

ENLLAÇ GITHUB: <https://github.com/MarquesSanchezMarc/PROJECTE-24-25.git>

INDEX

[INTRODUCCIÓ/PLANIFICACIO 5](#_Toc197726857)

[BENEFICIS 5](#_Toc197726858)

[PROXMOX 6](#_Toc197726859)

[BASE TEORIA - DISSENY 6](#_Toc197726860)

[IMPLEMENTACIÓ DE LA SOLUCIÓ 8](#_Toc197726861)

[- INSTAL·LACIÓNS I CONFIGURACIONS INICIALS 8](#_Toc197726862)

[- CONFIGURACIÓ DE XARXA 9](#_Toc197726863)

[- CONFIGURACIÓ DEL EMMAGATZEMATGE 11](#_Toc197726864)

[- CONFIGURACIÓN DE RECURSOS 12](#_Toc197726865)

[- CONFIGURACIÓ CLUSTER 13](#_Toc197726866)

[- CONFIGURACIÓ HA (ALTA DISPONIBILITAT) 14](#_Toc197726867)

[- CONFIGURACIÓ REPLICA 15](#_Toc197726868)

[VALIDACIÓ I PROVES 16](#_Toc197726869)

[- AIXECAR EL CLUSTER I PFSENSE 16](#_Toc197726870)

[- PROVA DELS DISCOS ZFS MIRROR 16](#_Toc197726871)

[- PROVA DE CLÚSTER I MIGRACIÓ EN VIU 16](#_Toc197726872)

[- SIMULACIÓ DE FALLADA I ALTA DISPONIBILITAT (HA) 16](#_Toc197726873)

[- RÈPLICA DE CONTENIDORS (ZFS REPLICATION) 17](#_Toc197726874)

[- MONITORATGE I SEGUIMENT DEL RENDIMENT 17](#_Toc197726875)

[DOCKER 18](#_Toc197726876)

[BASE TEÒRICA I DISSENY 18](#_Toc197726877)

[IMPLEMENTACIÓ DE LA SOLUCIÓ 19](#_Toc197726878)

[Fase 1: Docker Compose 19](#_Toc197726879)

[Fase 2: Docker Swarm 21](#_Toc197726880)

[Fase 3: Mesures de seguretat 23](#_Toc197726881)

[Fase 4: Kubernetes 24](#_Toc197726882)

[VALIDACIÓ I PROVES 25](#_Toc197726883)

[- PROVA DE DESPLEGAMENT AMB DOCKER I KUBERNETES 25](#_Toc197726884)

[- ESCALABILITAT D’UN SERVEI WEB A KUBERNETES 25](#_Toc197726885)

[- FUNCIONAMENT DE LA WEB I INTRODUCCIÓ DE DADES A LA BASE DE DADES 25](#_Toc197726886)

[- XAT EN TEMPS REAL I CONSULTA D’USUARIS 25](#_Toc197726887)

[- SIMULACIÓ DE FALLADA I AUTORECUPERACIÓ AMB DOCKER SWARM 25](#_Toc197726888)

[SNORT 26](#_Toc197726889)

[BASE TEÒRICA I DISSENY 26](#_Toc197726890)

[IMPLEMENTACIÓ DE LA SOLUCIÓ 27](#_Toc197726891)

[Fase 1: Instal·lació i compilació de Snort 27](#_Toc197726892)

[Fase 2: Preparació de l’entorn 28](#_Toc197726893)

[Fase 3: Creació de regles pròpies 29](#_Toc197726894)

[Fase 4: Automatització de notificacions per correu 30](#_Toc197726895)

[VALIDACIÓ I PROVES 31](#_Toc197726896)

[- DETECCIÓ D’AMENACES EN TEMPS REAL AMB SNORT 31](#_Toc197726897)

[- ENVIAMENT AUTOMÀTIC D’ALERTES PER CORREU 32](#_Toc197726898)

[- BLOQUEIG AUTOMÀTIC D’IP AMB IPTABLES 33](#_Toc197726899)

[ZABBIX 34](#_Toc197726900)

[BASE TEORIA - DISSENY 34](#_Toc197726901)

[- INTRODUCCIÓ A LA MONITORITZACIÓ 34](#_Toc197726902)

[- SELECCIÓ I JUSTIFICACIÓ DE L’EINA 34](#_Toc197726903)

[IMPLEMENTACIÓ DE LA SOLUCIÓ 35](#_Toc197726904)

[- INSTAL·LACIÓ I CONFIGURACIÓ BÀSICA 35](#_Toc197726905)

[- TRIGGERS 38](#_Toc197726906)

[- ALERTA 38](#_Toc197726907)

[- SCRIPTS CUSTOM 41](#_Toc197726908)

[- CONFIG EN ZABBIX 41](#_Toc197726909)

[- CONFIG EMAIL 43](#_Toc197726910)

[- DASHBOARD PERSONALITZAT 44](#_Toc197726911)

[- INFORMES 44](#_Toc197726912)

[VALIDACIÓ I PROVES 45](#_Toc197726913)

[CPD 46](#_Toc197726914)

[CONCLUSIONS 47](#_Toc197726915)

[ANNEX 48](#_Toc197726916)

[Annex – Proxmox 48](#_Toc197726917)

[Annex – Docker 48](#_Toc197726918)

[Annex – Snort 48](#_Toc197726919)

[Annex – Zabbix 48](#_Toc197726920)

[BIBLIOGRAFIA 49](#_Toc197726921)

[PROXMOX VE 49](#_Toc197726922)

[ZABBIX 49](#_Toc197726923)

[PFSENSE 49](#_Toc197726924)

[SNORT (IDS/IPS) 49](#_Toc197726925)

[DOCKER 49](#_Toc197726926)

[KUBERNETES 50](#_Toc197726927)

[VIRTUALBOX 50](#_Toc197726928)

INTRODUCCIÓ/PLANIFICACIO

Disseny i implementació d'un entorn de virtualització basat en Proxmox, en el qual s'instal·laran contenidors Docker per al funcionament d'aplicacions i serveis. A més, s'implementarà un sistema de supervisió de xarxes amb Zabbix i un sistema de detecció d'intrusions (IDS) utilitzant Snort per assegurar la seguretat i el rendiment de l'entorn.

Aquest projecte se centrarà en assegurar una alta disponibilitat, eficàcia operativa i ràpida resposta a incidents, optimitzant l’entorn per a un ús segur i escalable. Així, possibilitaria integrar virtualització, contenidors, monitorització i seguretat en una única solució sòlida i completa.

BENEFICIS

**Major accessibilitat i redundància:** Entorn molt disponible, minimitzant el temps d'inactivitat i garantint un accés ininterromput als serveis.

**Escalabilitat efectiva:** Desenvolupament d'aplicacions escalables mitjançant Docker, facilitant un creixement continu.

**Monitorització anticipada:** Detecció inicial d'inconvenients amb Zabbix, cosa que facilita actuar abans que impactin al servei.

**Seguretat reforçada:** Snort oferirà una capa extra de defensa en identificar i reduir intrusions de manera instantània.

**Optimització de recursos:** Ús més eficient del maquinari a través de virtualització i contenidors, enllaçant rendiment al màxim.

**LINK TRELLO:** [**https://trello.com/invite/b/67c8904e9f7fe1c80961f621/ATTI0c5eef765d468892d2f640c8508f66caE52B1691/projecte-asix-24-25**](https://trello.com/invite/b/67c8904e9f7fe1c80961f621/ATTI0c5eef765d468892d2f640c8508f66caE52B1691/projecte-asix-24-25)

PROXMOX

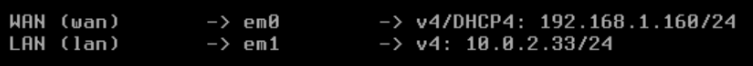
BASE TEORIA - DISSENY

En aquest apartat s’expliquen els conceptes tècnics i el raonament del disseny de la infraestructura virtual. S’hi justifica la tria de tecnologies, la topologia de xarxa, l’estructura dels nodes i l’estratègia d’emmagatzematge i seguretat.

Per desplegar una infraestructura virtualitzada funcional i segura, vam utilitzar PFSense com a firewall i servidor DHCP, i Proxmox VE com a plataforma de virtualització. Aquesta combinació ens permet controlar tant el trànsit de xarxa com la gestió de màquines virtuals i contenidors des d'una interfície centralitzada.

PFSense actua com a punt de control entre la xarxa externa (WAN) i la xarxa interna (LAN):

* Interfície WAN: 192.168.1.160, amb IP fixa assignada al router domèstic per proporcionar accés estable a Internet.
* Interfície LAN: 10.0.2.33, des d'on s’assignen automàticament adreces IP dins el rang 10.0.2.0/24 a totes les màquines i al propi Proxmox mitjançant DHCP.



A més de filtrar el trànsit, PFSense ofereix serveis com VPN segures (WireGuard) i control precís de ports amb regles personalitzades.

Proxmox és el pilar de la infraestructura virtual. Tenim tres nodes:

* PX1 amb IP 10.0.2.70
* PX2 amb IP 10.0.2.71
* PX3 amb IP 10.0.2.72

Formen un clúster, cosa que permet l’administració unificada i l’alta disponibilitat.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Cada node disposa de:

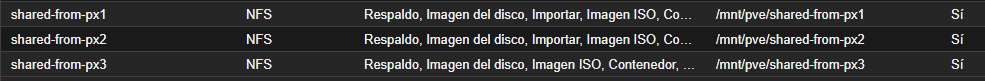
* 1 disc de 1 TB per al sistema operatiu (basat en Debian).
* 2 discos addicionals d’1 TB configurats com a ZFS en mirror, garantint redundància davant fallades de disc.

Texto

El contenido generado por IA puede ser incorrecto.Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

L’emmagatzematge es comparteix mitjançant NFS dins la xarxa 10.0.2.0/24, permetent ha els nodes que accedeixin a les dades dels contenidors (CTs) i màquines virtuals (VMs) de manera simultània.



IMPLEMENTACIÓ DE LA SOLUCIÓ

Aquí es descriu com s’ha dut a terme el projecte en la pràctica: des de la instal·lació del sistema, la configuració de màquines virtuals i contenidors, fins a la definició dels recursos, la configuració de la xarxa interna i la implementació de l’emmagatzematge compartit. És la part operativa on es detalla que s’ha fet i com de manera resumida, si vols més informació tens els annexos de cada mini projecte.

* INSTAL·LACIÓNS I CONFIGURACIONS INICIALS

Per iniciar el projecte, descarregarem la ISO oficial de Proxmox VE, <https://www.proxmox.com>, crearem les maquines a VirtualBox (PX1, PX2, PX3).

Exemple de la configuració en quan recursos Hardware (RAM, NUCLIS, EMMAGATZEMATGE) i Xarxa (ADAPATADOR EN RED INTERNA) de PX1.

Texto

El contenido generado por IA puede ser incorrecto.

Per millorar el rendiment en la nostre maquina important tenir aquesta opció activada.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Aquest es el procés de instal·lacio del SO Proxmox VE base, sense cap configuració avançada.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

* CONFIGURACIÓ DE XARXA

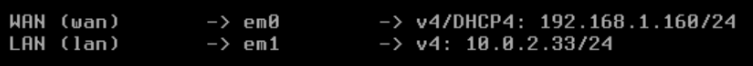
Procés d’instal·lació de PFSense

Interfaz de usuario gráfica, Texto, Aplicación, Tabla

El contenido generado por IA puede ser incorrecto.

Configuració de PFSense

* Interfície WAN: 192.168.1.160, amb IP fixa assignada al router domèstic per proporcionar accés estable a Internet.
* Interfície LAN: 10.0.2.33, des d'on s’assignen automàticament adreces IP dins el rang 10.0.2.0/24 a totes les màquines i al propi Proxmox mitjançant DHCP.



Configuració Xarxa dins Proxmox

La xarxa 10.0.2.0/24 és completament funcional i interna, per la qual cosa, les VMs poden fer ping entre elles i poden accedir a Internet si PFSense ho permet

enp0s3: És la interfície de xarxa física (o en aquest cas virtual, ja que s’està utilitzant VirtualBox). Aquesta interfície representa el dispositiu de xarxa que connecta la màquina host amb la xarxa externa.

vmbr0 (Linux Bridge): És un switch virtual creat per Proxmox. Aquesta interfície actua com una passarel·la perquè les màquines virtuals i contenidors puguin accedir a la xarxa. Està en mode bridge amb enp0s3, permetent que les màquines virtuals comparteixin la mateixa xarxa que l’host.

Captura de pantalla de un videojuego

El contenido generado por IA puede ser incorrecto.

* CONFIGURACIÓ DEL EMMAGATZEMATGE

Aquí es on creem els pools ZFS en mirror en cada node i els NFS compartits a la xarxa.

Tal com es pot veure a la captura, hem creat un pool anomenat pool-compartido utilitzant dos discos virtuals (dispositius /dev/sdb i /dev/sdc). Aquests dos discos estan configurats en mode mirror amb ZFS.

Si un dels discos falla, el sistema pot seguir funcionant amb l’altre, garantint redundància i alta disponibilitat de les dades.

Captura de pantalla de un celular

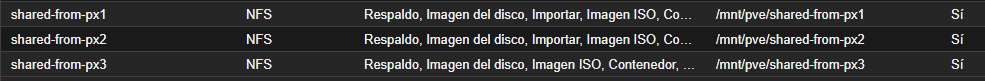
El contenido generado por IA puede ser incorrecto.

**DEMO AQUÍ!**

Tal com es pot observar a la captura, s'han configurat tres recursos d'emmagatzematge compartit mitjançant NFS, un per cada node del clúster: shared-from-px1, shared-from-px2 i shared-from-px3.

Cada un d'aquests recursos es munta a la ruta corresponent dins de /mnt/pve/, permetent que tots els nodes tinguin accés als fitxers compartits com ara còpies de seguretat, imatges de disc, ISOs o contenidors.

Aquesta configuració facilita la col·laboració entre nodes i garanteix una infraestructura flexible i escalable dins de l'entorn virtualitzat amb Proxmox.



* CONFIGURACIÓN DE RECURSOS

Els recursos de CPU, RAM i disc es van assignar segons les necessitats de cada màquina. Per defecte, les VMs disposen de 2 CPUs i 2 GB de RAM, i els CTs, més lleugers, de 1 CPU i 1 GB de RAM.

VM (DOCKER)

Captura de pantalla con la imagen de una pantalla

El contenido generado por IA puede ser incorrecto.

CT (NGINX)

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Per exemple, el CT de Nginx, en servir només contingut web, funciona correctament amb 1 GB i 1 nucli. En canvi, la VM de Zabbix, que fa monitoratge i gestiona una base de dades, requereix 4 GB de RAM i 2 CPUs.

CT (ZABBIX)

Interfaz de usuario gráfica, Aplicación, Sitio web

El contenido generado por IA puede ser incorrecto.

Cada node compta amb 1 TB per a emmagatzematge, repartit segons les necessitats de cada servei. Proxmox facilita l’ajust dels recursos en temps real, fet que permet adaptar l’entorn de manera flexible i eficient.

* CONFIGURACIÓ CLUSTER

Gràcies a la creació del clúster, la interfície de Proxmox es transforma en una plataforma de gestió centralitzada i molt més potent. Ara podem veure i controlar tots els nodes (px1, px2, px3) des d’un sol punt, cosa que simplifica enormement l’administració de la infraestructura.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.Una de les opcions més interessants és la migració en viu de màquines virtuals i contenidors entre nodes sense necessitat d’apagar-les, ideal per fer manteniment sense interrupcions. També destaca la possibilitat de tenir emmagatzematge compartit, com es veu a les etiquetes “shared-from”, que permet accedir als mateixos volums des de diferents nodes. Això facilita la redundància, alta disponibilitat i escalabilitat.

En aquesta imatge es pot veure que el procés de unió del PX2 al clúster s’ha completat correctament.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

* CONFIGURACIÓ HA (ALTA DISPONIBILITAT)

L’alta disponibilitat (HA) és un sistema que ens assegura que les màquines virtuals o contenidors continuaran funcionant encara que un dels nodes del clúster falli. Això es fa possible perquè tenim diversos servidors (nodes) treballant junts dins d’un mateix clúster, i si un d’ells cau, un altre pot continuar oferint el servei automàticament.

Perquè l’alta disponibilitat funcioni, el primer pas és crear un grup HA amb almenys tres nodes del clúster. A la imatge es pot veure com s’ha creat el grup HA-CLUX1, format pels nodes px1, px2 i px3. Cada node té assignada una prioritat, que determina quin serà el següent en agafar el relleu si hi ha una fallada.

El PX1 és el més important, per tant li hem posat més prioritat. El PX2 és el segon més important. El PX3 no volem que tingui màquines, excepte en cas d’un col·lapse total; en aquest cas s’utilitzaria el PX3.

Captura de pantalla de un videojuego

El contenido generado por IA puede ser incorrecto.

Haurem de agregar totes les maquines que volem que es migrin soles en cas de fallada.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

**DEMO AQUÍ!**

* CONFIGURACIÓ REPLICA

Una de les funcions més útils de Proxmox VE és la possibilitat de fer còpies (rèpliques) de màquines virtuals entre diferents ordinadors del clúster. Això serveix per tenir una còpia actualitzada d’una màquina en un altre node, per si hi ha algun problema o falla.

Per poder fer-ho, cal tenir mínim dos nodes en clúster, i l’espai d’emmagatzematge ha de ser de tipus ZFS, ja que aquest sistema de fitxers permet la sincronització eficient de volums i snapshots.

A la imatge podem veure que es pot triar cada quan volem fer la còpia de la màquina: cada 30 minuts, cada dia a una hora concreta, només de dilluns a divendres, o fins i tot cada 15 minuts en horari laboral. Això ens ajuda a adaptar les còpies segons com s’utilitza la màquina.

També es pot posar un límit de velocitat perquè la còpia no ocupi tota la xarxa, i només cal activar la casella “Activado” per començar. Un cop fet això, Proxmox farà les rèpliques automàticament segons l’horari que hem escollit.

Per crear un “Trabajo de replicación” haurem de anar a la maquina o contenidor que volem replicar i buscar “Replicación”, on podrem agregar-la.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.Com es pot veure en les següents imatges, em creat un replica en el contenidor nginx, cada dia a les 21 hores, on el node destí serà PX3.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.Haurem de tenir em compte que a maquina haurà de estar en el ZFS, per poder-se replicar.

Per fer la prova em programat una ara, com es pot veure en el registre la replica s’ha replicat correctament.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

VALIDACIÓ I PROVES

En aquest apartat es comprova que la solució funciona correctament. Inclou les proves de comunicació entre màquines, clúster i alta disponibilitat (HA), rèpliques entre nodes, així com la monitorització del rendiment. També s’avalua la capacitat de resposta davant fallades i la flexibilitat de l’entorn.

* AIXECAR EL CLUSTER I PFSENSE

Es va aixecar manualment pfSense i els tres nodes del clúster Proxmox (PX1, PX2 i PX3). Un cop en funcionament, el sistema va mostrar tots els serveis actius, els nodes sincronitzats i el clúster operatiu, confirmant que tot l’entorn virtual es pot iniciar de forma correcta.

[**DEMO AQUÍ!**](DEMOS/LEVANTAR-CLUSTER.mp4)

* PROVA DELS DISCOS ZFS MIRROR

Es va simular la desconnexió d’un dels discos del ZFS mirror al node PX1 per comprovar la tolerància a fallades. El sistema va continuar funcionant sense problemes i ZFS va marcar el pool com a “DEGRADED”, mantenint les dades gràcies al segon disc (/dev/sdc).

**[DEMO AQUÍ!](DEMOS/ZFS.mp4)**

* PROVA DE CLÚSTER I MIGRACIÓ EN VIU

Un cop creat el clúster entre PX1, PX2 i PX3, es va comprovar la funcionalitat de live migration. Es va migrar una màquina virtual d’un node a un altre sense necessitat d’apagar-la, assegurant la continuïtat del servei.

[**DEMO AQUÍ!**](DEMOS/MIGRACION.mp4)

* SIMULACIÓ DE FALLADA I ALTA DISPONIBILITAT (HA)

Es va crear un grup HA amb prioritats entre nodes. Per validar-lo, es va apagar manualment el node principal (PX1) i es va comprovar que les màquines crítiques es reassignaven automàticament a PX2 o PX3.

[**DEMO AQUÍ!**](DEMOS/MIGRACION.mp4)

* RÈPLICA DE CONTENIDORS (ZFS REPLICATION)

Es va configurar una rèplica programada per al contenidor de Nginx, amb sincronització automàtica cap a PX3. A més, es va fer una prova de restauració manual en cas de pèrdua del node original.

[**DEMO AQUÍ!**](DEMOS/REPLICAS.mp4)

* MONITORATGE I SEGUIMENT DEL RENDIMENT

Mitjançant la interfície de Proxmox i l’eina Zabbix, es va monitorar l’ús de CPU, RAM, disc i trànsit de xarxa. Es van detectar pics puntuals i s’ajustaren els recursos de les màquines per optimitzar-ne el rendiment.

**[DEMO AQUÍ!](DEMOS/ESTADO-NODOS.mp4)**

DOCKER

BASE TEÒRICA I DISSENY

Aquest miniprojecte té como objectiu implementar un desplegament de microserveis amb orquestradors utilitzant Docker Swarm i Kubernetes dins de l’entorn de Proxmox, on hem creat les màquines virtuals i contenidors pel desplegament. El contenidors permeten executar aplicacions més eficient i lleuger a diferencia de les màquines virtuals.

Nosaltres hem escollit l’arquitectura LAMP (Linux, Apache, MySQL i PHP), on hem desplegat cada servei en un contenidor independent. Per gestionar aquests serveis hem comparat 3 opcions: Docker Swarm, Docker Compose i Kubernetes.

IMPLEMENTACIÓ DE LA SOLUCIÓ

Fase 1: Docker Compose

Hem creat una màquina de Ubuntu on vam fer la instal·lacció de Docker Compose, vam crear el fitxer docker-compose.yml on configurem el diferents ports, volums i variables d’entorn per poder desplegar el serveis LAMP.

Texto

El contenido generado por IA puede ser incorrecto.

Després d'executar docker-compose up -d, els serveis es van posar en marxa i vam comprovar el correcte funcionament del phpmyadmin i la web.

**Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.**Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

**Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.**

Fase 2: Docker Swarm

Per escalar el projecte, es va inicialitzar un clúster amb `docker swarm init` i s'hi va afegir un node secundari.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Es va crear un fitxer docker-stack.yml per desplegar els serveis amb rèpliques, configuracions de volum i secrets.

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Pel desplegament dels serveis definits hem utilitzat el docker stack deploy i després hem comprovat el seu correcte funcionament.

Texto

El contenido generado por IA puede ser incorrecto.Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Fase 3: Mesures de seguretat

S'han aplicat pràctiques de seguretat com l’autenticació entre nodes mitjançant certificats, xifratge TLS per a les comunicacions internes i la gestió de secrets amb docker secret create, evitant exposar contrasenyes als fitxers.

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Fase 4: Kubernetes

Hem migrat tota la infraestructura a Kubernetes creant fitxers deployment, service, pvc i namespace.

Texto

El contenido generado por IA puede ser incorrecto.

Hem desplegat tots els recursos i comprovem la persistència, escalabilitat i l'accés extern amb serveis de tipus NodePort i LoadBalancer.

**Pantalla de computadora con letras

El contenido generado por IA puede ser incorrecto.**

VALIDACIÓ I PROVES

* PROVA DE DESPLEGAMENT AMB DOCKER I KUBERNETES

Es van crear els fitxers necessaris per definir els serveis web, base de dades i gestor phpMyAdmin. Amb docker-compose up es va desplegar l'entorn inicial. Posteriorment, es va aplicar kubectl apply -f k8s/ per desplegar l’arquitectura completa dins de Kubernetes, creant automàticament pods, serveis i volums persistents al clúster. Es va validar l’accés a través dels ports NodePort i LoadBalancer.

[**DEMO AQUÍ!**](DEMOS/Desplegament%20dels%20serveis%20Docker.mp4) **(DOCKER)**

[**DEMO AQUÍ!**](DEMOS/Desplegament%20de%20Kubernetes.mp4) **(KUBERNETES)**

* ESCALABILITAT D’UN SERVEI WEB A KUBERNETES

Per comprovar la capacitat d’escalat, es va escalar manualment el servei web a 3 rèpliques amb kubectl scale deployment web --replicas=3. Es va verificar que totes les rèpliques es trobaven en estat Running, demostrant que Kubernetes gestiona l’escalabilitat dels serveis de manera efectiva.

[**DEMO AQUÍ!**](DEMOS/Escalabilitat%20d'un%20servei.mp4)

* FUNCIONAMENT DE LA WEB I INTRODUCCIÓ DE DADES A LA BASE DE DADES

Es va accedir a la pàgina web desplegada i es va utilitzar un formulari PHP per registrar usuaris. Les dades es van emmagatzemar a la base de dades MySQL i es van consultar des de phpMyAdmin. Es va validar que la connexió entre serveis funcionava correctament i que els registres es guardaven persistentment.

[**DEMO AQUÍ!**](DEMOS/Funcionament%20de%20la%20pàgina%20i%20introducció%20a%20la%20base%20de%20dades.mp4)

* XAT EN TEMPS REAL I CONSULTA D’USUARIS

Un cop iniciada sessió, la pàgina web permet accedir a un xat en temps real entre usuaris. Els missatges es van emmagatzemar en una taula MySQL separada. Es va validar que el xat funcionava correctament entre diferents usuaris registrats, reforçant la funcionalitat multiusuari de l’aplicació.

[**DEMO AQUÍ!**](DEMOS/Funcionament%20del%20xat.mp4)

* SIMULACIÓ DE FALLADA I AUTORECUPERACIÓ AMB DOCKER SWARM

Per comprovar la tolerància a fallades, es va eliminar manualment una rèplica del servei web dins del clúster Docker Swarm. Automàticament, el sistema va detectar la pèrdua i va crear una nova instància per mantenir les rèpliques definides. Aquesta prova va demostrar la funcionalitat d'autoreparació integrada en Swarm.

[**DEMO AQUÍ!**](DEMOS/Simulació%20de%20fallida%20i%20autorecuperació%20en%20Docker%20Swarm.mp4)

SNORT

BASE TEÒRICA I DISSENY

En un entorn de xarxa, la seguretat no només es basa en tallafocs i autenticacions, sinó també en la capacitat de **detectar i respondre a amenaces internes o externes**. Per això, en aquest projecte hem treballat amb sistemes **IDS (Intrusion Detection System)** i **IPS (Intrusion Prevention System)**, enfocats a identificar comportaments anòmals, atacs i vulnerabilitats explotades dins del nostre entorn.

IMPLEMENTACIÓ DE LA SOLUCIÓ

Fase 1: Instal·lació i compilació de Snort

Vam preparar una màquina virtual amb sistema operatiu Linux (Ubuntu 24.04 LTS), on vam instal·lar totes les dependències necessàries per compilar Snort des del codi font. Entre aquestes dependències hi havia llibreries essencials com libpcap-dev, daq, luajit, libluajit-5.1-dev, així com eines de compilació com gcc, make i autoconf.

Texto

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

Fase 2: Preparació de l’entorn

Després de compilar i instal·lar Snort amb èxit, vam procedir a preparar l’entorn per garantir-ne un funcionament correcte i organitzat. Aquest pas és fonamental, ja que Snort necessita una estructura clara per emmagatzemar les regles, la configuració i els logs d’alertes generades.

Amb aquesta configuració vam indicar que la nostra subxarxa protegida és 10.0.2.0/24, mentre que qualsevol altre origen es considera tràfic extern.

Texto

El contenido generado por IA puede ser incorrecto.

Pel que fa a la sortida d’alertes, vam configurar Snort perquè enregistrés les deteccions a un fitxer concret amb la següent línia:

Texto

El contenido generado por IA puede ser incorrecto.

Fase 3: Creació de regles pròpies

A local.rules, vam afegir regles com:

* Detecció de ping ICMP.
* Connexions SSH sospitoses.
* Escaneig ràpid de ports amb Nmap.
* Peticions HTTP GET.
* Atacs de força bruta via SSH.

Això ens va permetre detectar activitats reals simulades des de Kali Linux.

Texto

El contenido generado por IA puede ser incorrecto.

Fase 4: Automatització de notificacions per correu

Vam instal·lar Postfix i mailutils i vam configurar l’enviament amb Gmail mitjançant TLS i autenticació SASL. Vam crear el fitxer /etc/postfix/sasl\_passwd amb la contrasenya d’aplicació de Gmail i el vam protegir amb permisos adequats.

Per automatitzar-ho, vam crear un script snort\_alert\_mailer.sh que llegeix el log, envia les alertes per correu i esborra el fitxer:

Texto

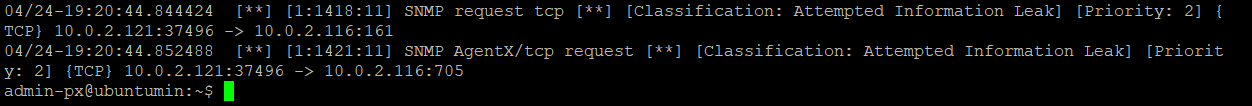
El contenido generado por IA puede ser incorrecto.

VALIDACIÓ I PROVES

* DETECCIÓ D’AMENACES EN TEMPS REAL AMB SNORT

Això va permetre monitoritzar el trànsit en temps real des de la interfície de xarxa virtual del nostre entorn. Es van generar intencionadament connexions sospitoses des de Kali Linux, com escaneigs amb Nmap, intents de connexió SSH i peticions ICMP. Snort va detectar correctament aquestes accions i les va registrar al fitxer /var/log/snort/alerts.log. Es va comprovar que totes les alertes apareixien amb la informació corresponent: tipus d’atac, protocol, IP d’origen i de destinació.

**Texto

El contenido generado por IA puede ser incorrecto.**

* ENVIAMENT AUTOMÀTIC D’ALERTES PER CORREU

Per automatitzar l’avís d’alertes, es va crear l’script snort\_alert\_mailer.sh, que llegeix el fitxer de logs i envia el contingut per correu electrònic utilitzant mailutils i postfix. Es va configurar correctament l’enviament SMTP a través de Gmail i es va validar l’entrega de correus a l’adreça configurada. L’script s’executa automàticament cada 5 minuts mitjançant cron, garantint que l’administrador rebi notificacions constants.

Texto

El contenido generado por IA puede ser incorrecto.Imagen de la pantalla de un computador

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

* BLOQUEIG AUTOMÀTIC D’IP AMB IPTABLES

Amb l’script snort-blocker.sh, es va afegir funcionalitat de resposta activa al sistema. Quan es detecta una IP sospitosa en els logs de Snort, l’script llegeix l’adreça i executa una regla de iptables per bloquejar-la automàticament. Aquesta acció es va validar provocant intents de força bruta amb Hydra, i es va comprovar que l’adreça atacant quedava denegada en posteriors intents de connexió.

**Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.Pantalla de computadora con letras

El contenido generado por IA puede ser incorrecto.**Texto

El contenido generado por IA puede ser incorrecto.

ZABBIX

BASE TEORIA - DISSENY

* INTRODUCCIÓ A LA MONITORITZACIÓ

La monitorització de xarxa és essencial per controlar el funcionament dels sistemes informàtics, ja que permet detectar anomalies, anticipar problemes i millorar l’eficiència. A través d’aquesta pràctica, es poden supervisar paràmetres com l’ús de CPU, memòria, estat dels serveis o la disponibilitat dels equips.

Durant la fase inicial del projecte es va fer una anàlisi comparativa d’eines populars com Nagios, Pandora, Observium, LogicMonitor i Cacti, estudiant els avantatges i inconvenients de cadascuna.

* SELECCIÓ I JUSTIFICACIÓ DE L’EINA

Després de valorar diferents opcions, es va optar per utilitzar Zabbix com a eina principal de monitorització. La decisió es va basar en criteris com la seva compatibilitat amb entorns virtualitzats (en aquest cas, Proxmox), la possibilitat de fer autodescobriment de dispositius, l’ús de triggers personalitzats, el suport per a notificacions automàtiques per correu electrònic i la seva extensa comunitat de suport.

Zabbix també destaca per la seva capacitat de gestionar múltiples dispositius i sistemes des d’una única interfície centralitzada.

IMPLEMENTACIÓ DE LA SOLUCIÓ

* INSTAL·LACIÓ I CONFIGURACIÓ BÀSICA

Per agilitzar la instal·lació, es va utilitzar un script automatitzat de la comunitat (Tteck Scripts) per desplegar Zabbix com a contenidor dins de Proxmox. Aquesta metodologia va permetre configurar de forma ràpida la IP, els recursos i la base de dades.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Un cop instal·lat, es va accedir a la interfície web per completar el procés de configuració i iniciar la gestió dels hosts.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

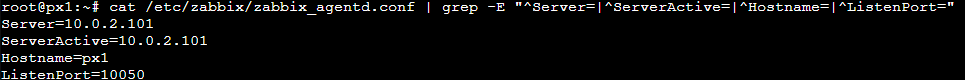
Es va afegir el node PX1 com a primer host i s’hi va instal·lar l’agent Zabbix per començar a recollir dades de rendiment en temps real.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Un cop configurat això haurem de instal·lar i configurar en cada node el zabbix-agent.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Tot seguit ja començarem a veure gràfics, items i triggers que s’han creat automàticament.

Imagen de la pantalla de un computador

El contenido generado por IA puede ser incorrecto.Imagen de la pantalla de un computador

El contenido generado por IA puede ser incorrecto.

* TRIGGERS

RAM – CPU

Aquest trigger detecta si l’ús de la CPU al host PX1 supera el 90 % durant un període d’1 minut. Si es compleix aquesta condició, s’activa una alerta amb severitat "Warning" per indicar una possible saturació del sistema. La descripció informa que l’elevada càrrega pot provocar lentitud en la resposta.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Aquest trigger comprova si l’ús de memòria al host PX1 supera el 80 % durant 1 minut. Si es compleix la condició, genera una alerta amb severitat "Average", indicant que el sistema està consumint gairebé tota la memòria disponible. La descripció informa que el sistema s’està quedant sense memòria lliure.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

* ALERTA

Aquesta acció està configurada per activar-se quan qualsevol dels tres triggers d'ús elevat de CPU (superior al 90 %) s’activa en els nodes PX1, PX2 o PX3. El tipus de càlcul "A or B or C" indica que només cal que un dels triggers salti perquè es generi l'acció. L’opció "Enabled" està activada, però falta definir una operació (com enviar correu) perquè funcioni correctament.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Aquesta configuració defineix l’operació de notificació per correu electrònic quan es detecta un ús elevat de CPU. El missatge s’envia a l’usuari *Admin (Zabbix Administrator)* a través del mitjà *Email*. El correu inclou informació personalitzada com el nom del host, la data, l’hora, el trigger activat, l’estat i el valor del paràmetre que ha provocat l’alerta. L’operació s’executa al pas 1, sense límit de repeticions.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Aquesta acció està configurada per enviar notificacions quan es detecti un ús elevat de memòria (RAM > 80 %) en qualsevol dels tres nodes PX1, PX2 o PX3. El càlcul està establert com a “A or B or C”, per la qual cosa només cal que un dels triggers definits s’activi perquè l’acció s’executi. L’opció "Enabled" està activada, però cal definir una operació perquè la notificació es pugui enviar correctament.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Perfecte. Aquesta operació envia un correu electrònic quan es detecta un ús elevat de memòria RAM. El missatge es dirigeix a l'usuari *Admin (Zabbix Administrator)* i s’envia per correu amb un text personalitzat que inclou el nom del host, la data, hora, trigger activat, estat i valor monitoritzat. L’operació s’activa en el pas 1 i no es repeteix més d’una vegada. Amb aquesta configuració, l'acció queda completament funcional.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

* SCRIPTS CUSTOM

S’ha configurat el fitxer zabbix\_agentd.conf del node PX1 per incloure tres paràmetres personalitzats (UserParameter), cadascun associat a un script que comprova si un punt de muntatge NFS està actiu.

Cada script, com el check\_nfs\_px1.sh, comprova si el directori /mnt/pve/shared-from-px1 està muntat. Si ho està, retorna OK; en cas contrari, retorna NOT\_MOUNTED. Aquesta sortida és llegida per Zabbix i permet generar alertes si algun NFS deixa d’estar disponible.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.Texto

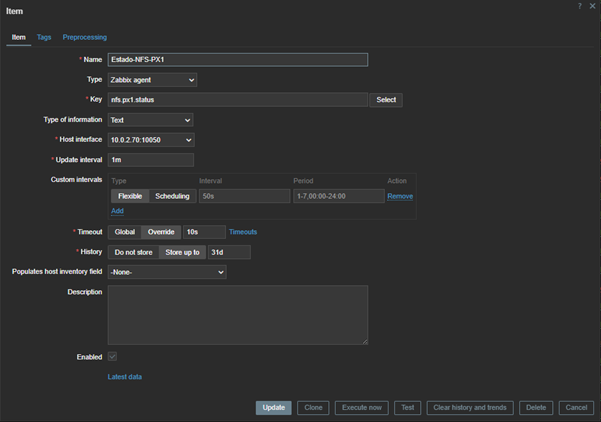
El contenido generado por IA puede ser incorrecto.

* CONFIG EN ZABBIX

ITEM

Aquest ítem de Zabbix comprova l’estat del muntatge NFS de PX1 mitjançant la clau personalitzada nfs.px1.status, definida prèviament al fitxer zabbix\_agentd.conf.

El tipus d’informació és "Text", ja que l’script retorna valors com OK o NOT\_MOUNTED.

****

TRIGGER

Aquest trigger supervisa si el punt de muntatge NFS compartit des de PX1 està actiu. L’expressió last(/PX1/nfs.px1.status)<>"OK" comprova si el darrer valor retornat per l’ítem nfs.px1.status és diferent de "OK". Si és així, s’activa una alerta amb severitat "Warning", indicant que el NFS no està muntat o ha deixat de respondre.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

ALERTA

Aquesta acció anomenada "NFS-Mount-Status" està dissenyada per detectar qualsevol problema relacionat amb el muntatge dels punts NFS entre els nodes PX1, PX2 i PX3.

Funciona amb diversos triggers que comproven si algun dels punts NFS està desmuntat o inaccessible.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Aquesta operació de Zabbix envia un correu electrònic a l’administrador quan es detecta que un punt de muntatge NFS no està actiu. El missatge inclou informació clau com el nom del host, la data, el trigger activat, l’estat de l’alerta i el valor obtingut. S’ha configurat perquè s’enviï immediatament i només una vegada, facilitant així una resposta ràpida davant possibles fallades de connexió NFS.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

* CONFIG EMAIL

S’ha configurat el tipus de mitjà “Email” a Zabbix utilitzant SMTP de Gmail (smtp.gmail.com, port 587) amb autenticació mitjançant usuari i contrasenya. La connexió està protegida amb STARTTLS i els correus es poden enviar en format HTML. Aquesta configuració permet que el sistema enviï alertes automàtiques per correu electrònic.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

* DASHBOARD PERSONALITZAT

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

* INFORMES

Zabbix permet generar informes personalitzats mitjançant la creació de dashboards, widgets i exportació de dades. A través dels panells es poden visualitzar gràfiques d’ús de CPU, memòria, estat de serveis o disponibilitat de xarxa. A més, és possible exportar aquests gràfics o informes en formats com CSV o PDF, fet que facilita la documentació i l’anàlisi fora del sistema.

Aquestes funcionalitats són especialment útils per fer seguiment periòdic de l’estat de la infraestructura i compartir resultats amb altres membres de l’equip o professors.

**EXEMPLES**:

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

VALIDACIÓ I PROVES

Durant aquesta fase es van realitzar proves de monitoratge per verificar el correcte funcionament dels serveis desplegats. Es va simular l'ús intensiu de CPU i RAM per comprovar si els triggers configurats a Zabbix generaven alertes automàtiques, tant al panell com via correu electrònic. També es van desmuntar punts de muntatge NFS per validar les alertes de supervisió d'emmagatzematge.

A mesura que es detectaven problemes o falses alarmes, es van ajustar els valors llindar, la configuració de les expressions i els scripts associats. Finalment, es va comprovar que la monitorització era efectiva, amb notificacions fiables, gràfics actualitzats en temps real i una visibilitat clara sobre l'estat de la infraestructura.

[**VIDEO NFS**](DEMOS/NFS.mp4)

[**VIDEO RAM**](DEMOS/RAM.mp4)

[**VIDEO CPU**](DEMOS/CPU.mp4)

[**VIDEO ESTADO NODOS**](DEMOS/ESTADO-NODOS.mp4)

CPD

CONCLUSIONS

Els resultats obtinguts amb aquest projecte compleixen de manera general els objectius que ens havíem plantejat inicialment. Hem aconseguit implementar correctament solucions tecnològiques com Proxmox per gestionar entorns virtualitzats, Docker i Kubernetes per facilitar el desplegament d’aplicacions escalables, Snort per detectar possibles intrusions, i Zabbix per tenir sota control l’estat dels serveis i infraestructures.

Durant el desenvolupament del projecte, ens hem trobat amb petites dificultats tècniques que hem resolt adaptant la planificació inicial. Tot i això, el resultat final s’ajusta en gran mesura al que havíem previst originalment.

Per tal d’evolucionar el projecte en el futur, considerem important potenciar encara més l'automatització de processos mitjançant eines com Ansible, millorar els sistemes d'alta disponibilitat i recuperació en cas de fallada, i incrementar el nombre d’elements monitoritzats per anticipar-nos millor a les incidències que puguin sorgir.

ANNEX

[Annex – Proxmox](ProxmoxVE.docx)

[Annex – Docker](Docker%20Swarm%20i%20Kubernetes.docx)

[Annex – Snort](IDS.docx)

[Annex – Zabbix](Zabbix.docx)

BIBLIOGRAFIA

PROXMOX VE

Proxmox VE Official Documentation. (s.f.). Proxmox Server Solutions GmbH. Recuperat de: <https://pve.proxmox.com/pve-docs/>

Proxmox VE Wiki. (s.f.). Recuperat de: <https://pve.proxmox.com/wiki/Main_Page>

Tteck's Proxmox Helper Scripts. (s.f.). GitHub Repository. Recuperat de: <https://tteck.github.io/Proxmox/>

Installing Proxmox VE. (s.f.). Proxmox YouTube Channel. Recuperat de: <https://www.youtube.com/@ProxmoxVE>

ZABBIX

Zabbix Documentation 6.0 LTS. (s.f.). Recuperat de: <https://www.zabbix.com/documentation/current>

Zabbix Community Templates. (s.f.). Recuperat de: <https://share.zabbix.com/>

Monitor Everything with Zabbix 6.0 (2023). NetworkChuck [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=U5JZcprPuzo>

Zabbix Install Script per Proxmox – Tteck Scripts. (s.f.). Recuperat de: <https://tteck.github.io/Proxmox/>

PFSENSE

pfSense Documentation. (s.f.). Netgate. Recuperat de: <https://docs.netgate.com/pfsense/en/latest/>

Introduction to pfSense. (2023). Lawrence Systems [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=3K8ppLz-dDs>

SNORT (IDS/IPS)

Snort Documentation. (s.f.). Cisco. Recuperat de: <https://docs.snort.org/>

Installing Snort on Ubuntu. (2022). NetworkChuck [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=ME9zP9-5Nsw>

DOCKER

Docker Docs. (s.f.). Docker Inc. Recuperat de: <https://docs.docker.com/>

Getting Started with Docker. (2023). TechWorld with Nana [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=3c-iBn73dDE>

DockerHub – Images oficials. (s.f.). Recuperat de: <https://hub.docker.com/>

KUBERNETES

Kubernetes Documentation. (s.f.). The Kubernetes Authors. Recuperat de: <https://kubernetes.io/docs/>

Kubernetes for Beginners. (2023). TechWorld with Nana [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=X48VuDVv0do>

VIRTUALBOX

Oracle VM VirtualBox User Manual. (s.f.). Oracle Corporation. Recuperat de: <https://www.virtualbox.org/manual/UserManual.html>

How to use VirtualBox for Proxmox Labs. (2023). TheDigitalLife [YouTube]. Recuperat de: <https://www.youtube.com/watch?v=R9hhxr-zoUQ>