Almacenamiento en Centros de datos

- DAS: Direct Atachment Storage
- SAN: Storage Area Network: Todo el conjunto de la red de almacenamiento: cabinas de discos duros, switches, tarjetas de red…. Almacenamiento por bloque, un servidor le pide a una cabina un bloque de datos, como si fuera un disco duro. Un disco de un SAN se ve como un disco duro
- NAS: Network Atached Storage: Es similar al SAN, pero funciona con direccionamiento a nivel de fichero. Cuando se trabaja con un NAS se le pide un fichero o un directorio.
- Hiperconvergencia: Se crean cabinas virtuales con discos duros introducidos en las máquinas.

Conceptos de almacenamiento

- Capacidad: Capacidad de un disco
- IOPS: Rendimiento de un disco (Cantidad de operaciones de entrada y salida que puede hacer un disco)
- Latencia: Asociada a las IOPS, cuanto tarda en responder el disco.
- Protocolos de acceso: SCSI, FC, SATA, SAS, NVMe
- Raids:
    - RAID 0: Divide datos entre discos
    - RAID 1: Mirroring, copia los datos en 2 o mas discos
    - RAID 5: Se distribuyen los datos y una paridad puesta en otro discos a mayores. De esta forma si falla un disco se puede recuperar la paridad
    - RAID 6: Realiza 2 copias de paridad, como el RAID 5 pero puede recuperarse del fallo de dos discos.
    - Spare: Disco duro que queda a la espera sin datos para reconstruir los datos en caso de que falle un RAID 5 o 6, lo malo es que hace un cuello de botella.
    - Spare Distribuido: Se tiene un espacio en cada disco a la espera de que falle un disco para usar dicho espacio para reconstruir los datos del raid.
- Cabina de discos duros: hardware dedicado a almacenamiento de datos compartido. Busca la protección absoluta de los datos.
    - Entrega de servicio: Como funcionan las controladoras
        - Activo activo: Todas las controladoras entregan datos de forma simultánea (Nivel empresarial)
        - Activo Pasivo: Solo una controladora da servicio, cuando falla entra otra en servicio.
        - Alua: Sistema simétrico, son activo activo, pero hay una preferencia, una controladora funciona de forma más optima que la otra.
    - Control de acceso con multifactor (Ahora se enjaulan de forma que solo se pueden gestionar en físico)
    - AIRGAP: Máquina que hace un backup y se desconecta de la red al finalizar
    - Cifrado de datos
    - Auditoría de accesos.
    - Rendimiento en base a caché de lectura y escritura
    - Distribuir los datos entre los discos para prevenir cuellos de botella provocados por los discos (Wide Stripping)
    - Protección contra pérdidas de datos.
    - Copias de seguridad automatizadas y réplicas
    - Ahorro de almacenamiento
        - Thin provisioning: Se le asigna a un usuario una cierta capacidad, pero en realidad

        solo se usan los datos que se consumen en el momento.
        - Compresión
        - Desduplicación: Se eliminan ficheros duplicados.
- LUN: Logical Unit Number
    - Es un trozode espacio de la totalidad del almacenamiento de una cabina.
    - Suele estar dividido entre la mayor cantidad de discos posibles para mejorar el rendimiento.
    - Tiene un identificador que lo identifica en los servicores

DAS

Direct Atached Storage, un disco duro conectado directamente. El problema de estos era la pérdida de espacio, problemas de rendimiento tiene las siguientes características:

- Bajo coste
- Simple
- Descentralizado
- Bajo rendimiento
- Escalabilidad limitada

SAN

Toda la red de almacenamiento, conformada por las cabinas, los switches y las tarjetas de conectividad (HBA: Host Bus Adapter, pueden ser tarjetas de red normales, normalmente HBA se usa en FC). Los protocolos más stándar son:

- Fiber Channel (FC): usan Fabrics (Switches de fibra)
- iSCSI: Usan ethernet normal y corriente

El FC va a 32Gbps y el iSCSI va a entre 100Gbps y 400Gbps. El san se diferencia del NAS en que en el NAS pides ficheros y en el SAN Bloques.

Conceptos importantes: Los Fabrics funcionan al revés que los Switches Ethernet, por defecto cuando se conecta algo no se conecta, necesita que se permita la conectividad.

- Zonning: Se establecen zonas a las que hay que dar permiso para realizar la conexión (Por ejemplo: permito la conectividad entre puerto 4 y Puerto 8). También existe en zonning lógico. Las HBA usan WWN (World Wide Number), que son su equivalente a la MAC. En el zonning lógico se puede conectar un WWN a otro WWN.
- LUN Masking: Para que un host sea capaz de usar un disco de una cabina hay que crear un zonning donde se indica que ciertas HBA tienen acceso a dicha cabina. Se tendrá acceso a las LUN que sean indicadas en el LUN Masking.
- Multipathing: Cada uno de los host está conectado a todos los switches y lo mismo con las tarjetas de red y HBA.

iSCSI funciona igual que canal de fibra pero con TCP/IP, usando identificadores iqn o eui.

NAS

Normalmente usan protocolo NFS (network File System) para compartir el almacenamiento de las cabinas. Este sistema funciona con almacenamiento de ficheros. A los clientes se les entrega una carpeta de ficheros y estos lo montan en su equipo. Generalmente se considera que es mejor SAN que NAS a nivel de CPD. Esto se debe a que tradicionalmente el entorno NAS tiene un rendimiento más bajo ya que ethernet era muy lento en comparación con fiber channel (16G vs 1G). El protocolo de compartición NFS es más lento que Fiber Channel. Generalmente el NAS es como un almacenamiento de segunda línea mientras que en el SAN está lo importante. En la actualidad el rendimiento es mejor al haber de 10G a 100G.

Hiperconvergencia

Una cabina de almacenamiento se considera algo caro y que, en el pasado, eran el cuello de botella del CPD. La cabina de discos duros se diseñó en los 90 y con el tiempo se le fueron añadiendo funcionalidades. La hiperconvergencia consiste en meter los disco de vuelta a los servidores (DAS) pero cambiando algunas cosas, se le pone una capa software por encima al disco y se crea una cabina de almacenamiento virtual. Para ello se usan los discos que están en los servidores. En caso de VMWARE a esto se le llama vSAN. Las ventajas de la hiperconvergencia frente a los SAN es que en teoría es más barato (En la práctica sale lo mismo por las licencias), en cuanto a rendimiento, tiene un buen rendimiento, siempre y cuando no lo comparemos con una cabina de unidades NVMe. En cuanto a la administración y operación, la hiperconvergencia facilita la gestión. Generalmente se usa la implementación de VMWare ya que es la que está mejor implementada. Existe la hiperconvergencia híbrica entre disco duro y unidad de estado sólido, pero es considerablemente peor.

La hiperconvergencia tiene las siguientes características importantes:

- Tecnología de 2014-2015 que trae conceptos que no traen las cabinas. Un Stretch cluster es un cluster que está distribuido entre dos CPD, lo que permite tener redundancia de CPD, hacer esto con cabinas de discos es extremadamente complejo y caro. La hiperconvergencia ya está preparada desde su creación para crear un stretch cluster, que soporta latencias mayores y permite la creación de “Metro Clusters” a cientos de kilómetros de distancia. La hiperconvergencia se centra en la virtualización, mientras que las cabinas se centran en los discos.
- Dominios de Error: cada servidor es un dominio de error. Una máquina virtual va a distribuir los datos, por ejemplo, entre 5 servidores, si se quiere proteger con un RAID 5 o 6 se van a dividir los datos entre los diferentes servidores que hay, de forma que si falla uno se mantenga el servicio. Si montamos un stretch cluster donde se ponen 6 servidores separados en 2 CPD y se quiere proteger una máquina con RAID 5 en multisite, se distribuyen los datos de la máquina en los servidores de ambos CPD, de forma que aunque caiga un CPD completo se mantenga el servicio.

Seguridad en el almacenamiento

Se quiere proteger los datos contra:

- Borrrado accidental
- Fallos o errores de hardware
- Desastres
- Ransomware

Se pueden proteger los datos para cada equipo dependiendo del caso:

- DAS: Se puede proteger la disponibilidad con RAIDs en cada uno de los servidores
    - Controladoras RAID
        - EVITAR RAID por SOFTWARE
        - Las controladoras suelen tener una caché que proporciona un mayor rendimiento. Se recomienda tener una batería para la cache de la controladora.
        - Cifrado de datos: Algunas controladoras cifran los datos.
    - Monitorizar la salud de los discos
    - Clonación de disco duro
- SAN
    - Controlar el Zonning de HBA en FC y los ACL de los Switches en iSCSI
    - Control de acceso a la cabina
        - LUN Masking
        - Permisos de lectura y escritura
    - Redundancia de comunicaciones
    - CHAP en iSCSI: Challenge handshake Authentication Protocol. Se usa para validar la identidad de los dispositivos.
        - Unidireccional: Se configura una Password en una LUN en una cabina y los clientes deben proporcionarla para conectar a esta.
        - Bidireccional: Se configura una Password para la LUN y otro para el CLiente, de forma que ambas partes deben tener sus contraseñas para poder realizar la conexión.
- NAS:
    - NFSv3:
        - se usa Auth_Sys siempre, el dueño de todo es root. En NFSv4 se puede usar el Active Directoyr
        - Se recomienda desactivar NFSv3.
        - Se usa kerberos para la autenticación y cifrado (Kerberos 5 y Kerberos 5p)
    - SMB:
        - Tiene cifrado extremo a extremo con AES
        - Integridad de datos SHA-256
        - Se usa Kerberos
        - Soporta clusters dentro de la propia definición del protocolo.
    - Hiperconvergencia:
        - Alta disponibilidad: un dato seguiráposible aunque falle:
            - Un disco
            - Un grupo de discos
            - Un Nodo
            - Una partición de red
            - El vCenter
        - Soporta cifrado tanto en tránsito como en reposo (AES-256)
        - Soporta 2-Way authentication (como CHAP bidireccional)
        - PowerCLI permite borrado seguro de datos según el estándar NIST.