



FIRMAT PER

Marta Chastel Mazarredo
Cap de l'àrea econòmic administratiu
28/9/2023

SEGUNDO EJERCICIO DE LA CONVOCATORIA 05/OPO2022 PARA CUBRIR UNA PLAZA DE TÉCNICO DE GESTIÓN INFORMÁTICA, SUBGRUPO A2.

SUPUESTO PRÁCTICO 1

RECORDATORIO: CADA SUPUESTO PRÁCTICO DE ESTE EJERCICIO ES TOTALMENTE INDEPENDIENTE DE LOS DEMÁS, POR LO QUE NO SE PUEDEN ASUMIR DATOS DE UN SUPUESTO PARA LA RESOLUCIÓN DE OTROS, AUNQUE HAYA INFORMACIONES QUE PAREZCAN SIMILARES O RELACIONADAS.

Planteamiento

La Sindicatura de Comptes está estudiando un cambio completo de su **sistema de virtualización**, ya que el actual no responde a las necesidades y el uso de servicios en la nube se reduce a unos pocos sistemas muy puntuales. Como técnico del departamento de sistemas y tecnologías de la información, se pide que plantee la arquitectura más adecuada para sustituir el sistema actual.

Los datos que se conocen para el diseño de la solución a plantear son los siguientes:

1. La Sindicatura ha categorizado sus sistemas como de nivel Medio del Esquema Nacional de Seguridad.
2. La política de aprovisionamiento de servicios y aplicaciones, dada la naturaleza de la información que trata la Sindicatura, es dar prioridad a los sistemas *on premise* (en local), salvo que no sea posible esa opción.
3. La Sindicatura dispone de servicios publicados en internet desde máquinas virtuales.
4. La máquinas virtuales alojadas actualmente tienen sistemas operativos Windows Server y diferentes versiones de Linux y UNIX.
5. El sistema actual de virtualización está compuesto por 3 nodos conectados por interfaz SAS a 2 cabinas de almacenamiento que no pueden servir otros protocolos ni ser ampliadas, y que ya no cuentan con soporte ni espacio para crecimiento alguno. Los nodos de virtualización tienen 4 años de antigüedad, disponen de 2 interfaces de red Ethernet a 1 GB y otros 2 a 10 GB. y están al 80% de utilización habitualmente. Se estima que, en los próximos 3 años, se incrementará la demanda





FIRMAT PER

María Chastel Mazarrero
Cap de l'àrea econòmic administratiu
28/9/2023

de recursos de las máquinas virtuales un 40%.

6. El sistema de virtualización a desplegar debe ubicarse repartido entre el Centro de Proceso de Datos (CPD) principal de la Sindicatura y su CPD de respaldo, en modo Activo-Pasivo.
7. El sistema de virtualización deberá disponer de funcionalidades de migración en caliente de máquinas virtuales entre nodos del mismo CPD.
8. Existe presupuesto únicamente para la adquisición de hardware de computación y de almacenamiento. Se dará por supuesto que el equipamiento de seguridad perimetral y redes se mantendrá.
9. La solución desplegada no puede incrementar el presupuesto de costes de mantenimiento que se abonaba anteriormente durante los años que dure la garantía y soporte del equipamiento nuevo a adquirir, lo cual descarta la contratación de módulos o servicios adicionales del software de virtualización.
10. Téngase en cuenta en las respuestas la eficiencia económica de la solución propuesta, y las posibilidades de reutilización de dispositivos.
11. No cite marcas comerciales para la definición de la solución que se pide, salvo en el caso de que así se le indique en la pregunta correspondiente. Responda sin entrar en especificidades de producto alguno.
12. En la Sindicatura se da prioridad a las soluciones de código abierto, a las soluciones disponibles en los repositorios de la Administración, y a las soluciones del Centro Criptológico Nacional.

Se pide

1. Especifique qué equipamiento se deberá adquirir como mínimo para desplegar el entorno de virtualización definido en el enunciado. Téngase en cuenta aspectos como la carga de computación, el quorum necesario, y la minimización de costes de licencias recurrentes, y no olvide indicar cuántos interfaces de red, de qué tipología, y para qué servicios, deberán disponer los equipos adquiridos.
2. Defina y justifique un mecanismo estandarizado para el uso del almacenamiento por parte de los nodos de virtualización, es decir, mediante qué protocolo(s) los diferentes nodos del sistema dispondrán de espacio de almacenamiento compartido, y cómo se arbitrará, en su caso, el acceso compartido a ese almacenamiento. Indique, además, si los dispositivos de almacenamiento propuestos en el punto 1 serán de tipo SAN, de tipo NAS o de tipo DAS.





FIRMAT PER

Marita Chastel Mazarredo
Cap de l'àrea econòmica administrativa
28/9/2023

3. Indique qué mecanismos de protección deberán poder implementarse en los dispositivos de almacenamiento para mejorar la tolerancia a fallos, de manera que puedan fallar dos discos de la cabina y el sistema siga funcionando (aunque de forma degradada).
4. Defina las diferentes VLAN que compartirán todos los elementos adquiridos, indicando la función de cada una de ellas y qué elementos se conectarán a las mismas.

Establezca las ventajas e inconvenientes que tendría la Sindicatura si se decanta por cada uno de los tres productos de virtualización siguientes: VMWare, HyperV y ProxmoxVE.





FIRMAT PER

Marta Chastel Mazarrredo
Cap de l'àrea econòmic administratiu
28/9/2023

SUPUESTO PRÁCTICO 2

Planteamiento

La Sindicatura de Comptes necesita elaborar un Plan de Continuidad de Servicios (o de Negocio, como se define en el sector privado), al que en adelante nos referiremos como PCS, para lo cual debe diseñar los componentes necesarios del mismo. Como técnico del servicio de sistemas y tecnologías de la información, se le pide colaboración para definir la parte del PCS que involucra al departamento. Para poder escribir el documento solicitado, se parte de la situación siguiente:

1. La Sindicatura ha categorizado sus sistemas como de nivel Medio del Esquema Nacional de Seguridad.
2. La Sindicatura dispone de un Centro de Proceso de Datos (CPD) propio en su sede, y de espacio reservado en el Centro de Proceso de Datos de la Generalitat Valenciana, donde se quiere establecer un CPD de respaldo. Dispone en ambos CPD de cortafuegos adecuadamente configurados.
3. La Sindicatura está conectada a Internet por una conexión independiente (WAN1), y por otro lado, está conectada a la Red Corporativa de la Generalitat Valenciana (WAN2), cuya latencia media es de 18 ms, aunque sus latencias varían entre los 12 y los 40 ms.
4. La gestión del enrutamiento de servicios y el DNS la realiza la propia Generalitat.
5. El 80% del personal de la Sindicatura teletrabaja un 80% del tiempo, a través del sistema de red privada virtual (VPN) establecido al efecto. Este servicio VPN se basa en el producto EMMA del Centro Criptológico Nacional, desplegado a partir de cinco máquinas virtuales. El acceso VPN se realiza a través del enlace de comunicaciones de Generalitat Valenciana.
6. La Sindicatura dispone, por tanto, de un entorno de virtualización, compuesto por seis (6) nodos idénticos. Es un producto que soporta la migración en caliente de máquinas virtuales, pero que es sensible a la falta de comunicación entre sus nodos, ya que en cuanto un nodo no responde al heartbeat durante 10 segundos, se le considera off line por el sistema y sus máquinas virtuales se reparten entre el resto de nodos. No es factible adquirir más nodos de virtualización, por limitaciones técnicas del sistema.
7. Ese sistema de virtualización dispone de un almacenamiento compartido entre sus nodos. Se trata de una cabina de discos capaz de realizar copias síncronas o asíncronas de volúmenes en otro dispositivo similar que disponga de la misma versión del sistema





FIRMAT PER

Marta Chastel Mazarredo
Cap de l'àrea econòmica administrativa
28/9/2023

operativo. La copia síncrona de volúmenes es muy exigente en lo que a la latencia entre los sistemas a sincronizar se refiere, con un requisito de latencia máxima de 7 ms.

8. Todas las máquinas virtuales pueden estar operativas, tras una parada completa, en un máximo de 15 minutos.
9. El sistema de virtualización está utilizado por debajo del 40% en la actualidad.
10. En CPD de respaldo actualmente sólo está desplegado el cortafuegos, conectado a la Red Corporativa de la Generalitat Valenciana como interfaz WAN.
11. Pese a disponer de un CPD de respaldo, seguirá siendo conveniente realizar copias de seguridad.

Se pide

1. Establezca la necesidad o no de la Sindicatura de disponer de medios alternativos de prestación de los servicios en base al cumplimiento del Esquema Nacional de Seguridad. Justifique adecuadamente su respuesta.
2. Defina la estructura del entorno de virtualización de manera que, aunque haga falta realizar tareas manuales, el tiempo máximo de parada de los servicios, en caso de indisponibilidad del CPD principal, sea de 45 minutos y la pérdida de información no sea superior a los 5 segundos. Indique los criterios de diseño utilizados.
3. Detalle el equipamiento que se ha de desplegar en el CPD de respaldo para dar soporte a los requisitos de disponibilidad y tiempo objetivo de recuperación.
4. Indique cuál sería el(los) procedimiento(s) técnicos, incluidos en los planes de recuperación ante desastres, a realizar de forma manual o automática para dejar el sistema funcional en el CPD de respaldo, y detalle los brevemente.
5. Especifique cómo se articularía el sistema de copias de seguridad para minimizar la ventana de backup, y cumplir con lo establecido en el Esquema Nacional de Seguridad y las buenas prácticas reconocidas al respecto.





FIRMAT PER

Marta Chastel Mazarrredo
Cap de l'àrea econòmic administratiu
28/9/2023

SUPUESTO PRÁCTICO 3

Planteamiento

La Sindicatura de Comptes tiene la necesidad de definir una nueva arquitectura de seguridad, ya que la actual ha sido auditada con pobres resultados recientemente. Como técnico del servicio de sistemas y tecnologías de la información, se le ha encargado participar en el diseño y las especificaciones del escenario de conectividad y seguridad perimetral.

Para ello, se dispone de la siguiente información previa:

1. La Sindicatura ha categorizado sus sistemas como de nivel Medio del Esquema Nacional de Seguridad.
2. La Sindicatura está conectada a Internet por una conexión independiente (WAN1, 1 Gbps simétrico), y por otro lado, su sede principal está conectada a la Red Corporativa de la Generalitat Valenciana (WAN2) con un enlace MacroLAN a 300 Mbps simétricos. No se pueden contratar más líneas ni ampliar capacidades.
3. La Sindicatura tiene unos 100 empleados, y unos 20 proveedores externos.
4. Un 80% del personal de la Sindicatura teletrabaja un 80% del tiempo, a través del sistema de red privada virtual (VPN) establecido al efecto a través de los cortafuegos existentes. También se conectan por VPN los técnicos de proveedores externos, con un máximo de dos cuentas VPN por proveedor.
5. La Sindicatura dispone de cuatro ubicaciones interconectadas a través de la Red Corporativa de la Generalitat. Salvo la principal, y la del CPD de respaldo, que ataca directamente a la red del CPD de la Generalitat, las otras dos son conexiones MacroLAN a 100 Mbps, ya que se corresponden con sedes 'tipo oficina' muy pequeñas. No se pueden contratar más líneas ni ampliar capacidades. Las dos sedes pequeñas se conectan a la sede principal, pero se han de poder conectar al CPD de respaldo en caso de caída del principal.
6. Los cortafuegos disponibles son antiguos, están fuera de vida útil, y sin soporte vigente. Actualmente, sólo la sede principal y el CPD de respaldo tienen cortafuegos, que se limitan a filtrar paquetes en capa 3 OSI.
7. Se establece un requisito de alta disponibilidad en el cortafuegos de la sede principal.
8. La segmentación de la red de la sede principal es correcta, y la electrónica de red





FIRMAT PER

María Chastel Mazarrado
Cap de l'àrea econòmic administratiu
28/9/2023

está renovada recientemente. Sin embargo, en las dos oficinas remotas no se ofrecen servicios wifi, y sería conveniente que estuvieran disponibles exactamente igual que en la sede principal.

9. Se busca que un PC o móvil corporativo que se conecte por Ethernet o de forma inalámbrica en cualquiera de las tres sedes tenga exactamente la misma configuración IP. En el CPD de respaldo está todo correcto.

10. En la sede principal y en las dos sedes 'tipo oficina' hay tanto PC, como móviles, como impresoras corporativas.

11. Ya se está tramitando el equipamiento inalámbrico necesario para que las sedes 'tipo oficina' tengan disponibilidad de servicios wifi.

12. Las VLAN disponibles en la red de la sede principal, y que afectan al supuesto práctico, son las siguientes:

1. LAN, para PC corporativos.
2. WifiCorp: para los interfaces inalámbricos de PC y móviles corporativos.
3. Guest: para equipos de invitados.
4. Server: para servidores.
5. Impresion: para impresoras.

13. En todas las sedes el único dispositivo capaz de enrutar el tráfico entre VLANs será el cortafuegos que se adquiera.

14. Todos los fabricantes de cortafuegos evaluados para su adquisición disponen de servicio de red privada virtual y de clientes adecuados para todas las plataformas de software de que dispone la Sindicatura. Se requiere que los clientes VPN permitan un sistema de doble factor de autenticación.

15. En la Sindicatura se da prioridad a las soluciones de código abierto, a las soluciones disponibles en los repositorios de la Administración, y a las soluciones del Centro Criptológico Nacional.

Se pide

1. Definición del equipamiento que habrá que adquirir para dar seguridad perimetral a las cuatro sedes de la Sindicatura, de forma económicamente eficiente, teniendo en cuenta la situación actual del mercado de ese tipo de productos, los niveles de protección





FIRMAT PER

Marta Chastel Mazarredo
Cap de l'àrea econòmica administrativa
28/9/2023

necesarios, y los parámetros indicados en el supuesto.

2. En base a su respuesta al apartado 1, defina qué servicios de seguridad se podrán tener en la nueva arquitectura de cortafuegos, que no se tuviesen anteriormente disponibles.
3. Explique de qué forma podrán prestarse exactamente los mismos servicios y con la misma configuración IP de los PC o terminales móviles, en las sedes remotas y en la sede principal.
4. Dibuje un esquema de la topología de la solución, indicando qué VLANs se dispondrán en cada sede y su justificación.
5. Evalúe, en función del coste y de otros parámetros indicados en el enunciado, para una Administración Pública española, las ventajas y desventajas de que el sistema de red privada virtual para teletrabajo sea proporcionado por el mismo fabricante que los cortafuegos o sea una solución separada (indíquela).

