Estudios

25 de enero de 2021

Índice

1. Tema 1: Infraestructura de los centros de datos.

¿Qué es un centro de datos?

Es un edificio o parte de un edificio destinado al almacenamiento de áreas de computación y sus zonas de soporte.

¿Qué significa que un centro de datos sea *single−tenant*?

Significa que solo tiene un propietario. Que es de carácter privado.

¿Qué significa que un centro de datos sea *multi−tenant*?

Significa que suele estar bajo la administración de empresas de telecomunicación o de proveedores de servicios, los cuales ofrecen bajo demanda su tecnología a terceros.

¿Cómo se estructuran?

Se estructuran en forma de doble estrella o copito de nieve. Se dividen en diferentes zonas: *Entrance Room*, *Main Distribution Area*, *Horizontal Distribution Area*, *Equipment Distribution Area*, *Telecommunications Room*.

¿De que se encarga un *MDA*?

En un MDA se suele encontrar el sistema de enrutamiento y conmutación principal, que además también sirve como *backbone* para la conexión con el ISP.

¿De que se encarga un *HDA*?

Un HDA o *Horizontal Distribution Area* consiste en la distribución de la red a los *EDAs*, además del almacenamiento SAN/NAS que pudiera haber.

¿Qué es un *ZDA*?

Un *Zone Distribution Area* complementa a un *HDA* y distribuye la red horizontalmente a un *EDA*. Ejemplo: switch común a varios racks.

¿En que consiste un *EDA*?

Distribuye el tráfico a los equipos finales. Ejemplo: switch local que da servicio a un solo rack.

¿Que es un *TR*?

Un *Telecommunications room* es el punto de control de un centro de datos. En los centros de datos privados sirve como zona de entrada para el tráfico de la organización.

Explica los diferentes niveles de redundancia definidos en `TIA-942`.

N — sin redundancia, no soporta ni fallos ni paradas.

N+1 — se cuenta con un equipo extra a mayores de los necesarios. Soporta el fallo/parada/mantenimiento de un solo equipo sin afectar a la disponibilidad.

2N — se cuenta con el doble de equipos de los necesarios. Soporta el fallo/parado/mantenimiento de *N* equipos.

2(N+1) — se cuenta con el doble de equipos de los necesarios más uno. Ante el fallo completo del sistema, aún quedaría una redundancia del tipo *N+1*. Soporta el fallo/parada/mantenimiento de un equipo además de un posible fallo/parada/mantenimiento de los equipos necesarios.

Explica las diferentes clasificaciones en TIERS definidas en la norma `TIA-942`.

TIER	Redundancia	Susceptible a	Líneas de corriente	Grupos electrógenos	Conexiones WAN	Desc.
1	N	Fallos / Mantenimiento	1	NO SIMPLES	1	
2	N+1 «parcial»	Fallos / Mantenimiento	1	Redundancia	1	Fuentes de alimentación redundantes.
3	N+1	Fallos	1+ (solo una al menos activa)	Redundancia	1+ Distintos proveedores, se necesita dos ER distintos.	
4	2(N+1)	Catástrofes	1+	Redundancia	1+	

2. Tema 2: RAID

2.1. RAID 0

- No tiene redundancia $\Rightarrow$ no tolera fallos.
- Capacidad efectiva: N * tamaño del disco más pequeño.

2.2. RAID 1

- Tiene redundancia ⇒ tolera fallos de N-1 discos.
- Capacidad efectiva: tamaño del disco más pequeño.

2.3. RAID 5

- Mínimo 3 discos
- Capacidad efectiva: (N-1) * tamaño de disco más pequeño.

3. Tema 3: Redes

3.1. ¿Qué es un firewall?

Un componente tanto hardware como software que se encarga de controlar el acceso a la red. Tiene como un objetivo principal impedir los ataques externos al interior de la red, y también monitorizar y controlar las conexiones internas al exterior.

3.2. ¿Cuáles son las limitaciones de un firewall?

Los firewall normalmente son un punto único de fallo, pues suele encontrarse solo uno entre la red externa y la interna. Además, no protege de las amenazas internas. También puede dar una sensación falsa de seguridad, pero las amenazas en la red constan de muchos aspectos.

3.3. ¿Qué diferentes filtros firewall hay? Explica cada uno.

Existen tres diferentes tipos de filtros firewall: filtro de paquetes, filtro de paquetes con estado, y filtro a nivel de aplicación.

En el filtrado de paquetes solo se tiene en cuenta la información de las capas 1-4 incluídas, es decir no se trata (por lo general) la capa de aplicación. Se suele leer las

cabeceras IP y también las de capa de transporte y con esa información decidir que hacer con el paquete. Los filtros de paquetes con estado se podría decir que tienen «memoria» y estudian paquetes de inicio y fin de conexión, y además pueden llegar a reconocer a que conexión pertenece un paquete.

Los filtros a nivel de aplicación ya conocen los protocolos de capa 5 TCP/IP que pasan por ellos. Así, pueden hacer un análisis más riguroso por ejemplo para vetar acceso a páginas web basado en el texto o palabras clave que pueda haber. Además, por lo general si no conoce el protocolo de capa de aplicación, como no cuenta con el «proxy» para ese protocolo ni siquiera deja pasar los paquetes.

3.4. ¿En que consiste una regla por defecto en un firewall?

La mayoría de los firewalls aplican una serie de reglas para decidir si un paquete pasa o no a través de él. Existen dos técnicas principales para el control del paso: aceptar por defecto (blacklisting) y denegar por defecto (whitelisting).

Aceptar por defecto significa que si un paquete no es detectado por las reglas como una «amenaza» se deja pasar. Esto está relacionado con el término blacklisting porque se puede entender que si cumple una regla que aparece en el archivo de «blacklist» significa que hay que parar el paquete.

Denegar por defecto significa que si un paquete no es detectado por las reglas como un paquete «benigno» se considerará una amenaza y no se dejará pasar. Esta relacionado con el término whitelisting porque se puede entender que si cumple una regla que aparece en la «whitelist» se deja pasar y en caso contrario no.

3.5. Ventajas e inconvenientes de los diferentes tipos de filtrado de paquetes.

Los filtros con estado o de paquetes tienen un buen rendimiento, pues tiene pocas dificultades en tomar las decisiones. Son transparentes para el usuario. Son simples. Pero tienen un mayor margen de error o falta de eficacia, pues la información que disponen para tomar las decisiones es limitada.

Los filtros a nivel de aplicación consiguen una mejor separación entre la red interna y la red externa. Evita comunicación directa con el servidor destino. Se tiene un mayor control para cada aplicación pues ahora se puede decidir en base a cada protocolo de aplicación. Permite tener registros (logs) a alto nivel, y también reducir tráfico con uso de cachés. Sus limitaciones son variadas: para los usuarios no es transparente la implantación de un firewall proxy, además, para cada tipo de protocolo de aplicación aceptado hará falta un firewall proxy diferente. Menor rendimiento que el filtrado de paquetes pues ahora las reglas pueden ser mucho más complejas.

Filtro a nivel de circuitos. Un híbrido entre un filtro de paquetes y uno de aplicación. No maneja contenidos de capa de aplicación, pero las conexiones no se hacen directamente interno-externo, si no que son interno - firewall,firewall - externo.

3.6. Ventajas e inconvenientes de topología *dual homed host*.

En una topología *dual homed host* se tiene un único host dedicado entre la red interna y la red externa. Sus ventajas son una mayor facilidad de gestión, un menor coste. Sus desventajas son las guisantes: un único punto de fallo, cualquier vulnerabilidad del SO o firewall de ese host nos pone en riesgo.

3.7. Ventajas e inconvenientes de topología *screened host o host bastion*.

En una topología *screened host* se tiene un único host visible a la red externa, tras un firewall. Sus ventajas son una mayor facilidad de gestión, un menor coste. Sus desventajas son las guisantes: un único punto de fallo, cualquier vulnerabilidad o ataque al *screened host* pone en riesgo a toda la red, pues ya esta detrás del firewall y no hay mucho que pueda hacer.

3.8. Explica la topología *untrusted host*.

El host con los servicios públicos se encuentra fuera de la red protegida. El firewall no tiene control sobre él. La configuración es delicada.

3.9. Explica la topología *DMZ*.

La topología DMZ cuenta con tres redes diferentes: la publica, la interna y protegida, y la zona desmilitarizada. Todas ellas interconectadas por un único firewall con tres interfaces. Los equipos de la DMZ no se pueden conectar a los de la red privada. La DMZ define una red de servicios públicos. Normalmente, se puede encontrar los servicios proxy en la DMZ.

3.10. Explica la topología *DMZ con doble firewall*.

En esta topología se cuenta con un firewall de acceso público que se conecta solamente con la red dmz, y uno en la red dmz que solo se conecta con la red interna y protegida.

```
RED PÚBLICA - F1 - DMZ - F2 - RED PRIVADA
```

Esto permite una doble protección a los equipos que se encuentran en la red privada, al tener que atravesar dos firewalls. Si se compromete un equipo de la DMZ la red privada sigue protegida. Como inconvenientes tiene una mayor complejidad de gestión al tener que configurar dos firewalls.

3.11. Por ahora no hay VPNs. Sorry!

4. Tema 4: Clusters, Balanceo de carga, alta disponibilidad, computación de altas prestaciones.

4.1. ¿Qué es un balanceador de carga?

Es un host que se encarga de distribuir la carga de procesamiento entre varios hosts. De tal forma que se maximice el número de peticiones.

Objetivo: atender el máximo número de peticiones.

4.2. ¿Qué es un cluster de alta disponibilidad?

Es un conjunto de nodos que intenta garantizar el acceso a un servicio, ya sea mediante la tolerancia a fallos o caída de algún elemento.

Objetivo: dar la máxima prestación de un servicio. Estar el mayor tiempo disponible o accesible.

4.3. ¿Qué es un cluster de alto rendimiento?

Es un conjunto de nodos que busca llevar a cabo una tarea de la forma más rápida posible. Ya sea mediante técnicas de procesamiento en paralelo y/o distribuído.

Objetivo: Maximizar el rendimiento y la potencia de cálculo.