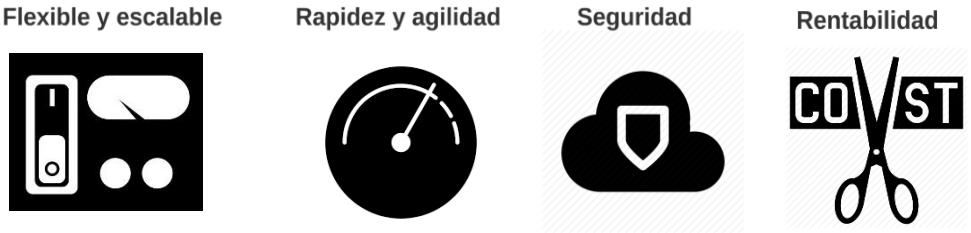




# Guía de Mejores Prácticas Servicios de Infraestructura




Claro cloud

## TE DAMOS LA BIENVENIDA AL SERVICIO DE SERVIDORES EN NUBE PÚBLICA

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 ayudarán a explotar al máximo los beneficios de Claro Cloud.

## NUBE PÚBLICA CLARO CLOUD

La familia de servicios y características incluidos en la Nube Pública de Claro, incluyen una amplia variedad de funcionalidades.

Las enumeramos aquí:

- Balanceador de Carga (Equilibradores de Carga HTTP)
- Generación de Imágenes de Servidores
- Back Up integrado con tres políticas de uso
- Monitoreo básico de tus servidores
- Auto-escalamiento de recursos (vCPU y GB RAM)
- Consola de conexión integrada.

Además, cada uno de los recursos contratados, serán facturados por hora de uso:

- Por cada servidor activo pero detenido, solo abonarás horas de uso del espacio de disco contratado, y la componente del Sistema Operativo, no se generarán cargos por GB RAM o vCPUs (Mhz).

# Servidores Nube Pública - Consideraciones generales

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

- ✓ Matriz de opciones y límites de recursos

| Características de la Oferta | | Standard | Mid | Performance |
|---|---|---|---|---|
| Procesamiento | #vCPU incluidas | 1 | 2 | 4 |
| | #vCPU máxima | 16 | 16 | 16 |
| Memoria | GB RAM incluida | 1 | 2 | 8 |
| | GB RAM máxima | 128 | 128 | 128 |
| Almacenamiento | Capacidad incluida | 50 | 200 | 1000 |
| | Capacidad máxima | 5000 | 5000 | 5000 |

- ✓ Cada servidor podrá tener un máximo de *16 vCPU* o virtual core, a su vez es importante notar que cada vCPU *equivale a un procesamiento de 1000Mhz*, y podrás incrementar cada uno de ellos *hasta 2000Mhz.*

- ✓ La herramienta de autoscaling / auto-escalamiento de recursos, se rige por ciertos límites:
  - ➢ GB RAM: se podrá escalar hasta el máximo de GB RAM por servidor, ***128 GB RAM.***
  - ➢ vCPU: como máximo cada vCPU puede tener 2000Mhz, por lo tanto, la capacidad máxima de procesamiento por servidor será:
    ***<cantidad de vCPUs * 2000Mhz>***

Por ejemplo, si tu servidor tiene 2 vCPUs, podrás escalar como máximo hasta 4000Mhz.

# Servidores Nube Pública - Consideraciones generales

✓ Familias de sistemas operativos disponibles:

- Windows Server 2016 R2 standard 64-bit
- CentOS 7
- Red Hat 7 Enterprise Linux
- Debian 9
- Ubuntu 16.04

✓ Por cada Suscripción de Nube Pública, estarán disponibles como máximo: ***15 SERVIDORES Y 15 IP PÚBLICAS***, cuyos servidores podrán tener conectividad entre sí.

✓ La infraestructura de Claro Cloud (Servidores de Nube Pública y Data Centers Virtuales) cuenta con un Firewall que filtra y analiza el tráfico de los servidores, a fin de garantizar la integridad de la plataforma. Si bien no hay límites establecidos a nivel de transferencia, sí existen políticas de restricción con el objetivo de evitar el uso abusivo o poco seguro de la plataforma. Ante el caso de un comportamiento sospechoso, (por ejemplo, pero no limitado a: utilización de puertos poco conocidos, excesivo consumo de datos – cantidad alta de peticiones/segundo), el Firewall puede bloquear el Servidor Virtual, o bien la dirección de la IP externa involucrada.

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

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

# Servidores Nube Pública - Consideraciones generales

- ✓ **IMPORTANTE**: La directiva predeterminada de todos los Servidores en Nube Publica Claro Cloud, permite todo el tráfico entrante y saliente de los siguientes puertos predeterminados HTTP, HTTP y SSH/RDP, y luego podrás generar o eliminar reglas para otros puertos.

  Así mismo, por la seguridad de tu infraestructura, hemos cerrado algunos puertos que consideramos para uso malicioso, de forma permanente desde el Firewall centralizado:

  - TCP/445 --> consultar por su necesidad de uso
  - UDP161/ SNMP --> consultar por su necesidad de uso
  - TCP/UDP 135 139 --> consultar por su necesidad de uso
  - TCP/UDP 27000 27050 --> cerrados permanentemente
  - TCP/UDP 5790 5850 --> cerrados permanentemente
  - UDP 2300 2400 --> cerrados permanentemente
  - TCP/UDP 3475 3480 --> cerrados permanentemente

- ✓ Respecto a los balanceadores de carga, recordá que, por cada balanceador o equilibrador de carga, de forma automática se estará asignando una IP pública, la cual tendrá costos adicionales.

- ✓ Hablando de direcciones de IP públicas, una vez que a un servidor se le asigna una IP pública, ésta estará dedicada al servidor, pero si luego se elimina o remueve esa IP, no habrá garantías de que el mismo número de IP esté disponible en tu pool de IPs.

# Servidores Nube Pública - Consideraciones de facturación

Creemos muy importante también, que puedas conocer muy claramente el mecanismo de facturación, así como algunas consideraciones relevantes y particulares que harán que puedas entender mejor tu facturación mensual.

- ✓ La facturación de cada recurso y componente es en relación a la cantidad de horas en que estuvo en uso o activo por el precio unitario, a saber:
  - ➢ Cada unidad GB RAM – GB de disco – GB de espacio de imágenes – GB de espacio de backups
  - ➢ Cada vCPU o vCore (1 vCPU = 1000Mhz)
  - ➢ Cada sistema operativo

- ✓ En especial si hablamos de la facturación del componente de vCPU, hay que tener en cuenta que un vCPU puede tener más o menos de 1000 Mhz, siendo la unidad mínima facturable 1 vCPU/1000 Mhz, por lo tanto, si un servidor tiene durante cierta cantidad de horas, 1500Mhz, al precio unitario por cada 1000 Mhz se lo facturará x 1.5 unidades, es decir 1500 Mhz.

- ✓ En relación con las capacidades de Mhz por cada vCPU, queda especificado que como máximo cada core o vCPU, *podrá tener 2000Mhz (2GHz) de capacidad*. Esto tiene un impacto directo en las capacidades para el auto-escalamiento de vCPU.

  Si un servidor tiene 2 vCPUs, podrá escalar en procesamiento hasta 4000 Mhz. Si tiene 1 vCPU, sólo podrá escalar hasta 2000 Mhz. Es decir, podrá escalar a un ***máximo de <cantidad de vCPUs> * 2000Mhz.***

- ✓ Para que la funcionalidad de auto-escalamiento no te impacte inesperadamente en tu factura, es aconsejable que setees límites no muy grandes para los recursos de RAM y vCPU.

# Servidores Nube Pública - Consideraciones generales
# Backup – Copias de Seguridad

Vale la pena tener en cuenta con algo más de detalle, el mecanismo que la plataforma utiliza para realizar backups. Ejemplo **Política Mensual**:

Se guardan 12 puntos de restauración, cada 1er día del mes a las 00:30 (***es decir 12 meses disponibles para recuperar),*** pero en realidad como máximo, se van a almacenar **16 backups facturables**.

En este ejemplo, vemos al llegar al **mes 13**, no se eliminará el backup del **mes 1**, ya que, si luego del **mes 13** se quisiera restaurar al **mes 2, mes 3 ó mes 4**, no se podría, porque no se tiene el Full Backup base de esa cadena (Cadena 1), por lo tanto, recién al tener toda la cadena 4 completa se elimina toda la cadena 1.

| **Cadena 1** | | | | **Cadena 2** | | | | **Cadena 3** | | | | **Cadena 4** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M10 | M10 | M11 | M12 | M13 | M14 | M15 | M16 |
| **Full** | Inc | Inc | Inc | **Full** | Inc | Inc | Inc | **Full** | Inc | Inc | Inc | **Full** | Inc | Inc | Inc |

Para el caso de las otras dos políticas, la cantidad de backups y puntos de restauración son los siguientes:

- Diario:
  - 30 puntos de restauración, con un total de 36 backups almacenados
  - Todos los días entre las 00:00 y 00:30 hs.
- Semanal:
  - 25 puntos de restauración, con un total de 29 backups almacenados.
  - Todos los Domingos a las 00:30 hs.

**IMPORTANTE:** Si se elimina manualmente algún backup de una cadena dada, y luego se quiere restaurar a ese backup o algún otro posterior de la misma cadena, el resultado podría no ser consistente.

# Seguridad en tus Servidores - Consideraciones generales

La plataforma de Claro Cloud cuenta con múltiples medidas de Seguridad, análisis de tráfico, DDOS, Firewall 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.

## Generalidades MUY IMPORTATES para aplicar:

- ✓ Se recomienda **armar esquemas de front-end / back-end** a la hora de recibir transacciones externas y no exponer servicios del back-end.
- ✓ **Realizar copias de seguridad** frecuentemente desde la herramienta unificada.
- ✓ **Cambiá** el protocolo de conexión a puertos "no conocidos". Esto te dejará fuera de típicos ataques. Por ejemplo, si vas a usar puertos de acceso remoto como RDP o SSH, te dejamos instrucciones:
  - En Windows: <click aquí para más información>
  - En Linux Debian y Ubuntu: <click aquí para más información>

  y Centos: <click aquí para más información>
- ✓ **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 (JAVA, Linux, Windows, etc.
- ✓ **Chequeo periódico de vulnerabilidades.**
- ✓ **Uso de Anti-Virus Anti-Spyware:** Recomendamos adquirir tus licencias de Seguridad Empresas (desde tu Tienda Claro Cloud, click aquí)
- ✓ Referencias generales:
  - "Information Security Policy Templates"

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

# Seguridad en tus Servidores - Consideraciones generales

## Windows:

- ✓ Referencia Windows:
  - ✓ "Microsoft Windows Server R2: Proteja su Windows Server" https://docs.microsoft.com/es-es/windows-server/security/security-and-assurance

## Linux:

- ✓ 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 sólo desde redes permitidas.

- ✓ Cambiar los puertos conocidos de conexión por aleatorios SSH:
  - Debian y Ubuntu, instrucciones en wiki.debian.org: click aquí
  - CentOS, instrucciones en wiki.centos.org: click aquí

- ✓ 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

---

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