PARLAMENTO DE ANDALUCIA

PROCESO SELECTIVO PARA EL INGRESO EN EL CUERPO TÉCNICO DEL PARLAMENTO DE ANDALUCÍA, ESCALA TÉCNICOS DIPLOMADOS, ESPECIALIDAD INFORMÁTICA

TERCER EJERCICIO

12 DE SEPTIEMBRE DE 2020

PARLAMENTO DE ANDALUCIA

Introducción

A raíz de la pandemia de COVID-19, el Parlamento de Andalucía decide actualizar su reglamentación interna para contemplar el teletrabajo de los empleados públicos en aquellos puestos cuyas funciones lo permitan, disminuyendo así el contacto entre trabajadores y minimizando el riesgo de contagio dentro del centro de trabajo. En consecuencia, el Servicio de Informática del Parlamento de Andalucía debe acometer las actuaciones necesarias para adaptar la infraestructura hardware y software, los procedimientos de gestión y la atención al usuario.

Suponga que la infraestructura de servidores del Parlamento utiliza virtualización basada VMware con hipervisor ESXi. Los equipos de usuario serán terminales Windows 10. Se cuenta con un servidor VPN y con un antivirus corporativo de acción en la red local.

Los servicios esenciales, que contemplan tanto la Sede Electrónica, la Oficina Virtual, el Sistema de Gestión Parlamentaria y el Sistema de Gestión Contable se suministran mediante servidores Linux virtualizados, siendo todos ellos Red Hat Enterprise Linux 7 o bien CentOS 7. Los servicios de bases de datos se proporcionan mediante un servidor Oracle 19c y un servidor PostgreSQL 12, estando cada uno desplegado en un servidor virtual con CentOS 7. Las aplicaciones se sirven haciendo uso de servidores de aplicaciones Wildfly 16 y Tomcat 8.5, además de servidores web Apache 2.4.

Usted como técnico informático de la Institución deberá resolver las cuestiones que se le plantean. Para contestar a las preguntas planteadas se podrán hacer las suposiciones que considere oportunas justificándolas adecuadamente.

Apartado 1 (25 puntos)

Para la puesta en marcha del nuevo entorno de teletrabajo, desde el Servicio de Informática se contemplan las siguientes medidas: incorporación de equipos portátiles adicionales, sustitución paulatina de los equipos de trabajo de los usuarios por terminales portátiles, adquisición de nuevos equipos para videoconferencias y ampliación del equipamiento red y seguridad existentes. A este respecto se le plantean las siguientes cuestiones:

1.1 Debido a una rotura en el stock de portátiles, el proveedor no puede suministrarlos a tiempo, estimándose un retraso de al menos 3 meses con respecto a la fecha prevista de inicio del teletrabajo. A fin de paliar los efectos de este contratiempo, el Parlamento de Andalucía propone permitir que aquellos a los que se permita teletrabajar se conecten a los equipos de sus respectivos puestos de trabajo desde sus equipos personales a través de una VPN. Describa los diferentes riesgos para la seguridad que plantea este escenario, relacionándolos con medidas de seguridad del Esquema Nacional de Seguridad y proponiendo medidas paliativas para los mismos.

1.2 Proponga y realice una breve descripción de otras alternativas que permitan que los usuarios teletrabajen de forma más segura. Proponga las modificaciones que considere oportunas sobre sistemas hardware y software descritos.

1.3 Se le solicita que aplique mejoras sobre los sistemas descritos con el objetivo de mejorar la provisión de servicio, la escalabilidad de los sistemas y el uso de recursos.

1.4 A fin de mejorar la seguridad en este nuevo escenario de trabajo, se desea efectuar el bastionado o *hardening* de los servidores anteriormente descritos. Proponga y describa posibles actuaciones a aplicar.

1.5 Se plantea la modificación radical del CPD (centro de procesamiento de datos) actual de forma que pase a ser una infraestructura hiperconvergente. Defina hiperconvergencia de sistemas y describa las ventajas y los inconvenientes que plantea esta infraestructura.

Apartado 2 (15 puntos)

Como parte de la infraestructura local de sistemas del Parlamento de Andalucía, se dispone de una solución de backup que realiza copias de seguridad de los sistemas de información esenciales. Esta infraestructura dispone de una red SAN con dos switches, una cabina de almacenamiento y una librería LTO.

2.1 Para la realización de las copias de seguridad, la ventana de backup de que se dispone es de lunes a jueves de 22:00 a 7:00 de la mañana y desde el viernes a las 16:00 hasta el lunes a las 7:00. Describa la política de backup que le parezca más adecuada para garantizar que se pueden recuperar los sistemas de información esenciales en caso de que se produzca algún desastre que precise la restauración de los mismos. En la solución debe indicar qué antigüedad mínima tendrán los datos en caso de que se realice una restauración, así como a partir de qué hora se podrían volver a tener disponibles los datos.

2.2 Actualmente, muchos usuarios siguen guardando ficheros de manera local en sus equipos y realizando copias de seguridad en dispositivos extraíbles, pese a que esta manera de trabajo incumple la normativa de seguridad y protección de datos de la Institución. Aprovechando la nueva forma de trabajo en remoto, desde el Servicio de Informática se va a promover el uso de un recurso de red compartido (servidor de ficheros) en el que los usuarios de los equipos Windows puedan consolidar copias de manera manual de sus ficheros de trabajo. Para este fin se ha pensado adquirir nuevo equipamiento de almacenamiento. El Parlamento cuenta con 200 usuarios, para cada uno de los cuales se estima que son necesarios unos 100 GB de almacenamiento. Describa las características técnicas y la configuración que realizaría de la infraestructura de almacenamiento que será necesario adquirir. Como mínimo debe indicar el tipo, cantidad y tamaño de los discos, el tipo de configuración RAID y los protocolos de comunicaciones que usaría, tanto a nivel de red como para la provisión del dato.

2.3 Proponga y describa alternativas para mejorar la solución de backup actual.

Apartado 3 (20 puntos)

Como técnico informático del Parlamento, se le solicita la administración de diversos servidores GNU/Linux mediante línea de comandos. La totalidad de los servidores a administrar son Red Hat Enterprise Linux 7 o bien CentOS 7, por tanto, utilizan *systemd*. Puede asumir que utiliza el intérprete de comandos *bash* con nomenclatura POSIX y que tiene permisos de *root* o similares para cada uno de los casos propuestos.

3.0 Indique mediante línea de comandos cómo puede modificar la caducidad de la contraseña de un determinado usuario, con nombre de usuario *examuser*, de forma que caduque a los 60 días, avisándole de la expiración de la misma durante los 10 días anteriores a tal fecha de caducidad.

3.1 Se le solicita que dé de alta un nuevo usuario con nombre de usuario *liferay*, sin directorio de inicio en */home*, impidiendo que haga login sobre el sistema y añadiéndolo al grupo de usuarios *wildfly* como grupo secundario.

3.2 Indique cómo finalizar, mediante el envío de una señal SIGKILL, todos los procesos de sistema que estén escuchando en el puerto TCP 8080.

3.3 Indique los comandos necesarios para instalar el servidor Apache, activándolo tras la instalación como servicio y haciendo que éste se inicie automáticamente en el inicio del sistema.

3.4 Modifique de forma recursiva todos los ficheros y subdirectorios del directorio */opt/serv/tomcat/webapps/miapp* para que pertenezcan al usuario *tomcat*, grupo *tomcat.*

3.5 Muestre el tamaño de subdirectorios del directorio */opt/serv*, llegando hasta el segundo nivel de anidación, mostrando los resultados en formato *human-readable*.

3.6 Busque y elimine recursivamente todos los ficheros con extensión *.log* con antigüedad mayor a 30 días, localizados en el directorio actual y en todos sus subdirectorios.

3.7 El sistema de monitorización del estado de servidores le advierte que un servidor tiene el disco principal del sistema al 85% de capacidad:

a) Especifique las diferentes alternativas de que dispone para ampliar el almacenamiento de la máquina virtual, el aprovisionamiento de disco que elegiría y cómo lo ampliaría en el sistema, intentando que no haya parada de servicio. Puede plantear el uso de cualquier plataforma de virtualización y cualquier hipervisor.

b) Suponga que la partición principal de disco forma parte de un volumen lógico generado mediante LVM.

La salida del comando *pvdisplay* indica lo siguiente:

```
--- Physical volume ---
PV Name               /dev/sda1
VG Name               centos
PV Size               39,51 GiB / not usable 3,00 MiB
```

La salida del comando *lvdisplay* indica lo siguiente

```
--- Logical volume ---
LV Path                /dev/centos/root
LV Name                root
VG Name                centos
```

Indique los comandos para ampliar el disco en 100GB. Puede generar otra partición en */dev/sda2* si es necesario.

3.8 Como apoyo al sistema de backup actual se dispone de un servidor *backupficheros* en el que se realizan copias de ficheros de otros servidores.

a) Escriba un script en *bash* que realice una copia de todos los ficheros del servidor *psedeelectronica*, ubicados en la ruta */opt/webapps/sede* en la ruta */backup/sede/* del servidor *backupficheros*.

Una vez realizada la copia de los ficheros se debe generar un fichero comprimido en formato tar.gz que contenga dichos ficheros. El nombre del fichero debe contener la fecha y hora actuales del sistema con el siguiente formato *sede_YYYYMMDD_hhmm*. Por ejemplo, el fichero de backup correspondiente al 1 de septiembre de 2020, generado a las 12:35 horas, tendrá como nombre *sede_20200901_1235.tar.gz* El fichero se almacenará en el directorio */opt/nfsbackup* del servidor *backupficheros*.. Por ejemplo, el fichero de backup correspondiente al 1 de septiembre de 2020, generado a las 12:35 horas, tendrá como nombre *sede_20200901_1235.tar.gz*

Para conectarse a ambos servidores puede utilizar el usuario *root* con contraseña *examenA2*.

Se valorará que se minimice el trasvase de datos entre el servidor origen y el de backup.

b) El script deberá ejecutarse diariamente de lunes a viernes a las 2:00 de la madrugada. Detalle la línea que deberá introducirse en el fichero *crontab* para programar la ejecución del script mediante cron. El script se encuentra almacenado en */opt/scripts/backup_sede.sh*.

3.9 En un servidor se encuentra instalado el servidor de bases de datos PostgreSQL, el cual hace uso del puerto 5432 del sistema. No obstante, el firewall del sistema bloquea por defecto, permitiendo que sólo accedan aquellas direcciones que se indiquen de forma expresa mediante reglas de firewall. Indique los comandos para permitir que el firewall del sistema permita que la dirección IP 10.145.1.2 tenga acceso al puerto 5432, así como para aplicar los cambios sin tener que reiniciar el sistema. Puede proporcionar soluciones utilizando *firewalld*, *iptables*, *nftables* o cualquier otra alternativa, siempre que lo indique.

Apartado 4 (10 puntos)

Dado el escenario anteriormente descrito, se le solicita que como técnico informático del Parlamento de Andalucía modele el proceso de negocio que permitiría a los empleados públicos del Parlamento de Andalucía solicitar la modalidad de teletrabajo desde la Sede Electrónica del Parlamento de Andalucía. Debe describir el proceso utilizando la notación gráfica del estándar BPMN 2.0.2.

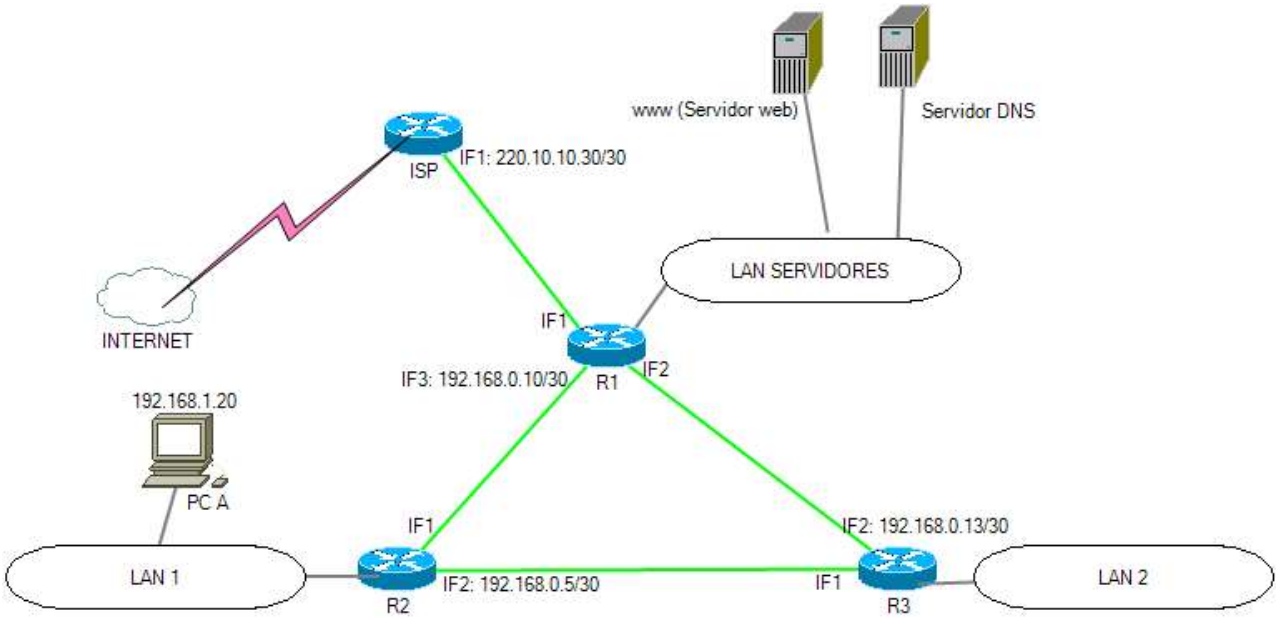
Se le facilitan las siguientes especificaciones sobre el proceso:

- El empleado público, autenticado en la Sede Electrónica, rellenará la solicitud, la firmará electrónicamente y la registrará en la sede, adjuntando los documentos justificantes que sean necesarios.
- Tras registrarse, se envía al Servicio de Personal. La persona con rol "Responsable del Servicio de Personal" aceptará o denegará la solicitud, firmando en todo caso su respuesta.
- En caso de denegación por parte del Servicio de Personal, se enviará al solicitante el documento de denegación de solicitud, previamente firmado electrónicamente por la persona con rol "Responsable del Servicio de Personal", indicando además si es subsanable o no. Si la denegación es por causa subsanable, el solicitante podrá enviar documentación anexa a la solicitud y reenviarla al Servicio de Personal, vía sede electrónica. Si la denegación es por causa no subsanable, el procedimiento finaliza.
- Si la solicitud se acepta por parte del Servicio de Personal, se envía a Secretaría General Adjunta, para el visto bueno, en forma de firma electrónica, de la persona con rol "Letrado Adjunto". La aceptación o denegación se enviará al solicitante en todo caso. Además, si se ha aceptado la solicitud, se enviará un aviso al Servicio de Personal.
- La revisión por parte de Secretaría General Adjunta caducará a los 10 días, transcurridos los cuales se entenderá por denegada. Se enviaría un aviso tanto al Servicio de Personal como una notificación electrónica al solicitante.
- Si el empleado público no recibe respuesta en 30 días, se da por denegada la solicitud. No obstante, se le enviará una notificación electrónica alertando de la caducidad de la solicitud y por tanto de su denegación.

Suponga que el proceso se encuentra exento del cumplimiento de los plazos descritos en la Ley 39/2015.

Apartado 5 (30 puntos)

Dado el siguiente diagrama de red:



5.1 Indique qué dirección IP y máscara de subred debe asignarse a las interfaces de enlace entre routers para las que el diagrama no muestra dicha información (interfaces IF1 e IF2) Indique también cuál sería la dirección de red de cada uno de esos enlaces.

5.2 Se dispone del direccionamiento privado 192.168.2.0/23. Asigne direcciones de red a las subredes LAN SERVIDORES y LAN 2 asumiendo que se conectarán 200 hosts por subred. Indique cuál sería el rango de direcciones IP disponibles para los hosts de cada una de estas subredes y la máscara de subred y puerta de acceso predeterminada que podría configurárseles. Indique también máscara de subred y puerta de acceso predeterminada para LAN 1, respetando la IP que se muestra en el diagrama para el PC A y suponiendo que tendrá un número de hosts similar a LAN 2.

5.3 Indique para qué utilizaría NAT en esta arquitectura de red y en qué puntos concretos de la misma lo usaría. Proporcione ejemplos con direcciones IP y puertos TCP/UDP concretos en los que detalle cómo el uso de NAT afectaría a los paquetes.

5.4 Especifique el contenido de las tablas de enrutamiento de los routers que aparecen en el diagrama, así como del PC A para que todos los hosts de las distintas LAN tengan conectividad entre sí y acceso a Internet.

5.5 Indique para qué podrían usarse firewalls y balanceadores de carga en esta red y dónde y cómo los colocaría.

5.6 Indique para qué podría resultar conveniente el uso de VLAN en esta red.

5.7 Especifique listas de control de acceso (ACL) que satisfagan los siguientes requerimientos, indicando en qué interfaces las aplicaría y en qué dirección. Asigne direcciones IP para los equipos que ofrecen los servicios que se mencionan de acuerdo con el direccionamiento que previamente ha asignado a la LAN a la que pertenecen. Puede utilizar la sintaxis de cualquier fabricante, como por ejemplo la de Cisco IOS, siempre que lo indique previamente.

a) Los equipos de las LAN 1 y LAN 2 sólo podrán acceder a Internet a través de un proxy web ubicado en la LAN SERVIDORES que escucha por el puerto 8123 y sólo podrán acceder a servicios HTTP y HTTPS de Internet.

b) Los equipos de las LAN 1 y LAN 2 podrán acceder directamente a los servicios HTTP y HTTPS que se ofrezcan internamente a través de servidores de la LAN SERVIDORES sin necesidad de hacer uso del proxy web anterior. De hecho, si intentan acceder a través del mismo deberán bloquearse dichos accesos para evitar saturarlo innecesariamente.

c) Los equipos de las LAN 1 y 2 deberán poder acceder a los siguientes servicios de la LAN SERVIDORES: DNS, SMTP, SMTPS, POP3, POPS, IMAP, IMAPS, LDAP, LDAPS, NTP y DHCP.

d) El equipo que ocupa la dirección IP más baja disponible de la LAN 2 debe poder abrir conexiones de escritorio remoto Windows (RDP) contra el PC A de la LAN 1.

e) Debe poderse usar *ping*, *tracert* y *traceroute* por toda la red para facilitar la depuración de problemas de conectividad.

f) El resto de accesos desde las LAN 1 y 2 deben ser bloqueados.

5.8 Suponga que el PC A acaba de encenderse y tiene vacías tanto su tabla ARP como sus cachés de DNS y de navegador web. Indique cuál sería la secuencia de mensajes que se intercambiarían para que su navegador pueda renderizar el resultado devuelto por la URL *http://www.mired.es/holamundo.html* correspondiente al servidor web que se muestra en el diagrama de red del presente ejercicio, cuyo contenido es el siguiente:

```
<!DOCTYPE html>
<html>
   <head>
      <title>Hola Mundo</title>
      <link href="/Estilos/MiApp.css" rel="stylesheet" type="text/css" />
   </head>
   <body>
      <h1> ¡Hola Mundo! </h1>
      <img src="/Imagenes/saludo.png" />
   </body>
</html>
```

De cada mensaje se debe indicar, al menos, las direcciones IP y MAC origen y destino, así como los protocolos de las distintas capas empleados y los números de puerto en el caso de protocolos de la capa de transporte. Considerar que el host tiene asignada de manera estática su configuración de red.

5.9 Indique cómo sería la secuencia de mensajes del caso anterior si el host tuviese que obtener su configuración por DHCP, tanto estando el servidor DHCP en la misma subred como en una subred diferente.

5.10 Indique cómo podría implementarse redundancia en la conexión a Internet a través de un ISP adicional. Tenga en cuenta tanto el tráfico saliente desde la red hacia Internet como el tráfico entrante desde Internet hacia los servidores internos.