Especificaciones técnicas para la arquitectura tecnológica en la nube

Breve descripción:

Este componente formativo brinda los conocimientos para definir especificaciones técnicas de acuerdo con los requerimientos de la arquitectura tecnológica de la organización, en donde se abarcan los aspectos tecnológicos necesarios para la apropiación y gestión de servicios en la nube.

Noviembre 2023

Tabla de contenido

Introducción

Le damos la bienvenida al componente formativo **Especificaciones técnicas para la arquitectura tecnológica en nube**. Para comenzar el recorrido por el mismo, se sugiere explorar el siguiente recurso audiovisual en el que se explica, de forma genérica, cada una de las temáticas que se desarrollarán.

Video 1. Especificaciones técnicas para la arquitectura tecnológica en nube

Enlace de reproducción del video

Síntesis del video: Especificaciones técnicas para la arquitectura tecnológica en la nube
Dentro de un proyecto de servicios en la nube, es de vital importancia realizar las especificaciones técnicas de acuerdo con los requerimientos de la arquitectura tecnológica de la organización, en donde se abarquen los aspectos tecnológicos necesarios para determinar los sistemas operativos y servicios base requeridos, así

como para establecer la capacidad de procesamiento, almacenamiento y conectividad requerida.

El presente componente ofrece varios temas, iniciando por el servicio de directorio, que permite almacenar y administrar información de usuarios, computadoras, impresoras aplicaciones y otros objetos de la red de forma centralizada y segura. Es necesario conocer los conceptos básicos en relación a su interacción, almacenaje de información y requerimiento de componentes.

Además, encontrará información respecto a **Active Directory**, se encuentra una distribución lógica que permitirá una mejor interacción de elementos como el árbol, el bosque y la unidad organizativa.

En **Active Directory** el bosque ("forest") es una colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración. Todos los dominios del bosque cuentan con relaciones de confianza automáticas de 2 vías y transitivas. El bosque representa una instancia completa del directorio y una frontera de seguridad.

Por otra parte, la virtualización presente también en las especificaciones técnicas, permite mejorar la agilidad, la flexibilidad y la escalabilidad de la infraestructura de TI, al mismo tiempo que proporciona un importante ahorro de costes.

Otras ventajas de la virtualización, es la mayor movilidad de las cargas de trabajo, el aumento del rendimiento y de la disponibilidad de los recursos o la

automatización de las operaciones; simplifican la gestión de la infraestructura de TI y permiten reducir los costes de propiedad y operativos.

Y por último los contenedores, en especial de trabajo realizado con **Docker**, permite establecer regulación en la información contenida, mejor definición de imagen, uso de comandos, etc. Para lo que se accede a la guía facilitada por el Ministerio de Tecnologías de la información y de las comunicaciones; elementos que están a su alcance para consulta en el componente formativo que va a desarrollar.

1. Servicios de directorio

Active Directory, o también conocido como Directorio Activo (AD), es una herramienta, propiedad de Microsoft, que brinda servicios de directorio en una red LAN. Microsoft es el gigante tecnológico del "software", proveedor de los sistemas operativos Windows, "software" ofimático MS Office, entre otros servicios en la nube.

A continuación, se presenta información en detalle de Active Directory:

a. El directorio activo tiene la capacidad de proporcionar un servicio ubicado en uno o varios servidores con capacidad de crear y orquestar objetos como usuarios, equipos o grupos, de tal manera que se pueda gestionar credenciales de inicio de sesión de los equipos conectados en una red.

b. El directorio activo permite administrar diversas políticas o reglas para los grupos de trabajo y equipos, en toda la red corporativa, para la cual se haya determinado el control de dominio al servidor de directorio.

c. Está orientada al uso profesional, en entornos de trabajo con importantes recursos informáticos, en donde es necesario administrar gran cantidad de equipos en cuanto a actualizaciones o instalación de programas o la creación de archivos centralizados para poder acceder a los recursos de forma remota desde las estaciones de trabajo.

Lo anterior ratifica que la implementación de Active Directory es la forma ideal de centralizar muchos de los componentes típicos de una red LAN sin necesidad de ir equipo por equipo y evitando que los usuarios puedan hacer lo que quieran en una red.

1.1. Conceptos de dominio

Un controlador de dominio, también conocido como directorio activo (Active Directory en inglés), cumple la función principal de agrupar varios ordenadores en una misma red, a lo que se conoce como dominio; el controlador de dominio es capaz de orquestar reglas o políticas para cada dominio que se tenga.

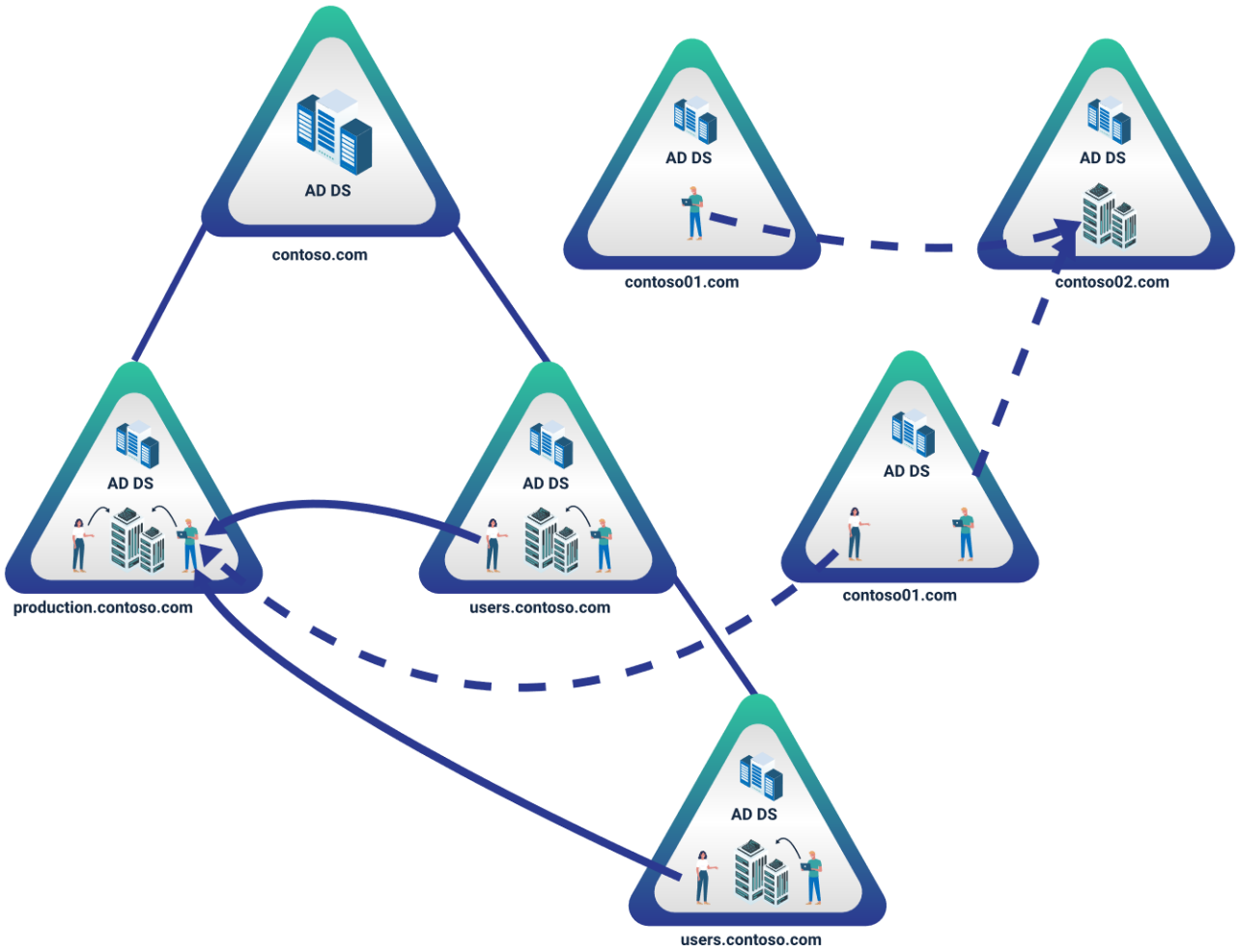
El dominio dentro de Active Directory consiste en varios ordenadores conectados a una red, los cuales cuentan con un equipo servidor para administrar las cuentas de usuario y credenciales de la red. Los dominios no necesariamente tienen que estar en contacto unos con otros; por ejemplo, un dominio (A) tiene acceso a otros dos dominios (B y C), esto no implica que C tenga acceso a B.

Entonces, cuando se hace referencia a Active Directory también se debe entender como controlador de dominio, en donde se pueden crear distintos dominios y gestionar permisos e interacción en cada uno de ellos. A esta relación entre dominios se le denomina relación de confianza o "trust".

1.2. Estructura física y lógica

Los servicios de directorio se pueden presentar en una red, la cual puede estar compuesta por una estructura física y lógica. Físicamente, los servicios se sirven sobre una topología de red que interconecta los "hosts" u ordenadores. La estructura lógica, por otro lado, es la parte fundamental en los servicios de directorio, desde allí se organizan diversas reglas para los dominios. La gestión de dichas reglas tiene un esquema en el Active Directory compuesto en árboles y bosques, que se distribuye como se muestra a continuación:

Figura 1. Bosque en Active Directory



a. **Unidad organizativa**. Una Unidad Organizacional (OU) es un objeto contenedor que se usa para organizar objetos (como cuentas de usuario, grupos, equipos, impresoras y otras OU´s.) dentro de un dominio. Las OU proveen un mecanismo sencillo para agrupar usuarios y es la unidad más pequeña a la que se le pueden asignar configuraciones de políticas de grupo. (SANS Institute, 2003)

b. **Árbol**. Consiste en uno o varios dominios, organizados jerárquicamente y que dependen de una raíz común, a esto se le conoce como DNS común. De esta

manera se pueden diferenciar o identificar un dominio de otro. Por ejemplo, un dominio **midominio.local** puede tener un subdominio que compone dicho árbol, entonces podría tener otro subdominio así **works.midominio.local**, y si se tiene otro dominio de nombre otro **otrodominio.local**, es fácil identificar que son árboles diferentes con respecto al anterior.

c. **Bosque**. Un bosque se compone de todos los dominios existentes, dentro del servidor de dominio. Se crean relaciones de confianza transitivas o intransitivas que están construidas automáticamente por el directorio activo para cada dominio, las cuales pueden ser modificadas posteriormente.

En cuanto al árbol, es necesario tener en cuenta que, a través de éste, el directorio activo puede ser dividido o segmentado en partes para optimizar la gestión de recursos, así entonces, un usuario perteneciente a un dominio también puede ser reconocido por los subdominios que pertenezcan al dominio principal.

Unidad organizativa, árbol y bosque

Un bosque contiene varios árboles de dominio con nombres diferentes. También, un bosque cuenta por lo menos con un dominio raíz, de tal manera que cuando se instala o configura el primer dominio se crea automáticamente la raíz de un árbol y por encima, la raíz de un bosque.

1.3. Cuentas

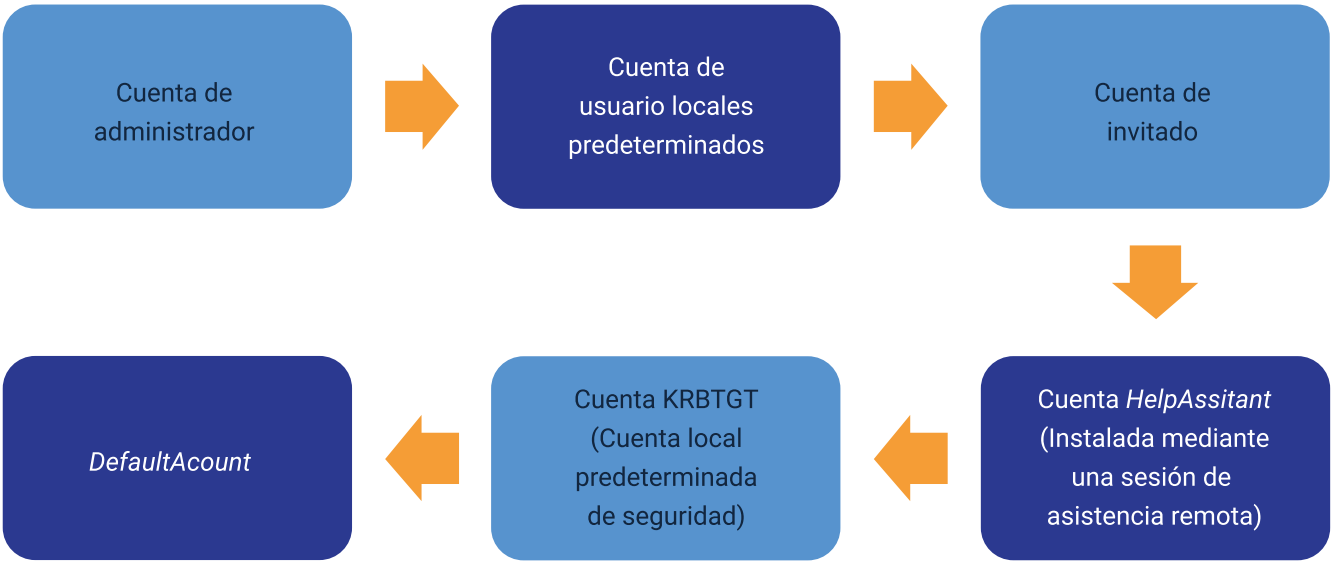
Dentro de los servicios de directorio, las cuentas hacen referencia a los usuarios digitales a los cuales se les brindará o no el acceso a servicios, sistemas, aplicaciones y funcionalidades dentro de un dominio, y son almacenadas localmente en el servidor de

dominio. A las cuentas se les pueden asignar derechos y permisos en un servidor determinado, pero solo en ese servidor.

Las cuentas de usuario también sirven para tener mayor control en los servicios y aplicaciones, pues se pueden considerar como entidades de seguridad que se utilizan para proteger y administrar el acceso a los recursos en un servidor independiente o miembro para servicios o usuarios.

Las cuentas de usuario se pueden agrupar de la siguiente manera:

Figura 2. Cuentas de usuario



Administración de cuentas

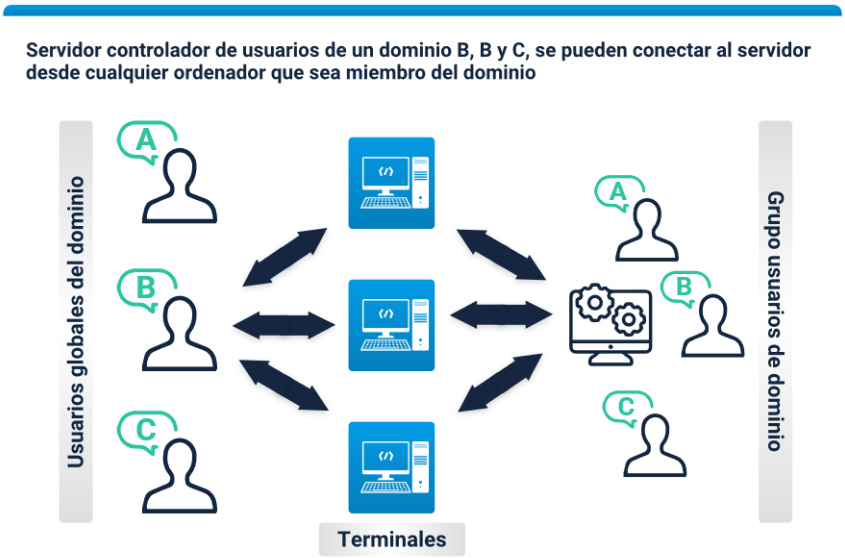
Cuando se instala el servidor de dominio y se configura el dominio, se instalan las cuentas locales predeterminadas, estas cuentas se guardan en el contenedor Usuarios en Usuarios y Equipos de Active Directory. Las cuentas locales predeterminadas se pueden crear, deshabilitar, restablecer y eliminar con la consola de administración de

Microsoft (MMC) de Usuarios y equipos de Active Directory y con herramientas de línea de comandos.

A continuación, se amplía la información sobre la administración de cuentas.

a. **Asignación de permisos**. Para asignar derechos y permisos a un controlador de dominio local determinado se puede utilizar las funciones disponibles en usuarios y equipos de Active Directory.
b. **Derecho**. Un derecho autoriza a un usuario a realizar determinadas acciones en un equipo, como hacer una copia de seguridad de archivos y carpetas o apagar un equipo.
c. **Permiso**. Un permiso de acceso es una regla asociada a un objeto, normalmente un archivo, una carpeta o una impresora, que regula qué usuarios pueden tener acceso al objeto y de qué manera.

   La administración de cuentas de usuario a través del servidor de dominio es importante, ya que desde allí se pueden brindar los derechos y permisos de acceso a los recursos como parte de la gestión de accesos.



Seguridad en las cuentas y los accesos

Es importante que se protejan las cuentas de dominio, para lo cual se debe restringir y limitar estrictamente la pertenencia a los grupos administradores, administradores de dominio y "Enterprise Admins", así como controlar de manera rigurosa dónde y cómo se usan las cuentas de dominio.

Estas son algunas de las medidas de seguridad para las cuentas y accesos:

- Separar las cuentas de administrador de las de usuarios.
- Para los administradores crear "hosts" de estación de trabajo dedicados.
- Restringir el inicio de sesión de administrador a servidores y estaciones de trabajo bajo control para quienes tienen derecho de uso, por medio de contraseñas seguras y cuando sea aplicable con doble factor de autenticación.
- Para cuentas de administrador deshabilitar el derecho de delegación de cuenta.

1.4. Directorios y objetos en general

Dentro del controlador de dominio o Active Directory, un objeto es la representación general que se utiliza para referirse a cualquier elemento del directorio sobre el cual se aplican reglas y atributos. Los objetos se pueden agrupar así:

a. **Usuario**. Consiste en las credenciales de acceso a estaciones de trabajo, aplicaciones o servicios.
b. **Recursos**. Son los elementos a los que los usuarios pueden acceder según los derechos de acceso asignados, estos elementos pueden ser carpetas en red, impresoras, entre otros relacionados.

c. **Servicios**. Consiste en las funcionalidades en red a las que el usuario puede acceder de acuerdo con los derechos de acceso otorgados, entre los cuales pueden ser correo, aplicaciones, sistemas de información, entre otros.

1.5. Políticas del dominio

Las políticas de dominio, también llamadas de políticas de grupo o reglas del active directory, consisten en las reglas para el control de acceso a recursos y servicios para los usuarios. De toda la gama de políticas de grupo, existen algunas que denotan mayor relevancia por su importancia en la seguridad digital, y que se deben seguir como buenas prácticas en la implementación de dominio, ya sea local o en la nube: a continuación, se describen algunas de estas:

a. **Configuraciones de servicios y seguridad por defecto**. Active directory es muy popular, esto hace que muchos delincuentes informáticos conozcan las configuraciones de los servicios y seguridad por defecto, aumentando la facilidad de acceso a los sistemas de las organizaciones. Por esto es importante que se revisen todas las funcionalidades y configuraciones del controlador de dominio que vienen por defecto, con el fin de desactivar los servicios y aplicar reglas de seguridad que sean mejores.
b. **Cuentas de acceso privilegiado**. La gestión de cuentas utiliza cuentas con acceso privilegiado para que se puedan administrar las funcionalidades del directorio activo, pero considerando el factor humano como uno de los vectores de ataque más vulnerables. Se debe evitar dar acceso privilegiado a demasiadas cuentas, ya que aumenta el riesgo de que los “hackers” utilicen ataques de ingeniería social y roben alguna de estas cuentas con accesos

privilegiados. Así entonces, se debe elegir con rigurosidad las cuentas que en verdad necesiten acceso privilegiado.

c. **Contraseñas seguras**. El uso de contraseñas es uno de los principales factores de seguridad de los usuarios para el acceso seguro a los recursos en la red (aplicaciones, servicios, etc.), por eso se deben aplicar políticas en el directorio activo para obligar a los usuarios a utilizar contraseñas robustas.
d. **Acceso remoto**. Se deben crear las políticas para asegurar el acceso remoto seguro de usuarios a los servidores y "hosts" que requieran permitirse este tipo de conexiones.
e. **Caducidad de contraseñas**. Se deben configurar las políticas para que las contraseñas sean cambiadas periódicamente, por lo general se da un tiempo de caducidad de 90 días.
f. **Registro de eventos**. Es importante activar el registro de eventos para aquellos componentes que sean vitales de revisar en caso de que se presenten sucesos adversos.

Introducción a AD DS

Se recomienda seguir la guía rápida de Microsoft que se encuentra en el material complementario y que también puede ser consultada a través del siguiente enlace. Allí se puede profundizar más sobre el directorio activo, los servicios de dominio y sus políticas: https://learn.microsoft.com/en-us/training/modules/introduction-to-ad-ds/

Las siguientes son algunas generalidades que usted debe tener en cuenta, en relación con directorio activo, servicios de dominio y políticas:

a. **Relaciones de confianza**. Existen entre dos dominios / bosques de Active Directory la relación de confianza, que consiste en un vínculo de confianza el cual permite a los usuarios autenticados acceder a los recursos de otro dominio.

   Las relaciones de confianza pueden ser:

   - Transitivo.
   - Bidireccional.
   - Unidireccional.

b. **Replicación de objetos**. Active Directory puede ser replicado por medio del método de transferir y actualizar objetos del controlador de dominio a otro controlador de dominio, por ejemplo, se podría replicar un controlador de dominio local a uno en la nube.

   Algo fundamental para la correcta replicación de objetos son las conexiones entre los controladores de dominios, ya que se apropian con base en la ubicación de los dominios dentro de un bosque. Los dominios deben estar conectados por medio de una o más subredes, de esta manera estarán en segmentos de red por medio de intervalo de direcciones IP asociadas al dominio. Cuando se asigna el direccionamiento IP de un controlador de dominio a una subred, Active Directory reconoce los controladores de dominio que se encuentran asociados a los dominios. Las conexiones de los dominios o sitios son configuradas de manera que se interconecten para garantizar la replicación de los objetos de Active Directory de los dominios.

c. **Redundancia**. La redundancia en servicios de directorio o en Active Directory, consiste en una estrategia para garantizar la disponibilidad del controlador de dominio, por medio de la agregación de controladores de dominio adicionales

alternos a un dominio, mejorando las solicitudes de autenticación y búsquedas en el servidor del catálogo global. También ayuda a que los servicios de dominio de Active Directory resuelvan problemas o errores de "hardware", "software" o del administrador ("SysAdmin").

Una de las opciones para la redundancia es realizar **configuración de redundancia geográfica con Replicación de "SQL Server"**, como lo sugiere Microsoft en su portal. La compañía asegura lo siguiente: "Si usa "SQL Server" como base de datos de configuración de AD FS ("Active Directory Federation Services"), puede configurar la redundancia geográfica para la granja de servidores AD FS mediante "SQL Server" replicación. La redundancia geográfica replica los datos entre dos sitios geográficamente lejanos para que las aplicaciones puedan cambiar de un sitio a otro. De este modo, en caso de error de un sitio, todavía puede tener todos los datos de configuración disponibles en el segundo sitio." Microsoft (2021)

Otras formas de replicación involucran la instalación y configuración de servidores de controladores de dominio en sitios o nubes alternas.

2. “Software” de virtualización

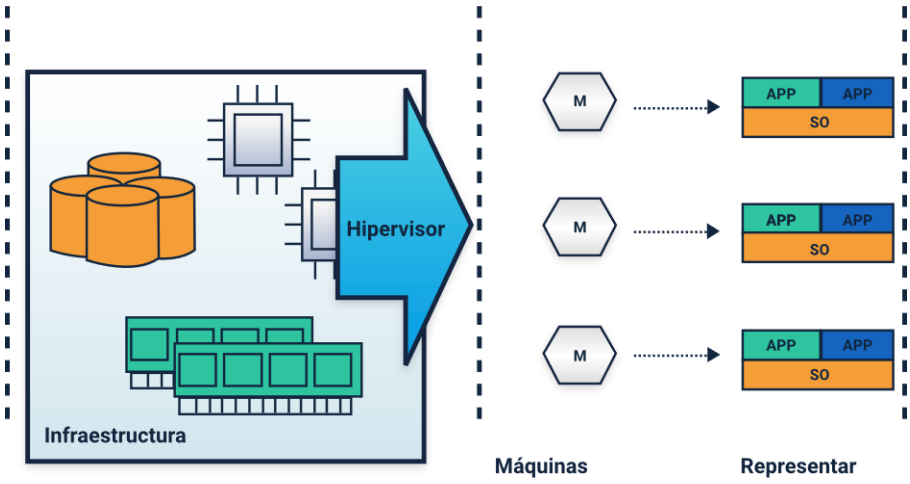
La virtualización es un tema base, sobre el que se fundamenta la computación en la nube y los sistemas actuales de despliegue de aplicaciones y servicios en la nube.

Es necesario conocer las generalidades de la virtualización, los diferentes tipos que existen y cuáles son más comunes en el uso de acuerdo con sus características. Son varias las herramientas para realizar un proceso de virtualización de servidores y virtualización de un sistema operativo Linux corriendo en una máquina Windows:

- Microsoft
- Linux
- Ubuntu

La virtualización es el proceso mediante el cual es posible crear una representación de elementos físicos como servidores, sistemas de almacenamiento, redes e, incluso, aplicaciones mediante “software” de modo que se puedan reducir los costos asociados a infraestructura de TI, al tiempo que se mejora la eficiencia en el uso de estos recursos (VMware, 2011).

Figura 3. Esquema de virtualización



2.1. Generalidades de la virtualización

Normalmente un conjunto de recursos de infraestructura, como discos, memorias, procesadores, etc., que están presentes en un equipo o grupo de servidores, son ocupados únicamente por el sistema operativo y las aplicaciones que se ejecutan sobre este; dichos recursos no siempre usan todo su potencial al 100 %, lo que provoca desperdicios. Con la virtualización, se puede hacer que estos recursos ejecuten una o varias máquinas virtuales al mismo tiempo y cada una de estas máquinas podrá ejecutar su propio conjunto de aplicaciones con sistemas operativos totalmente independientes.

Una máquina virtual (MV) es un "software" especial que funciona como un contenedor de "software" donde se incluye un sistema operativo y aplicaciones que funcionan totalmente independientes. De esta forma un equipo puede tener instaladas varias máquinas virtuales, cada una de las cuales se ejecutan independientemente en un mismo equipo que sirve como "host".

Ventajas al implementar esquemas de virtualización

a. **Aumento de rendimiento**. Se puede asignar más o menos recursos dinámicamente a una máquina dependiendo de la utilidad real requerida.
b. **Automatización de operaciones**. Reducción en la inversión de capital y gastos operativos asociados a la infraestructura de TI. Reducción de tiempos de inactividad de los recursos.

Tipos de virtualización

Existen varias formas de virtualizar, pero el común denominador de la virtualización es el aprovechamiento de los recursos de "hardware" y "software"

para que estos puedan ser utilizados de forma flexible por parte de los usuarios o clientes. A continuación, se describen los tipos de virtualización.

Virtualización de servidores

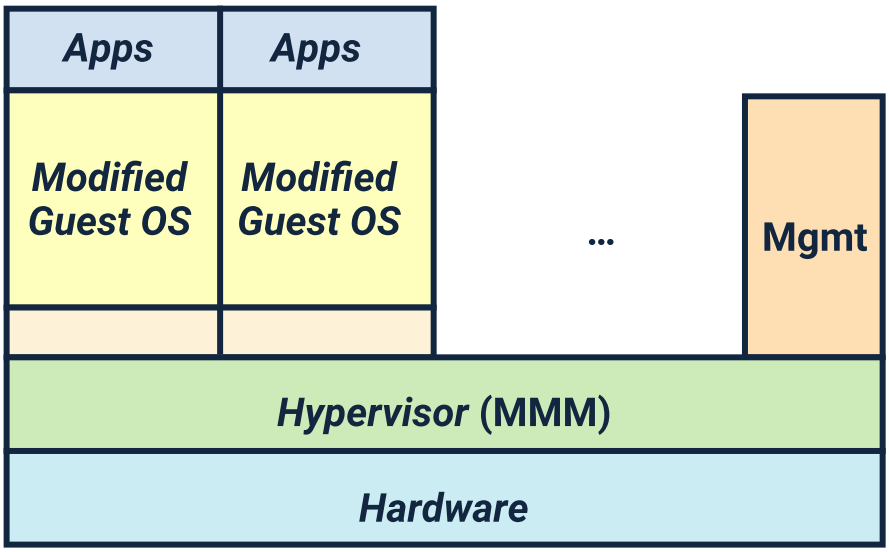
Este tipo de virtualización tiene ventajas clave:

- Mayor disponibilidad de los servidores.
- Reducción en costes operativos.
- Eliminación de la complejidad de los servidores.
- Mejora en el rendimiento de las aplicaciones.
- Distribución más rápida de las cargas de trabajo.

La virtualización de servidores es una implementación en la que un servidor físico ("host") se divide mediante "software" en varios servidores virtuales únicos y aislados, los cuales se visualizan al cliente como servidores independientes.

Se clasifica en dos tipos, estos son:

a. **Virtualización completa**. En este tipo de virtualización se usa el hipervisor, el cual es un "software" que se encarga de la supervisión y gestión de los recursos físicos y adicionalmente se encarga de independizar cada servidor virtual. Sin embargo, el hipervisor requiere recursos para hacer el procesamiento correspondiente, lo que puede afectar el rendimiento general del servidor.



b. **Paravirtualización**. En este esquema, cada sistema operativo de los servidores virtuales tiene conocimiento de la existencia de los otros, por lo cual el hipervisor se libera un poco de la carga para gestionar los sistemas operativos. Adicionalmente, se tienen ventajas como la posibilidad de crear copias de seguridad más fácilmente, migraciones más rápidas, mejor utilización del sistema y ahorro de energía. No todos los sistemas operativos soportan paravirtualización y, en algunos casos, se pueden presentar problemas de compatibilidad de "hardware".

Virtualización a nivel de sistema operativo o basada en contenedores

Es este esquema de virtualización no se usa Hipervisor, sino que es el sistema operativo del servidor físico quien se encarga de las actividades de virtualización, sin embargo, en este esquema los servidores virtuales deben ejecutar el mismo sistema operativo del "host".

Virtualización de red

Consisten en crear redes virtuales independientes y separadas mediante el uso de "software" sobre redes físicas. Este tipo de virtualización se puede presentar de dos maneras:

a. **Virtualización externa**. La cual consiste en la combinación de varias redes completas o partes en una unidad virtual.
b. **Virtualización interna**. La cual hace uso de contenedores de "software" para proveer la funcionalidad de una unidad de red física. Algunos ejemplos de aplicaciones y enfoque de virtualización de red son: VPN, VLAN, SDN.

Virtualización de escritorios

Estas máquinas de escritorio virtuales se entregan a los usuarios de forma remota a través de una red pública o privada, los usuarios no necesitan descargar la máquina virtual.

a. Empleada por muchas empresas en la actualidad y también se conoce como VDI por su sigla en inglés (infraestructura de escritorios virtuales). En este esquema se dispone de un conjunto de servidores o data centers, los cuales publican varias páginas virtuales, cada una con su propio sistema operativo, aplicaciones y servicios con su propio entorno de escritorio.
b. La máquina virtual se ejecuta en los servidores y no en el equipo del usuario. Es decir, la carga de procesamiento, almacenamiento y demás capacidades de gestión desde el servidor remoto.
c. Reciben la imagen de sus escritorios desde los servidores de forma remota.

Herramientas de virtualización de servidores

En el mercado existen muchas herramientas de "software" creadas para facilitar el proceso de virtualización de servidores. A continuación, se listan algunas de estas herramientas para entornos domésticos y pequeñas empresas junto con cada una de sus características principales.

Listado de herramientas para virtualización de servidores

a. **VMware**.

- Gran cantidad de paquetes de software disponibles para virtualización.
- Tiene soluciones libres y de pago.
- Compatibilidad con la tecnología Intel VT-x, la cual le permite ejecutar máquinas virtuales en forma nativa de la "CPU host" cuando esta tiene procesadores Intel.

  Es el hipervisor de escritorio estándar de la industria para ejecutar máquinas virtuales en PC con Linux o Windows. En el enlace se podrá descargar una prueba gratuita y completamente funcional de 30 días: https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

b. **Oracle VM VirtualBox**.

- "Software" gratuito descargable desde su sitio web oficial.
- Posibilidad de instalar máquinas Linux, MacOS y Windows en la gran mayoría de versiones de forma gratuita.
- Soporta virtualización en tecnologías Intel y AMD.

En el enlace se encuentran los vínculos a los binarios de VirtualBox y su código fuente: https://docs.docker.com/desktop/install/windows-install/

c. **Microsoft Hyper-V**.

- Disponible en forma nativa en S.O Windows en versión pro y "server". Es decir, si se tiene este tipo de versiones estará disponible de forma gratuita y no requiere de instalación de "software" externo al sistema.
- Sirve para virtualizar sistemas Windows y otros como Linux y FreeBSD.
- Soporta virtualización en tecnologías Intel y AMD.

  En este enlace se puede obtener el código fuente de los últimos lanzamientos para compilarlos. Las instrucciones detalladas para ello se pueden encontrar en la "wiki" para Linux, Win32 y macOS.
  https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v

d. **Qemu**.

- Es un "software" libre y está disponible para diferentes tipos de sistemas operativos.
- No dispone de GUI, pero se puede instalar mediante una extensión para en Mac y en Windows.
- Soporta virtualización en tecnologías Intel y AMD

  Obtenga el código fuente de los últimos lanzamientos y compílelo usted mismo. Las instrucciones detalladas de compilación se pueden encontrar en la "wiki" para Linux, Win32 y macOS.
  https://www.qemu.org/download/

e. **Parallels**.

- Hypervisor para sistemas operativos MacOS
- Permite ejecutar máquinas virtuales de otros sistemas sobre la plataforma de Apple.
- Compatibilidad con la tecnología Intel VT-x.
- Permite traspaso de archivos, carpetas compartidas y comunicación de todo tipo de dispositivos de E/S entre la máquina "host" y las virtuales.
- Se debe pagar licencia para su uso.

  Una aplicación rápida, sencilla y potente para ejecutar Windows en Mac Intel o Apple M1, todo sin reiniciar. Incluye más de 30 herramientas de un solo toque para simplificar las tareas diarias en Mac y Windows.

  https://www.parallels.com/

Ejemplo de virtualización

A continuación, se podrá consultar un ejemplo, paso a paso, de cómo realizar un proceso de virtualización de una máquina con sistema operativo Linux, en una máquina con sistema operativo Windows. Para este ejemplo, se utilizará una máquina "host" con sistema operativo Windows 10 Home de 64 "bits" y se virtualizará y ejecutará una máquina virtual con sistema operativo Ubuntu desktop 20.04, por medio de la herramienta Oracle Virtual Box.

Consulte la información contenida en el video que se muestra enseguida y amplíe sus conocimientos y habilidades en lo relacionado con la instalación de VirtualBox:

Video 2. Instalación de VirtualBox

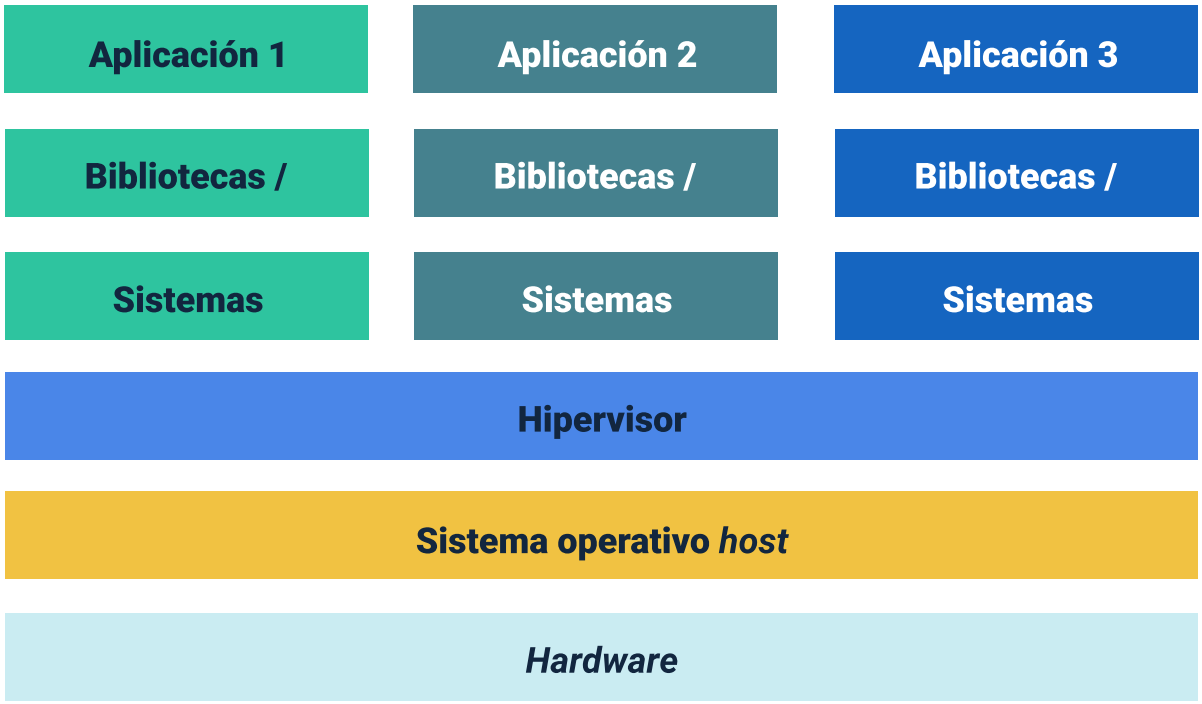
Enlace de reproducción del video

Síntesis del video: Instalación de VirtualBox
En este video se ofrecen, de manera detallada, los pasos, condiciones y requerimientos para ejecutar el proceso de instalación de VirtualBox. Además, se ofrecen algunas recomendaciones claves para su uso y provecho.

2.2. Máquinas virtuales

Las máquinas virtuales son un sistema operativo completo funcionando de manera aislada dentro de otro sistema operativo anfitrión (Alarcón, 2018). De igual manera debe existir un componente de infraestructura de tipo “hardware” que soporte todo lo anterior que, en últimas, es el servidor o equipo donde se haga el desarrollo y creación de la máquina virtual o, si se trata del despliegue y puesta en producción final de la aplicación, puede referirse a un proveedor que suministra el “hardware” necesario que soportará la máquina virtual como Azure, Google Cloud, AWS, Digital Ocean, entre otras, como lo muestra la siguiente imagen:

Figura 4. Funcionamiento de una Máquina virtual



2.3. Características de la virtualización

Existen ventajas que son características del proceso de virtualización, permitiendo de esta forma obtener mejores y mayores recursos, sistemas de soporte, la migración de datos e información, así como una alta disponibilidad de los recursos. A continuación, se ofrece una breve descripción de estas:

a. **Almacenamiento**. Es la agrupación de todos los recursos de almacenamiento lógico y físico, de tal forma que la gestión de dispositivos de almacenamiento en red se simplifica al reunirlos en un único almacén que es administrado desde un lugar central. Las necesidades de almacenamiento pueden variar mucho de una empresa a otra, ya que algunas requieren perdurabilidad de los

sistemas, otras precisan lidiar con distintos dispositivos, potencia en la nube, etc.

Gestionar distintos dispositivos de almacenamiento puede resultar una tarea muy compleja, pero la virtualización del almacenamiento ha llegado para poner solución a este problema.

b. **Redundancia**. Vamos a imaginar que queremos crear un sistema disponible el 99,99 % del tiempo, bien porque es un servicio vital para la empresa, bien porque cualquier pérdida o corte, puede provocar pérdidas económicas o de cualquier otro tipo. ¿Qué hacemos entonces?

   Se suele configurar lo que se denomina un «sistema redundante», es decir dos o más sistemas configurados de forma que uno de ellos sea el que está en funcionamiento y, en el caso en que deje de funcionar por cualquier motivo, se active otro de los sistemas que hasta ese momento estaba «en espera» o «inactivo», tan rápidamente como sea posible. Mediante este sistema, incluso en el peor de los casos (la rotura de un disco duro, un desbordamiento de memoria que mate un proceso vital o, incluso, que alguien le pegue una patada al cable) puede seguir funcionando gracias al siguiente equipo hasta entonces «dormido».

c. **Migración**. Describe el proceso de mover una máquina virtual de un "host" a otro. Esto es posible porque los invitados están corriendo en un entorno virtualizado en lugar de directamente sobre el "hardware". Hay dos maneras de migrar una máquina virtual: en vivo y fuera de línea.

   - Migración fuera de línea: una migración fuera de línea suspende al invitado y después mueve una imagen de la memoria del invitado al "host" destino. El invitado es posteriormente puesto en marcha sobre

el “host” destino y la memoria usada por el invitado en la “host” fuente liberada.

- Migración en vivo: la migración en vivo es el proceso de migrar un invitado activo de un “host” físico a otro.

d. Alta disponibilidad. Hasta hace poco, las redes y los sistemas de la tecnología de la información (IT) y la tecnología de operaciones (OT) funcionaban de manera completamente independiente entre sí. Sin embargo, desde hace unos años, a medida que la fabricación industrial ha aumentado su nivel de conexión, también han ido convergiendo en la planta los mundos de la IT y la OT de nuevas y trascendentales maneras.

La digitalización de la fabricación implica enviar y recibir una gran cantidad de datos desde numerosos orígenes y puntos de datos diferentes. Las aplicaciones y paquetes de “software” encargados de conectar estos puntos de datos requieren más capacidad de computación de la que jamás habían necesitado. Las empresas industriales están comenzando a cambiar de soluciones físicas de “hardware” a ambientes virtuales donde pueden residir varias aplicaciones y sistemas operativos.

Virtualización, ¿para qué sirve?

La virtualización esencialmente elimina la dependencia entre el sistema operativo y el “hardware” físico. Ha sido una implementación más habitual en plantas y líneas de nuevo diseño, en las que es posible comenzar desde cero con un ambiente virtual.

Las plantas de mayor tamaño también han comenzado a cambiar a servidores virtuales, gracias a los grandes centros de datos. Sea cual sea el tamaño de su planta, la planta conectada es el futuro de la fabricación y la virtualización desempeñará un papel

cada vez más importante en el espacio de la OT. La tendencia de migración a servidores permite, ahora, trasladar servidores virtuales de una máquina física a otra y se encuentra aún en sus primeras fases.

3. Contestadores

Una vez revisados los conceptos y características del servicio de directorio y la virtualización, es tiempo de profundizar en los modelos de virtualización a nivel de sistema operativo en el que se desarrollarán varios ejercicios como introducción a la plataforma Docker, la cual es ampliamente utilizada por la industria de desarrollo de "software".

Al finalizar este componente formativo el aprendiz estará en la capacidad de crear imágenes de Docker, construir y ejecutar contenedores Docker a partir de imágenes locales, modificar contenedores locales, transformar un contenedor editada a una imagen y compartir una imagen local en el repositorio en la nube Docker Hub.

3.1. Contenedores de "software"

El término de contenedores se ha vuelto muy común en la jerga actual asociada a la administración de servicios de infraestructura, pero en esencia hace referencia a un modelo de virtualización repasado en el componente anterior, específicamente la virtualización a nivel de sistema operativo.

En este modelo los contenedores no son más que máquinas virtuales aisladas entre sí, con un "software" específico que no tiene un sistema operativo propio, sino que comparte los recursos y el "kernel" del sistema operativo de la máquina anfitriona o "host", logrando un mejor rendimiento ya que solo existe un sistema operativo encargado de la gestión de la infraestructura en la máquina anfitriona o "host". López (2018)

Los contenedores encapsulan únicamente el "software" específico de la aplicación que se ejecuta dentro de él, junto con las librerías de las cuales depende

para su ejecución, abstrayendo el servidor en el que se va a ejecutar; logrando, entonces, una portabilidad real, ya que es posible predecir el comportamiento de un "software" cuando este se mueve desde un servidor a otro.

Ventajas

a. **Disminución de gastos**. Requieren menos recursos del sistema comparado con sistema de virtualización tradicionales.
b. **Mayor portabilidad**. Se pueden implementar fácilmente en diferentes plataformas y sistemas operativos.
c. **Funcionamiento coherente**. Siempre se ejecutan de la misma manera independientemente del lugar donde se implementen.
d. **Mayor eficiencia**. Permiten la implementación de modificaciones y/o escalamiento de funcionalidades con mayor rapidez.
e. **Mejor desarrollo de aplicaciones**. Este modelo de virtualización se alinea perfectamente con las metodologías ágiles y enfoques de DevOps de la industria actual para acelerar el proceso de construcción de "software".

Mayor uso

- Migración y/o refactorización de aplicaciones existentes a entornos más modernos.
- Aplicaciones distribuidas y arquitecturas de microservicios.
- Implementación de prácticas de integración y despliegue continuo.

3.2. Hipervisor vs contenedores

Hay similitudes y diferencias entre la forma en cómo estas dos tecnologías facilitan el proceso de virtualización de aplicaciones, razón por la cual es más

conveniente una u otra dependiendo del contexto particular y las necesidades establecidas por la organización.

En ambos casos se requiere de una máquina "host" que contendrá la infraestructura física con todos los dispositivos y recursos necesarios, sobre los cuales se monta un sistema operativo que puede ser de cualquier tipo. Luego, sobre este sistema operativo se monta un "software", que en el caso esquema de máquinas virtuales tradicionales será un hipervisor y en el esquema de contenedores será un gestor de contenedores.

En las máquinas virtuales, para poder ejecutar una aplicación específica; se requiere de librerías, códigos binarios y del montaje de un sistema operativo invitado. Así, por ejemplo, si la aplicación a ejecutar en la máquina virtual fue construida con Visual Studio Net, es necesario también montar en la máquina virtual el sistema operativo Windows; ahora bien, si la aplicación a ejecutar en la máquina virtual fue construida en Swift, requiere entonces la instalación del sistema operativo MacOS, y así sucesivamente. En todas las máquinas virtuales se debe correr el sistema operativo completo de acuerdo con las "App" a utilizar.

En el caso de las tecnologías de contenedores, estos se construyen exclusivamente con las aplicaciones, librerías y archivos binarios a ser utilizados y compartirán recursos con el sistema operativo anfitrión o máquina "host".

3.3. Docker

Docker es una de las plataformas de "**software**" más ampliamente utilizada en el mundo para la gestión de contenedores.

Para realizar el proceso de instalación de Docker en el sistema operativo Windows, hay que dirigirse directamente a la página oficial de Docker disponible en: https://docs.docker.com/desktop/install/windows-install/

En el enlace anterior se encuentra el acceso directo al proceso de descarga y también una descripción de los requerimientos específicos respecto a versiones del sistema operativo, memoria RAM mínima, procesadores compatibles, entre otros.

En el siguiente video se presentan las características de Docker:

Video 3. Docker

Enlace de reproducción del video

Síntesis del video: Docker
Docker Hub es un servicio proporcionado por la compañía Docker Inc donde se puede almacenar, compartir y extraer imágenes para crear contenedores de Docker;

este servicio requiere la creación de una cuenta de usuario y funciona muy similar a como lo hacen los repositorios de archivos en la nube.

Comandos de Docker: hay varios comandos de Docker que debe conocer cuando trabaje con Docker. Podemos ver algunos de los comandos más utilizados en el proceso de gestión de imágenes y contenedores usando la plataforma Docker.

- docker ps: muestra todos los contenedores en ejecución
- docker ps -a: muestra todos los contenedores en ejecución y detenidos
- docker start: inicia un contenedor
- docker stop: detiene un contenedor
- docker attach: se conecta a un contenedor que está en ejecución
- docker run: crea y ejecuta un contenedor.
- docker rm: elimina un contenedor
- docker images: muestra todas las imágenes
- docker build: crea una imagen de un tarball
- docker search: busca imágenes disponibles en Docker Hub para reutilización

Definición de imagen. Una imagen es una especie de plantilla que usa el motor de Docker para la construcción de un contenedor. Es un archivo del sistema privado solo para contenedores y provee todos los archivos y códigos que el contenedor necesita.

"**Containers**". Los contenedores de Docker pueden considerarse como la instancia donde se implementa todo lo descrito en una imagen de Docker, es decir, un contenedor se construye a partir de una imagen. Si se tuviera que hacer un paralelo

con sistemas de virtualización con hipervisores, una imagen sería el equivalente a lo que representaría un archivo ISO y un contenedor sería el equivalente a una máquina virtual.

"**Dockerfile**". Es un archivo de texto simple con un conjunto de comandos o instrucciones. Estos comandos / instrucciones se ejecutan sucesivamente para realizar acciones en la imagen base para crear una nueva imagen de la ventana acoplable: comentarios y comandos + argumentos.

Los comandos más usados son:

- "**From**": le indica la imagen inicial a descargar y a partir de la cual se espera montar el contenedor a construir. Esta sentencia es obligatoria ya que todos los contenedores se construyen de imágenes.
- **"Maintainer"**: nombre de la persona que está creando el archivo.
- **"Run"**: ejecución de comandos específicos sobre la imagen descargada en el "From".
- "**Expose**": apertura de puertos en el contenedor.
- **CMD**: fija un comando o proceso que se ejecutará cada vez que se ejecute un contenedor desde la nueva imagen.

Revise el siguiente enlace para chequear información detallada sobre la documentación de referencias de Doker y archivos Dockerfile: https://docs.docker.com/engine/reference/builder/

Chequee también el siguiente enlace y estudie, de manera precisa la documentación de Dockerfile para Windows: https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-docker/manage-windows-dockerfile

4. Almacenamiento

Un asunto indispensable para la construcción de una solución de virtualización es el almacenamiento. De hecho, es una de las decisiones más importantes a tener en cuenta, ya que los entornos no son iguales debido a su tipo de requerimiento y finalidad.

Por mucho tiempo la solución más utilizada ha sido Fibre Channel (FC) y, en los últimos años, han sobresalido tecnologías como NAS o iSCSI, convirtiéndose en alternativas tentadoras para entornos de virtualización, gracias a su diferencia en rendimiento y precio.

4.1. Generalidades

Hay que tener ciertos criterios a la hora de elegir una solución como son: presupuesto disponible, rendimiento y capacidad. Además, hay fabricantes que ya cuentan con una propuesta en virtualización, que se pueden adoptar en el proyecto que se esté proponiendo, como una alternativa para trabajar con la misma línea.

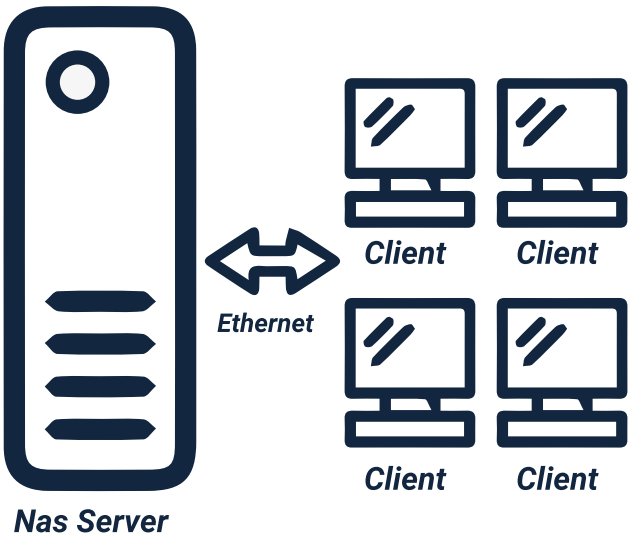
Normalmente, en el campo de la virtualización se encuentran tecnologías como FC, que es de las más reconocidas. Sin embargo, no se debe pasar por alto iSCSI o NAS como alternativas. Estas últimas tienen un abanico de dispositivos iSCSI o NAS en el mercado, con características como capacidades, escalabilidad y ver que nuestro requerimiento sea compensado. Por eso, se precisa que en este momento del proyecto el almacenamiento es una parte crítica para ello.

4.2. Tipos de almacenamiento

Existen diferencias en los tipos de almacenamiento de datos. A continuación, se desarrollará aquello de carácter principal, de acuerdo a las especificaciones técnicas para la arquitectura en nube:

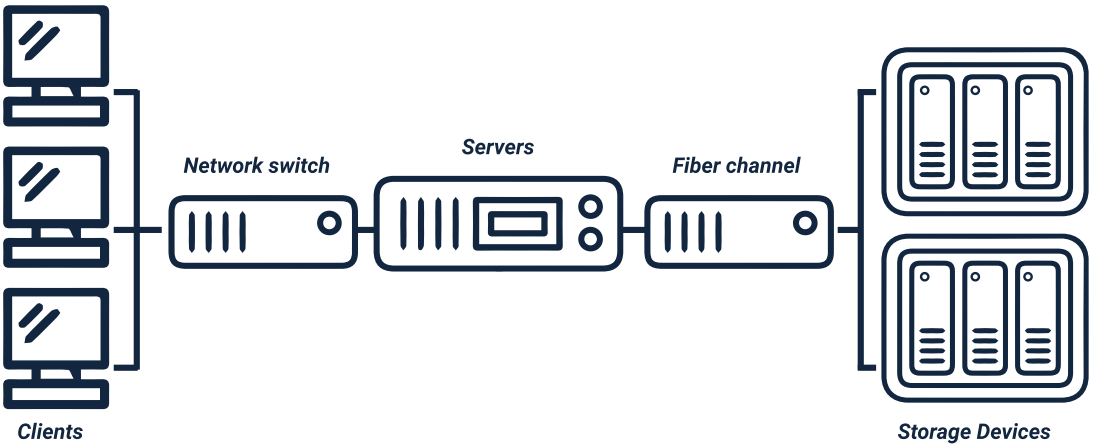
a. **"DAS Direct Attached Storage"**. Son dispositivos de almacenamiento directamente conectados a la máquina, como es el caso de discos duros internos, cabinas de disco o unidades de cinta para "backup".
   Suelen basarse en tecnologías SCSI- "Small Computers System Interface" y FC- "Fiber Channel". Esta arquitectura de almacenamiento se relacionaba principalmente con la época de los "Mainframe" de IBM. Sin embargo, hoy en día, los PC's de sobremesa utilizan arquitectura de almacenamiento DAS, mientras que, en los servidores de las empresas, empieza a caer en desuso, utilizándose únicamente para el almacenamiento del sistema operativo.
   La arquitectura de almacenamiento DAS presenta muchos inconvenientes, como la dispersión del almacenamiento, que implica una dificultad en la gestión de los "backups", así como una baja tolerancia a fallos (sólo posible a través de soluciones RAID), y un alto TCO- "Total Cost of Ownership", debido a las dificultades de mantenimiento.

b. **“NAS Network Attached Storage”**. Con la introducción de las redes locales (LAN), se empezaron a utilizar servidores de almacenamiento conectados a la red, a los cuales se podía acceder directamente a través de la propia infraestructura mediante protocolos específicos como NFS –“Network File System”, en entornos UNIX y CIFS –“Common Internet File System”, en entornos Microsoft (antes conocido como SMB, protocolo original de IBM que fue mejorado por Microsoft en CIFS) o incluso mediante FTP, HTTP, etc. Los principales beneficios de las Arquitecturas de Almacenamiento NAS son los que proporcionan un mejor TCO –“Total Cost of Ownship”, resultando fácilmente escalable y capaces de ofrecer una alta disponibilidad. Actualmente, las soluciones NAS se basan en TCP/IP, con protocolos NFS o CIFS por encima. En consecuencia, un dispositivo NAS será una máquina dedicada con una o varias direcciones IP y además estará dotado de una conexión de alta velocidad a la red LAN. De esta forma, los equipos clientes, en una arquitectura de almacenamiento NAS, delegan la gestión del sistema de ficheros al propio dispositivo NAS, que se limita a montar las unidades de red exportadas o compartidas. Es así que los usuarios y aplicaciones utilizan estos sistemas de ficheros como si fueran locales, aunque para el sistema operativo se trate claramente de sistemas de ficheros remotos.



c. **"**SAN Storage Area Network**"**. Esta arquitectura implica disponer de una infraestructura de red de alta velocidad dedicada sólo para almacenamiento y "backup", optimizada para mover grandes cantidades de datos y consistente en múltiples recursos de almacenamiento geográficamente distribuidos o no, además de otros elementos (cables, "switches" de fibra FC, "routers", adaptadores HBA, etc.).

Las redes de almacenamiento SAN han facilitado enormemente la creación de Centros de Procesos de Datos (CDP) distribuidos, "Clusters" Geográficos, creación de centros de respaldo (BDC), etc.



4.3. Tecnologías de almacenamiento

Las principales tecnologías de almacenamiento se relacionan con los protocolos de uso, componentes y costos. A continuación, se describen las principales.

"iSCSI - Internet Small Computer System Interface"

Sistema de almacenamiento basado en bloques como FC – "Fiber Channel". Se diferencia porque utiliza componentes de una red "Ethernet" tradicional para realizar la conexión entre los "hosts" y el sistema de almacenamiento. Al utilizar componentes "Ethernet", iSCSI es más barato de implementar.

- iSCSI utiliza los llamados iniciadores ("initiator") para enviar comando iSCSI a los dispositivos de almacenamiento. Estos iniciadores pueden ser basados en "software" o "hardware". En la mayoría de las situaciones, los iniciadores "software" pueden ser suficientes, una solución "hardware" ofrece un mejor rendimiento en E/S utilizando menos recursos del "host". Hay que tener en cuenta que una solución "software" introduce un "overhead" de CPU en el "host" que se conecta a la red de almacenamiento.
- iSCSI da un buen rendimiento en redes de 1Gbps (más si utilizamos "multipathing"), pero actualmente se pueden construir redes iSCSI de 10 Gbps que ofrecen un rendimiento parecido e incluso mejor que FC. El problema de las redes de 10 Gbps es que son tan caras de implementar como una red FC.
- En cuanto a seguridad, a diferencia de FC, iSCSI implementa sistemas de autenticación (CHAP) y encriptación.

“FC - Fiber channel”

FC presenta un grado alto de rendimiento y fiabilidad, pero implica realizar una inversión económica mayor e introduce complejidad en la configuración del centro de datos. FC es la solución más utilizada para entornos de virtualización de gran dimensión o máquinas virtuales con IOPS (número de E/S de acceso a disco) gracias a los anchos de banda que se alcanzan (8 Gpbs e incluso 16 Gbps).

Seguridad

Las redes de almacenamiento basadas en FC, en principio, son más seguras que las basadas en “Ethernet” ya que el tráfico está aislado del tráfico normal. Pero por otro lado es más complicado implementar sistemas de autenticación y encriptación.

Costos

La necesidad de disponer de “hardware” propio para la tecnología (HBAs y “switches” FC), hacen la solución más cara y compleja de administrar e implementar. Puede darse el caso de que la empresa no disponga de personal con conocimientos en entornos FC, por lo tanto, se puede incurrir en costes adicionales de formación o consultoría externa.

“NAS - Network Attached Storage”

a. **Protocolo de uso**. La principal diferencia entre iSCSI y NAS es el tipo de protocolo utilizado. Mientras que iSCSI está basado en bloques de discos, NAS es un sistema de compartición de archivos.

De este modo, se descarga al dispositivo de almacenamiento de la responsabilidad de escribir datos a disco. NAS utiliza un "software" cliente que se comunica al servidor NFS mediante red "Ethernet".

b. **Costo y rendimiento**. La mayor parte de las plataformas de virtualización soporta NAS. Debido a que NAS es un protocolo muy utilizado, existen diferentes opciones para utilizar un almacenamiento NAS con las máquinas virtuales: desde un servidor físico convertido en servidor NAS o un dispositivo de almacenamiento dedicado basado en NAS.

   El coste y rendimiento de cada solución puede variar grandemente siendo los dispositivos dedicados los que ofrecen mayor rendimiento, pero a un coste más alto.

   En la mayoría de los casos, NAS no ofrece el mismo rendimiento que una red SAN FC pero una arquitectura de red bien configurada puede ofrecer un rendimiento adaptado a tus necesidades. De manera similar a iSCSI, NAS utiliza tarjetas de red para comunicarse con los dispositivos de almacenamiento, por lo tanto, tiene un límite de 1 Gpbs. A diferencia de iSCSI no permite "multipathing" ofreciendo un rendimiento inferior.

c. **Desventajas**. Entre las desventajas de NAS, no es posible arrancar un servidor directamente desde un dispositivo NAS. Adicionalmente, ciertos fabricantes no recomiendan NAS para ciertas aplicaciones sensibles a latencias.

4.4. Arreglos RAID

RAID es la sigla para "Redundant Array of Independent Disks". Su definición en español sería **Matriz Redundante de Discos Independientes**. Se trata de una tecnología que combina varios discos rígidos (HD) para formar una única unidad lógica,

donde los mismos datos son almacenados en todos los discos (redundancia). En otras palabras, es un conjunto de discos rígidos que funcionan como si fueran uno solo.

Este tipo de implementación permite tener una tolerancia alta contra fallas, pues si un disco tiene problemas, los demás continúan funcionando, teniendo el usuario los datos a su disposición como si nada pasara. La tecnología RAID está consolidada hace décadas, ya que surgió de la Universidad de Berkeley, en California (EUA) a finales de la década de 1980.

Para conformar el RAID es preciso utilizar por lo menos 2 discos rígidos. El sistema operativo, en este caso, mezclará los discos como una única unidad lógica. Cuando se graban datos, los mismos se reparten entre los discos del RAID, siempre dependiendo del nivel de RAID adoptado.

Mediante la implementación de RAID, además de garantizar la disponibilidad de los datos en caso de fallo de un disco, es posible también equilibrar el acceso a la información, de forma que no haya “cuellos de botella”.

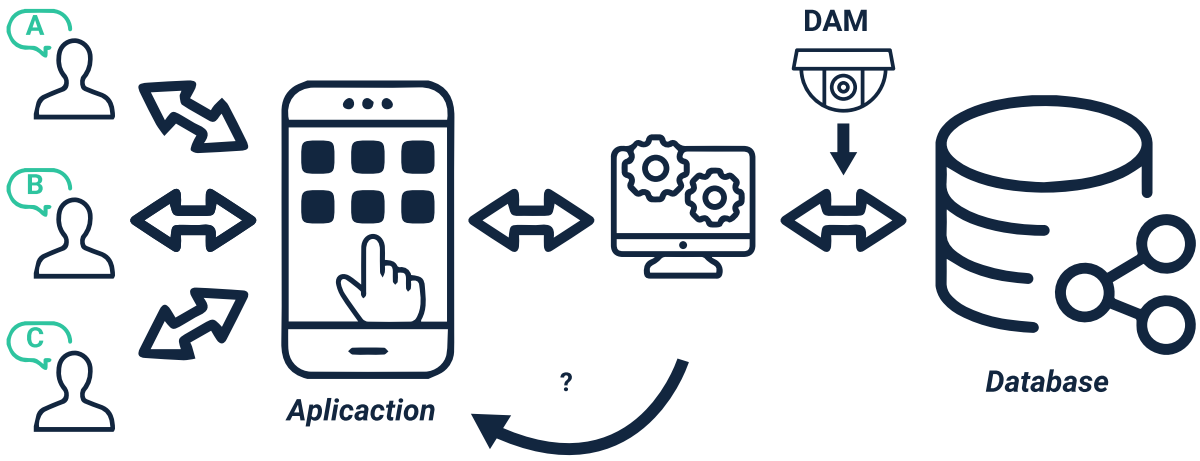
5. Seguridad en la nube

Para familiarizarse con este tema y apropiar conocimientos previos a su abordaje, explore el contenido del PDF denominado **Seguridad-nube**, específicamente los puntos del numeral 11, sobre el modelo MSPI del ministerio TIC, el cual puede ser consultado en la carpeta Anexos.

Un problema frecuente es la gestión de los datos en Cloud, migraciones de datos sensibles sin aprobación o informado a las áreas necesarias para ello.

Además de los controles tradicionales de seguridad de los datos (como controles de acceso o cifrado), hay otros dos pasos que ayudan a gestionar la migración no autorizada de datos a servicios Cloud, los cuales son:

a. Monitorizar la existencia de grandes movimientos internos de datos con herramientas de monitorización de actividad de bases de datos ("DAM - Database Activity Monitoring") y de monitorización de actividad en archivos ("FAM - File Activity Monitoring").



b. Monitorizar la migración de datos a Cloud con filtros URL y herramientas "Data Loss Prevention". En las implementaciones de Cloud públicas y privadas, y a través de los diferentes modelos de servicio, es importante proteger los datos en tránsito. Esto incluye:

- Los datos moviéndose desde la infraestructura tradicional a los proveedores.
- Cloud, incluyendo público/privado, interior/exterior y otras combinaciones.
- Los datos migrando entre los proveedores de Cloud.
- Los datos moviéndose entre instancias (u otros componentes) en un "cloud" determinado.

Hay tres opciones.

a. Cifrado cliente/aplicación. Los datos son cifrados en el extremo o en el servidor antes de enviarse por la red o ya están almacenados en un formato de cifrado adecuado. Esto incluye el cifrado en cliente local (basado en agente), por ejemplo, para archivos almacenados, o el cifrado integrado en aplicaciones.

b. Cifrado enlace/red. técnicas de cifrado de red estándar incluyendo SSL21, VPNs22, y SSH23. Puede ser "hardware" o "software". Es preferible extremo a extremo, pero puede no ser viable en todas las arquitecturas.

c. Cifrado basado en "proxy". los datos son transmitidos a un servidor dedicado o servidor "proxy", el cual los cifra antes de enviarlos por la red. Es la opción escogida frecuentemente para la integración con aplicaciones "legacy" pero no es generalmente recomendable.

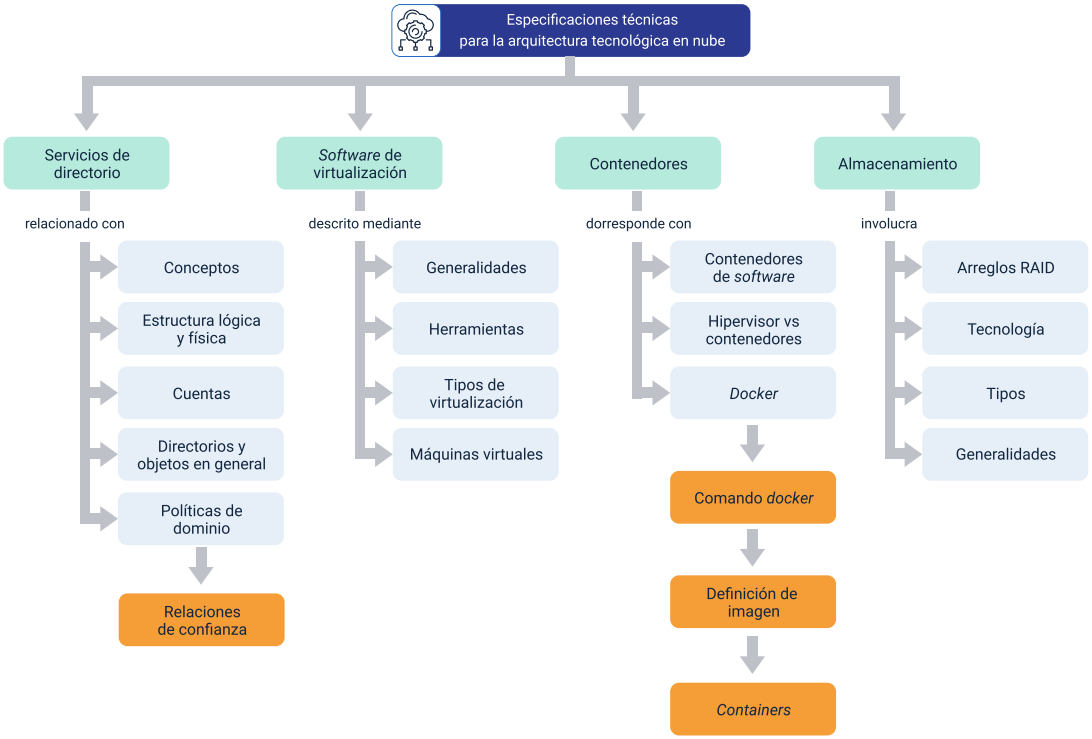
Síntesis

La arquitectura de la nube, tiene algunas especificaciones técnicas que deben tenerse en cuenta cuando se van a llevar a cabo procesos de gestión en Cloud.

En algunos casos la estructura lógica y física posibilitará un mejor y mayor desarrollo de la gestión, sin embargo, es necesario tener en cuenta las características propias del dominio, la seguridad con que deben establecerse las cuentas, que permiten generar relaciones de confianza para el usuario y el administrador.

Por otra parte, el recurso del Docker, como contenedor, es de fácil manejo y servicio, posibilitando un mejor almacenamiento de información, todo esto enmarcado en las guías que ha facilitado Min Tic para el desarrollo tecnológico.

Un resumen de lo visto en el presente componente, está registrado en el siguiente mapa:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Servicios de directorio	Microsoft. (2023). Introducción a AD DS.	Página web	https://learn.microsoft.com/en-us/training/modules/introduction-to-ad-ds/
3.3 Docker	Docker docs. (2023). Install Docker Desktop on Windows.	Página web	https://docs.docker.com/desktop/install/windows-install/
3.3 Docker	Docker docs. (2023). Dockerfile reference.	Página web	https://docs.docker.com/engine/reference/builder/
3.3 Docker	Microsoft. (2023). Dockerfile on Windows.	Página web	https://learn.microsoft.com/en-us/virtualization/windowscontainers/manage-docker/manage-windows-dockerfile
5. Seguridad en la nube	MinTIC. (2016). Seguridad en la Nube. Guía 12.	Guía	https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

Glosario

Active Directory: es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.

Contenedores: en el sector del transporte se usan contenedores físicos para aislar diferentes cargas (por ejemplo, para el transporte en buques y en trenes). Las tecnologías de desarrollo de "software" usan cada vez más un método denominado contenerización.

Dominio: cuando hablamos de virtualización, almacena una partición de directorio de dominio que consta de información sobre el dominio en el que se encuentra, más el esquema y las particiones del directorio de configuración para todo el bosque.

Migración: la migración de la TI consiste en trasladar datos o "software" de un sistema a otro.

Virtualización: es una tecnología que permite crear servicios de TI útiles, con recursos que están tradicionalmente vinculados al "hardware".

Referencias bibliográficas

A Linux a Day (2016). ALMACENAMIENTO, INTRODUCCIÓN Y TERMINOLOGÍA. [Blog]. Wordpress. https://alinuxaday.wordpress.com/2016/01/19/almacenamiento-introduccion-y-terminologia

Amazon. (2021). AWS Directory Service. https://aws.amazon.com/es/directoryservice/?nc=sn&loc=1

Astaiza y Taborda (2021). Componente Formativo 5. Virtualización del módulo 5 del tecnólogo Despliegue de aplicaciones y servicio en la nube. SENA.

Astaiza y Taborda (2021). Componente Formativo 6. Contenedores del tecnólogo Despliegue de aplicaciones y servicio en la nube. SENA.

Castillo, J.A. (2018). Active Directory Que es y para qué sirve. Profesional review. https://www.profesionalreview.com/2018/12/15/active-directory/

Microsoft (2021). Configuración de redundancia geográfica con Replicación de SQL Server. https://docs.microsoft.com/es-es/windows-server/identity/ad-fs/deployment/set-up-geographic-redundancy-with-sql-server-replication

Microsoft. (2021). Cuentas de Active Directory. https://docs.microsoft.com/es-es/windows/security/identity-protection/access-control/active-directory-accounts

Microsoft. (2021). Línea base de seguridad de Azure para Azure Active Directory https://docs.microsoft.com/es-es/security/benchmark/azure/baselines/aad-security-baseline?toc=/azure/active-directory/fundamentals/toc.json

MinTIC (2016). Seguridad en la Nube. Guía 12. https://mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

RDR-IT.COM. (2021). Active Directory: relación de confianza entre dos bosques / dominios. https://rdr-it.com/es/active-directory-relacion-de-confianza-entre-dos-bosques-dominios/

SANS Institute. (2003). Global Information Assurance Certification Paper. https://wwgrupo/105441#:~:text=Las%20pol%C3%ADticas%20de%20grupo%20del,las%20necesidades%20de%20cada%20usuario

Tecnología+informática. (2021). ¿Qué es RAID? Los niveles de RAID. https://www.tecnologia-informatica.com/que-es-raid-los-niveles-de-raid

virtualizamos.es (2021). ¿Qué tecnología de almacenamiento elijo? Fibre Channel, iSCSI o NAS. https://www.virtualizamos.es/que-tecnologia-de-almacenamiento-elijo-fibre-channel-iscsi-o-nas

Créditos

Nombre	Cargo	Centro de Formación y Regional
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Pablo Cesar Pardo Ortiz	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Hernando José Peña Hidalgo	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
José Luis Bastidas Pérez	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Joaquín Patiño Cerón	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Peter Emerson Pinchao Solís	Experto temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Henry Eduardo Bastidas Paruma	Instructor	Centro de Teleinformática y Producción Industrial - Regional Cauca
María Inés Machado López	Diseñadora instruccional	Centro de Diseño y Metrología - Regional Distrito Capital
Carolina Coca Salazar	Metodóloga	Centro de Diseño y Metrología - Regional Distrito Capital
Sandra Patricia Hoyos Sepúlveda	Corrección de estilo	Centro de Diseño y Metrología - Regional Distrito Capital
Miroslava González Hernández	Diseñadora Instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martínez Torres	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Centro de Formación y Regional
Wilson Andrés Arenales Cáceres	“Storyboard” e ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andrés Bolaño Rey	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Blanca Flor Tinoco Torres	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Andrea Paola Botello De la Rosa	Desarrollador “Full-stack”	Centro Industrial del Diseño y la Manufactura - Regional Santander
Andrea Paola Botello De la Rosa	Actividad didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander