS, GCP, GitHub, Docker, etc) and automates the creation of those resources at the time of apply.

Packer

HashiCorp Packer automates the creation of any type of machine image. It embraces modern configuration management by encouraging you to use automated scripts to install and configure the software within your Packer-made images. Packer brings

machine images into the modern age, unlocking untapped potential and opening new opportunities.

Seguretat: Intrusion detection Systems

Snort

It is an **open source** intrusion prevention system capable of **real-time** traffic analysis and packet logging. Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013.

Snort's open source network-based intrusion detection/prevention system (IDS/IPS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: 1. sniffer, 2. packet logger, and 3. network intrusion detection.

Sniffer Mode

The program will read network packets and display them on the console.

Packet Logger mode

In packet logger mode, the program will log packets to the disk.

Network Intrusion Detection System Mode

In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Objectius:

- Explicar el concepte de Intrusion detection Systems.
- Explicar el funcionament de snort.
- Mostrar amb exemples reals el funcionament d'Snort.

OpenVAS

https://en.wikipedia.org/wiki/OpenVAS

The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

OpenVAS (Open Vulnerability Assessment System, originally known as GNessUs) is a software framework of several services and tools offering vulnerability scanning and vulnerability management.

All OpenVAS products are free software, and most components are licensed under the GNU General Public License (GPL). Plugins for OpenVAS are written in the Nessus Attack Scripting Language, NASL.

OpenVAS began under the name of GNessUs, as a fork of the previously open source Nessus scanning tool, after its developers Tenable Network Security changed it to a proprietary (closed source) license in October 2005.[2] OpenVAS was originally proposed by pentesters at SecuritySpace[3], discussed with pentesters at Portcullis Computer Security[4] and then announced[5] by Tim Brown on Slashdot.

OpenVAS is a member project of Software in the Public Interest.

Authenticació

Nextcloud + Collabora / OnlyOffice

Nextcloud és una sèrie de programaris client-servidor amb l'objectiu de crear servei d'allotjament de fitxers. La seva funcionalitat és similar al programari Dropbox, encara que Nextcloud és de tipus codi obert, permetent a qui ho desitgi d'instal·lar-lo en un servidor privat. La seva arquitectura oberta permet d'afegir funcionalitats addicionals al servidor en forma d'aplicacions. Nextcloud és un projecte paral·lel d'ownCloud, que també én un programari de servei d'allotjament al núvol.

Tasques a fer:

- Configurar un servidor segur amb Nextcloud, incloent les apps de Collabora i OnlyOffice com a complements via App Store.
- Documentar el procés d'instal·lació i d'assegurar el servidor
- Comparar funcionalitats respecte Google Suite pel que fa a:
    - Sincronització d'arxius (Google Drive)
    - Sincronització de calendaris
    - Sincronització de contactes
    - Treball col·laboratiu en línia: comparar Google Docs amb Collabora i OnlyOffice
        - Diferents tipus de documents: Text, Fulls de càlcul, Presentacions. Altres (si n'hi ha)
        - Control de versions d'arxius o històric de versions
        - Possibilitat d'edició simultània
        - Control d'accés: (visualització, edició) × (usuaris autenticats, usuaris anònims)
- Recursos / escalabilitat: quins recursos de maquinari / connectivitat calen en funció dels usuaris (totals / simultanis)?
- Comparació d'aplicacions/funcionalitats entre clients PC i clients per a mòbil (Android i iOS).

LPIC3 FreeIPA

Tecnologies: FreeIPA

Implementar els continguts descrits a LPIC3 303-200 326-Host Security corresponents a 326.4 FreeIPA Installation and Samba Integration

326.4 FreeIPA Installation and Samba Integration
Weight: 4

Description: Candidates should be familiar with FreeIPA v4.x. This includes installation and maintenance of a server instance with a FreeIPA domain as well as integration of FreeIPA with Active Directory.

Key Knowledge Areas:

- Understand FreeIPA, including its architecture and components
- Understand system and configuration prerequisites for installing FreeIPA
- Install and manage a FreeIPA server and domain
- Understand and configure Active Directory replication and Kerberos cross-realm trusts
- Be aware of sudo, autofs, SSH and SELinux integration in FreeIPA

Terms and Utilities:

- 389 Directory Server, MIT Kerberos, Dogtag Certificate System, NTP, DNS, SSSD, certmonger
- ipa, including relevant subcommands
- ipa-server-install, ipa-client-install, ipa-replica-install
- ipa-replica-prepare, ipa-replica-manage

Autenticació: OAUTH / OTP / 2factors

Implementar mecanismes d'autenticació de tipus OAUTH, també mecanismes OTP i mecanismes de 2-factors. Explicar què són, com funcionen, tecnologies actuals i implementar-ho en casos concrets.

Per exemple:

- Funcionament de OAUTH de google.
- Funcionament OAUTH de amazon.
- Implementar autenticació OAUTH a un servidor grafana en funcionament.
- Implementar autenticació OAUTH en un servei http.

- Funcionament de OTP
- Eines actuals.
- Exemples pràctics de implementació.

- Funcionament de autenticació amb 2-factors.
- Eines actuals.
- Implementació pràctica.

Seguretat / Certificats Digitals

Processament de Certificats

Els objectius a aconseguir d'aquest crèdit són els següents :

- Compilar tots (o la majoria) de certificats digitals que s'estan fent servir actualment, tant per identificar-se com a persona física per entrar a Aplicacions com LaMevaSalut, com per identificar-se com a empresa per entrar a Aplicacions com les de declaració d'impostos de l'AEAT.

Cal tenir en compte que quan el certificat digital és d'una empresa, conté el nom de l'empresa, el nom de la persona física I el tipus de representació que aquesta persona física té atorgat en nom de l'empresa (administrador, representant legal, membre junta executiva, etc

- Especificar I exemplificar l'estructura que utilitza cadascun dels certificats digitals segons quina sigui l'entitat certificadora

- Llegir les dades de cadascun dels tipus certificats des d'una web I des d'un o més navegadors

- Validar cadascun dels certificats a través d'apis publicades per les entitats certificadors

- Construir un servei que retorni les dades I la validació de qualsevol certificat digital, sigui quin sigui el tipus i sigui quina sigui l'entitat certificadora

DNSSEC

Tecnologies: DNS, OpenSSL, TLS

Implementar un servidor DNSSEC seguint els requeriments de coneixements descrits al LPIC3 303-200 325.4 DNS and Cryptography

325.4 DNS and Cryptography

Description: Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. The version of BIND covered is 9.7 or higher.

Key Knowledge Areas:

- Understanding of DNSSEC and DANE
- Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones
- Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients
- Key Signing Key, Zone Signing Key, Key Tag
- Key generation, key storage, key management and key rollover
- Maintenance and re-signing of zones
- Use DANE to publish X.509 certificate information in DNS
- Use TSIG for secure communication with BIND

Terms and Utilities:

- DNS, EDNS, Zones, Resource Records
- DNS resource records: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM, TLSA
- DO-Bit, AD-Bit
- TSIG
- named.conf
- dnssec-keygen
- dnssec-signzone
- dnssec-settime
- dnssec-dsfromkey
- rndc
- dig
- delv
- openssl