Supuesto 1

Planteamiento

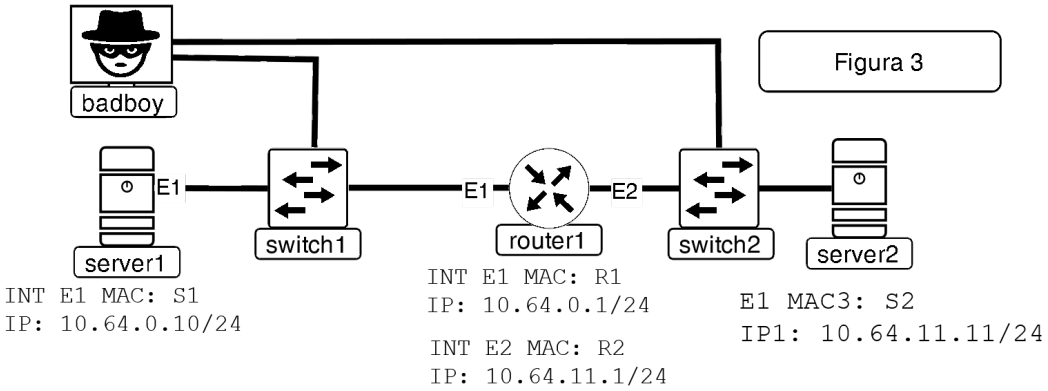
La recién creada universidad de la Valldigna pretende dotar de red cableada y Wi-Fi a un nuevo edificio en el que se instalarán un aula con 25 PC, un CPD con 10 servidores y un total de 20 puntos de acceso Wi-Fi.

Cuestiones:

1. (1 punto) Si solo se dispone de conmutadores ethernet de 24 puertos y 2 de *uplink*, diseñe un esquema de conexión en donde se indique segmentación, tipos de dispositivos conectados y en donde se priorice la seguridad y la eficiencia de recursos. ¿Qué características adicionales debería tener el conmutador o conmutadores del CPD?
2. (1 punto) En un conmutador del aula se detecta un conjunto de paquetes unicast idénticos en todas sus interfaces a excepción de la última. Indique cuál o cuáles pueden ser el origen de este comportamiento y su posible solución. ¿Por qué no se detectan dichos paquetes en la última interfaz?
3. (1 punto) Se pretende dotar a nuestro CPD de un sistema de orquestación de máquinas virtuales (VM) para un conjunto de servidores de API REST. Para ello se decide elegir una opción que soporte la hiperconvergencia y la migración en caliente de VM. Explique qué es la hiperconvergencia, una ventaja y nombre al menos un hipervisor y un orquestador que sean de código abierto (*open source*) y que permitan un funcionamiento hiperconvergente. Nombre un sistema de almacenamiento de código abierto (*open source*) distribuido.
4. (1 punto) Para la base de datos institucional se ha optado por una instalación en la que se pretende hacer uso de volúmenes lógicos de Linux (LVM) sobre un RAID de 2 discos. ¿Qué tipo de esquema RAID escogería y por qué motivo? Indique qué pasos deben seguirse para la creación de un volumen LVM sobre un RAID y qué comando Linux permite crear un RAID. ¿Qué consideración se debe tener respecto al gestor de arranque GRUB con el RAID?
5. (1 punto) Tras sufrir un ataque de denegación de servicio en un servidor REST sobre Linux. se pretende analizar el archivo del log de las conexiones (access.log). Las entradas de dicho log tienen el siguiente formato: [IP ORIGEN] [METODO] [CODIGO]. Sabemos que el ataque está relacionado con peticiones PUT con respuesta de código de estado 200 (OK) En un entorno con múltiples servidores Linux, indique una utilidad para la centralización de los logs. Para evitar el llenado del disco nombre una utilidad concebida para el rotado de logs en sistemas Linux. ¿Qué comando o comandos deberíamos ejecutar para obtener la lista de las últimas 100 IP que cumplan este requisito?
6. (1 punto) Se pretende pasar el servicio REST a un modelo basado en contenedores con escalado bajo demanda. Se baraja el uso de Docker o Kubernetes. Indique cual sería el más adecuado para dicho propósito justificando su elección. Indique qué comando CLI se usa para gestionar tanto Docker como Kubernetes y ponga algún ejemplo de su uso.
7. (1 punto) En un aula con equipos con Windows 11 y Debian GNU/Linux 12 se ha detectado un ataque de suplantación de servidor de DHCP. El ataque consiste en asignar direccionamiento válido y proponerse como router por defecto. Indique brevemente qué

procedimiento usaría para identificar al equipo atacante si solo se tiene acceso a uno de los equipos de laboratorio. ¿Qué comando o comandos usaría en dicho equipo, ya sea Windows o Linux? Indique alguna técnica que poseen algunos conmutadores para protegerse de dichos ataques de DHCP.

8. (1 punto) Durante cierto tiempo el atacante ha conseguido hacer un Man-In-The-Middle y capturar el tráfico de los clientes del aula. Si los clientes se conectan solo por HTTPS y no por HTTP, ¿podría saber el atacante a qué dominios se ha conectado en base a los certificados web destino? Si se quieren servir varios dominios en el mismo servidor web, indique qué ventajas o inconvenientes tiene usar certificados con diversos subjectAltName frente al uso de SNI. ¿Qué mejora introduce ESNI?
9. (1 punto) La siguiente figura describe el montaje de red en el que el equipo *badboy* mediante un ataque ha saturado la tabla CAM del conmutador *switch2* y ha puesto su propio equipo en modo captura de paquetes en ambas interfaces en las que está conectado.



Indique los cinco primeros paquetes que capturará el equipo *badboy* si el servidor *server1* hace un:

```
ping -c1 10.64.11.11    (envía un paquete ICMP ECHO REQUEST)
```

Considere que todas las tablas de ARP están vacías. Indique MAC origen/destino, protocolo y mensaje tal y como muestra el ejemplo (2 puntos).

ORDEN	MAC ORIGEN	MAC DESTINO	MENSAJE
1	S1	FF (Bcast)	ARP: ¿Quién es 10.64.0.1?
2	R2	FF	ARP: ¿Quién es 10.64.11.11?
3	S2	R2	Soy yo, S2

4	R2	S2	ICMP ECHO REQUEST a 10.64.11.11
5	S2	R2	ICMP ECHO REPLY

10. (1 punto) Indique qué diferencias hay entre un cortafuegos *stateless* y uno *stateful*. Indique brevemente las diferencias que hay entre un cortafuegos tradicional, un IDS, un IPS y un WAF. ¿Qué problema puede surgir con equipos con doble tarjeta de red que estén detrás de un cortafuegos?

Supuesto 2

Planteamiento

La Universitat de la Valldigna ha desarrollado una aplicación llamada uvPatentesWeb para la gestión de las patentes de los investigadores. Los datos de la aplicación residen en una base de datos Oracle concretamente en el esquema *patentes*.
Entre otras, con la siguiente tabla:

```
CREATE TABLE "PATENTES"."INVESTIGADORES"
   (
    "COLUMN1" VARCHAR2(20 BYTE) NOT NULL ENABLE,
    "COLUMN2" VARCHAR2(100 BYTE),
    "COLUMN3" VARCHAR2(200 BYTE),
    "COLUMN4" VARCHAR2(20 BYTE),
    "COLUMN5" VARCHAR2(20 BYTE)
   )

   COMMENT ON COLUMN "PATENTES"."INVESTIGADORES"."COLUMN1" IS 'Número de documento, identificador único del investigador';
   COMMENT ON COLUMN "PATENTES"."INVESTIGADORES"."COLUMN2" IS 'nombre del investigador';
   COMMENT ON COLUMN "PATENTES"."INVESTIGADORES"."COLUMN3" IS 'apellidos del investigador';
   COMMENT ON COLUMN "PATENTES"."INVESTIGADORES"."COLUMN4" IS 'fecha de nacimiento';
   COMMENT ON COLUMN "PATENTES"."INVESTIGADORES"."COLUMN5" IS 'fecha de alta en el sistema';
```

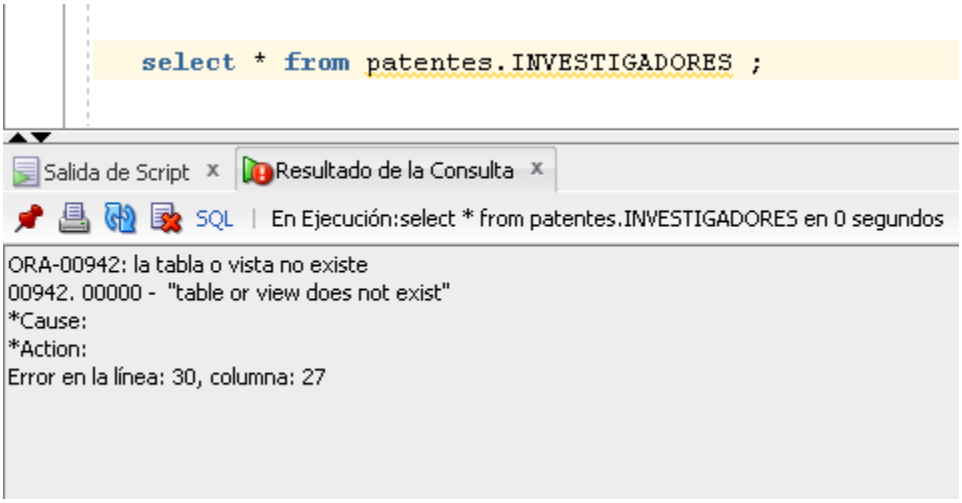
Cuestiones a contestar

1. (1 punto) Desde el punto de vista de la coherencia de la información y la mantenibilidad del código, proponga mejoras modificando la DDL de las tablas.

2. (1 punto) Diseñe una consulta SQL (sobre la tabla de la DDL del apartado número 1 modificada) que devuelva los investigadores que se han dado de alta en el año 2025.

3. (1 punto) Se ha detectado un problema de rendimiento en las consultas de la aplicación que buscan investigadores por apellidos. Proponga alguna medida, mediante DDL, que permita solucionar este problema.

4. (1 punto) Cuando un desarrollador se conecta con su usuario personal a la base de datos donde reside el esquema *patentes* e intenta ver el contenido de la tabla *patentes.investigadores* para ver sus datos, obtiene el siguiente error. Partiendo de que la tabla existe ¿Qué puede estar pasando? ¿Cómo se podría solucionar el problema?



5. (1 punto) Al conectarse con su usuario personal a la base de datos le deja realizar el proceso de *login* pero recibe un mensaje diciendo que tiene que cambiar la contraseña.

Escriba la sentencia para realizar ese cambio, teniendo en cuenta que el nombre de usuario es *manolo*, la contraseña antigua era *roqu2wer* y la nueva *p0l0st0n0.*

6. (1 punto) ¿Qué tecnología Oracle permite ver estados anteriores de objetos de base de datos o devolver objetos de base de datos a un estado anterior sin utilizar la recuperación desde medios físicos o copias de seguridad? Escriba la sentencia SQL necesaria utilizando esta tecnología para recuperar los datos que tenía la tabla investigadores hoy a las 9 de la mañana.

7. (1 punto) Un usuario ha detectado una excepción (NullPointerException) en la aplicación y se requiere encontrarla en los logs de la aplicación que se encuentran en un servidor Linux. Escriba la sentencia que permitiría localizar mediante el comando grep la excepción en todos los ficheros .log del directorio /apps/investigacion/patentes/logs.

8. (1 punto) Se plantea integrar la información de los contratos laborales de los investigadores que reside en una aplicación de RRHH que se encuentra en una base de datos Oracle diferente. Comente dos posibles soluciones tecnológicas para integrar los datos de las aplicaciones y ventajas e inconvenientes de cada una de las soluciones.

9. (1 punto) Diseñe una pizarra Kanban para llevar el control de los bugs que se producen en la aplicación.

10. (1 punto) Es necesario redactar un pliego para el mantenimiento de la aplicación. Diseñe dos indicadores de nivel de servicio que debe cumplir la empresa que resulte adjudicataria del contrato para medir y asegurar el nivel de calidad de dicho servicio.

Supuesto 3

Planteamiento inicial

La universidad de la Valldigna desea desplegar un entorno altamente disponible para sus aplicaciones web y J2EE, así como para páginas web estáticas. Dispone de tres ubicaciones:

- **CPD-A** (principal).
- **CPD-B** (secundario).
- **CPD-C,** una ubicación menor con capacidad limitada de alojamiento de hardware pero sin infraestructura de CPD.

Se dispone de conectividad TCP/IP entre los tres y posibilidad de un enlace de fibra oscura dedicada, con baja latencia y alta capacidad, entre el CPD-A y CPD-B.

El despliegue propuesto deberá cumplir los siguientes requisitos:

- Alta disponibilidad (HA)
- Capacidad de recuperación ante desastres (DR)
- Balanceo de carga
- Consistencia de dato entre sitios

Especificaciones

- La topología debe considerar tanto servicios web (estáticos y dinámicos) como aplicaciones J2EE.
- Aplicaciones Web J2EE desplegadas sobre servidores de aplicaciones.
- Se deberá considerar la publicación de contenido web estático.
- Acceso web externo a través de balanceadores.
- El almacenamiento deberá estar replicado entre el CPD-A y el CPD-B.
- Se deben considerar mecanismos de recuperación ante desastres.
- Se debe incluir un mecanismo de monitorización y alertas.

Cuestiones a contestar:

1. (2 puntos) Proponga una topología lógica y física describiendo la función de cada uno de los componentes. Describa y justifique cada uno de los elementos tales como balanceadores, frontales web, servidores de aplicaciones, servidores de bases de datos, almacenamiento replicado, elementos de monitorización y de seguridad, etc.
2. (1 punto) Plantee protocolos, mecanismos y procedimientos de recuperación en caso de un escenario de parada total de un CPD y un escenario de caída de las comunicaciones entre dos CPDs.
3. (1 punto) Describa la configuración de una estrategia de alta disponibilidad para los servidores de aplicaciones tales como Websphere, Weblogic o JBoss.
4. (1 punto) Proponga estrategias y herramientas para monitorización y resiliencia de los CPDs basadas en respuestas automáticas ante eventos provenientes de la

monitorización. Ponga un ejemplo de procedimiento de respuesta ante una situación de incremento de tráfico en los frontales web.

5. (1 punto) Describa al menos dos mecanismos para evitar el *split-brain* en el clúster de base de datos teniendo en cuenta la topología descrita en el enunciado, describiendo las ventajas e inconvenientes de los mismos.
6. (1 punto) Proponga mecanismos de seguridad para proteger los servicios ofrecidos vía web ante ataques de nivel de aplicación como XSS o inyección de SQL. Justifique su respuesta en función de criterios de coste, funcionalidad y prestaciones y, en caso de añadir nuevos elementos a la topología propuesta, indique los cambios.
7. (1 punto) Defina una estrategia de backup que cumpla las políticas 3-2-1 (3 copias en al menos 2 soportes y al menos 1 fuera de las instalaciones). ¿Qué elementos adicionales serían necesarios para implementar esta estrategia?
8. (2 puntos) Suponga que uno de los sistemas de la Universidad está categorizado con nivel alto en el Esquema Nacional de Seguridad. Indique dos medidas técnicas obligatorias sobre el sistema operativo de los servidores y justifique su relación con los principios de integridad y trazabilidad.