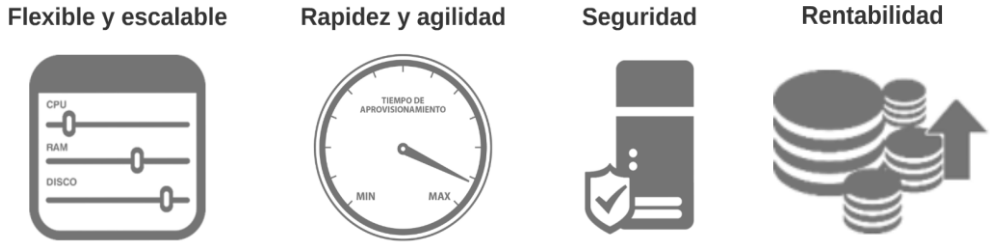
Guía de Mejores Prácticas
Servicios de Infraestructura
“Datacenter Virtual + Servidores Virtuales”



Claro cloud

Claro
Es simple

TE DAMOS LA BIENVENIDA AL SERVICIO DE INFRAESTRUCTURA COMO SERVICIO

Esperamos poder satisfacer y exceder tus expectativas como usuario de nuestros servicios. Por ese motivo te brindamos una guía rápida con las mejores prácticas y algunos comentarios que te ayudaran a explotar al máximo los beneficios de Claro Cloud.

DATACENTERS VIRTUALES

También existe la opción de contratar un Datacenter Virtual (DCV), como una unidad de networking y cómputo, e incluir dentro del mismo los Servidores Virtuales que sean necesarios, según el tipo y capacidad de cada DCV.

Los DCV te permiten manejar esquemas de Nubes privadas e híbridas, así como arquitecturas de Front End – Back End.

SERVIDORES VIRTUALES

Windows Server 2016
CentOS
MySQL
redhat
Microsoft SQL Server
debian
ubuntu

NUESTROS SOCIOS ESTRATÉGICOS

Powered Cisco Cloud Service
vmware
redhat LINUX
EMC²

Claro
Es simple

Servidores Virtuales - Consideraciones generales

Con Servidores Virtuales Claro Cloud, podés disponibilizar múltiples aplicaciones y servicios. Para potenciar el rendimiento y performance de tus servidores, te hacemos llegar lo siguiente:

- ✓ El servicio incluye 1 snapshot por SV, que puede generarse cada vez que quieras, pero siempre quedara el último generado. El mismo capturará la imagen únicamente del Disco donde esta el SO, no se debe mantener por mas de 72hs ya que puede perder integridad.

- ✓ Desde tu panel de control podés incrementar y disminuir la configuración en minutos y sin penalizaciones de acuerdo a la siguiente matriz (Figura 1)

- ✓ Tené en cuenta que cualquier cambio que realices en el SV requiere el reinicio del mismo. Esta tarea se realizará automáticamente. O podes apagar aplicar cambios y volver a encender. (solo aplica a CPU y RAM)

Servidores Virtuales - Información importante

- ✓ Recorda que será muy importante modificar tus contraseñas de acceso a los servidores virtuales y panel de control Claro Cloud para evitar vulnerabilidades.

- ✓ Si sos usuario de servidores Linux, recordá que para acceder a comandos con privilegios *root*, podés usar el comando *–sudo. (no utilizar el usuario root para inicios de sesión remotos)*

- ✓ Si sos usuario de *MySQL o de MSSQL Web o MSSQL STD edition* y necesitás acceso como usuarios SA, consultá las passwords con nuestro Soporte Cloud.

- ✓ Los servidores virtuales(SV) en Nube Pública o en Data Center Virtuales asignados a vLANs públicas, tendrán acceso directo a Internet.

Es simple

Servidores Virtuales - Información importante

- ✓ En el uso de SV, si tu aplicación tiene una tasa de transferencia de paquetes por segundo muy alta o bien hace un uso excesivo del ancho de banda disponible, por cuestiones de seguridad y performance de la plataforma, la IP del SV se bloqueará y vas a tener que comunicarte con nuestro Soporte Cloud. Para mas detalle sobre este punto, consulta a tu Ejecutivo de Ventas y Consultor, o comunicate con nuestro soporte.

- ✓ El ancho de banda asignado a tu infraestructura no es ilimitado.

- ✓ Por defecto cada SV cuenta con la disponibilidad de dos usuarios de acceso remoto, recurrentes. Si fueran necesarios más se deben de contratar por separado.

Servidores Virtuales – Manteniendo el Automatismo

Contrataste un servicio único en el mercado, que te permite gestionar tus servidores virtuales con total automatismo, para preservar y mantener el correcto funcionamiento de la automatización de nuestra plataforma, te recomendamos:

Claro
Es simple

Servidores Virtuales – Manteniendo el Automatismo

Contrataste un servicio único en el mercado, que te permite gestionar tus servidores virtuales con total automatismo, para preservar y mantener el correcto funcionamiento de la automatización de nuestra plataforma, te recomendamos:

- ✓ No modificar el nombre del host (máquina virtual). Se debe mantener el nombre de host que se le asignó desde el panel de control al momento de la compra.

- ✓ Las IPs y puertos de servicios que se utilizan para aprovisionar y administrar los servidores son:
  - 172.24.70.14
  - 172.24.203.0
  - 172.24.201.89 (ACM.AD.DC01.CLOUDCLARO)
  - 172.24.201.90 (ACM.AD.DC02.CLOUDCLARO)
  - El agente de blade logic (rscd) y el puerto que usa es el 4750

Es necesario no filtrar estas IPs y puertos desde el firewall del servidor, llámese iptables, firewalld, firewall de windows,etc.

- ✓ Validar que los siguientes procesos, estén siempre ejecutándose (ejemplo sobre Linux):

```
root      2818     1  0 may07 ?        00:00:00 bin/rscw
root      2819  2818  0 may07 ?        00:00:00 bin/rscd
root      2820  2818  0 may07 ?        00:00:00 bin/rscd
```

vmware

Es simple

Datacenter Virtuales consideraciones generales

También contas con la posibilidad de armar y diseñar una arquitectura virtual a tu medida. Para eso hemos creado los Datacenter Virtuales Claro Cloud.

- ✓ Disponemos de múltiples tipos de Datacenters, cada uno cuenta con configuraciones y características particulares. Visita nuestra pagina web para mas detalles de la oferta: ***mas info***

- ✓ Cada vez que agregues un servidor virtual a tu DCV, deberás elegir a que vLANs asociarlo, de acuerdo al rol que el SV tenga en tu solución.

- ✓ Si sos usuario de un DCV Corporativo Híbrido, recordá que el mismo cuenta con dos zonas de conectividad, una zona pública, con sus vLANs públicas y privadas, y a su vez una Zona privada, con solo vLANs privadas con conectividad exclusiva al enlace MPLS/RPV contratado.

- ✓ Te entregaremos usuarios y acceso por *VPN client (IP-SEC)* o *VPN Box to Box,* si así lo solicitaste, para poder conectarte a tu DCV

- ✓ Por cuestiones de seguridad entregamos el DCV sin reglas cargadas en el FW, por lo cual para ingresar a tu SV deberás cargar la regla que te permitirá conectarte desde tu origen. Luego deberás generar las reglas por cada servidor según los permisos que consideres necesarias.

  IMPORTANTE: No es necesario cargar reglas de salida. De hacerlo eliminaran la regla por default que permite todo el trafico saliente sobre el contenedor de red y deberán cargar reglas individuales sobre cada SV.

Para mas detalles, te aconsejamos leer el
"Manual de Configuración y Conexión Datacenter Virtual"
en donde encontraras todos los pasos a seguir para poder conectarte sin problemas.

- ✓ No es recomendable desactivar los NICs del sistema operativo, por más que no estén en uso, ya que puede traer problemas en la gestión de toda la solución.

Claro
Es simple

Seguridad en tus Servidores, consideraciones generales

La plataforma de Claro Cloud cuenta con múltiples medidas de Seguridad, análisis de trafico, DDOS, Firewalls Avanzado, etc, tanto a nivel de cada instancia como a nivel general. Pero es altamente recomendable que por tu parte sumes una capa de seguridad adicional, haciendo uso de estas recomendaciones generales:

- ✓ Se recomienda armar esquemas de front-end / back-end a la ahora de recibir transacciones externas y no exponer servicios del back-end.
- ✓ Cerrar puertos conocidos cuando no fueran necesarios/utilizados (SSH, RDP, HTTP, HTTPS). No establecer reglas con “Permit Any”
- ✓ Utilizar contraseñas robustas (mínimo ocho caracteres, que contengan números, letras mayúsculas y minúsculas), mas aún para usuarios administradores.
- ✓ Aplicar actualizaciones de parches de seguridad en sistemas operativos y aplicaciones (Apache, JAVA, Linux, Windows, etc.)
- ✓ Chequeo periódico de vulnerabilidades.
- ✓ Referencias generales:
  - “Information Security Policy Templates”

    https://www.sans.org/security-resources/policies/

Windows:

- ➢ Aplicar parches críticos de seguridad recomendados por Microsoft.
- ➢ No modificar el usuario “Administrator”, para no romper automatismo.
- ➢ Si utilizas conexión por Remote Desktop, recomendamos cambiar los puertos conocidos de conexión por aleatorios RDP: click aqui
- ➢ Uso de Anti-Virus / Anti-Spyware: Recomendamos adquirir tus licencias de Seguridad Negocios (McAfee) desde tu Tienda Claro Cloud, ckick aquí
- ➢ Referencia Windows:
  - “Microsoft Windows Server R2: Proteja su Windows Server” https://docs.microsoft.com/es-es/windows-server/security/security-and-assurance

Es simple

Seguridad en tus Servidores, consideraciones generales

Linux:

- ✓ Aplicar parches críticos de seguridad recomendados en la distribución utilizada (Ubuntu, Centos, etc).
- ✓ Utilizar contraseñas robustas para todos los usuarios, muy especialmente para el usuario "root" (mínimo ocho caracteres, que contengan números, letras mayúsculas y minúsculas)
- ✓ Para el usuario "root" en lo posible utilizar "Trusted Hosts" para autorizar el acceso solo desde redes permitidas.
- ✓ Mantener un usuario con perfil de administrador archivado para casos de emergencias.
- ✓ Cambiar los puertos conocidos de conexión por aleatorios SSH
  - Debian y Ubuntu, instrucciones en wiki.debian.org: click aqui
  - CentOS, instrucciones en wiki.centos.org: click aqui
- ✓ Referencias Linux:
  - "Best Practices guide for securing the Linux Workstation" http://www.linuxsecurity.com/content/view/117700/171/
  - "How To Make Your Linux Server More Secure" https://www.linux.com/learn/how-make-your-linux-server-more-secure

SQL Server:

- ✓ Aplicar parches críticos de seguridad recomendados por Microsoft.
- ✓ Utilizar contraseñas robustas.
- ✓ Referencias SQL:
  - "Mejores Prácticas de Auditoria y Seguridad SQL 2005, 2008" https://blogs.technet.microsoft.com/jahalva/2009/09/29/mejores-practicas-de-auditoria-y-seguridad-sql-2005-2008/
  - "Microsoft Baseline Security Analyzer" https://technet.microsoft.com/es-es/security/cc184924.aspx

---

No dudes en contactarte con nosotros antes cualquier duda o inquietud. Recordá también que si querés más información de nuestros productos y servicios Cloud, podés visitar nuestra pagina web http://cloud.claro.com.ar/