
# INSTRUCCIONES GENERALES PARA EL ACCESO A LA PLATAFORMA - CONFIGURACIÓN Y USO DEL SERVICIO VPS

**ÍNDICE**

## Introducción

El servicio de **Arrendamiento de Servidor Privado Virtual (VPS**) brinda a las **personas naturales** la posibilidad de configurar uno o varios servidores virtuales en función de sus necesidades y con las características en cuanto a recursos que requiera, siempre dentro de los límites que establece el servicio y plantillas predefinidas en la **Plataforma**. Puede administrar sus servidores por SSH o escritorio remoto y modificar dinámicamente las características de un servidor, incluso con el servidor en producción sin afectar el servicio.

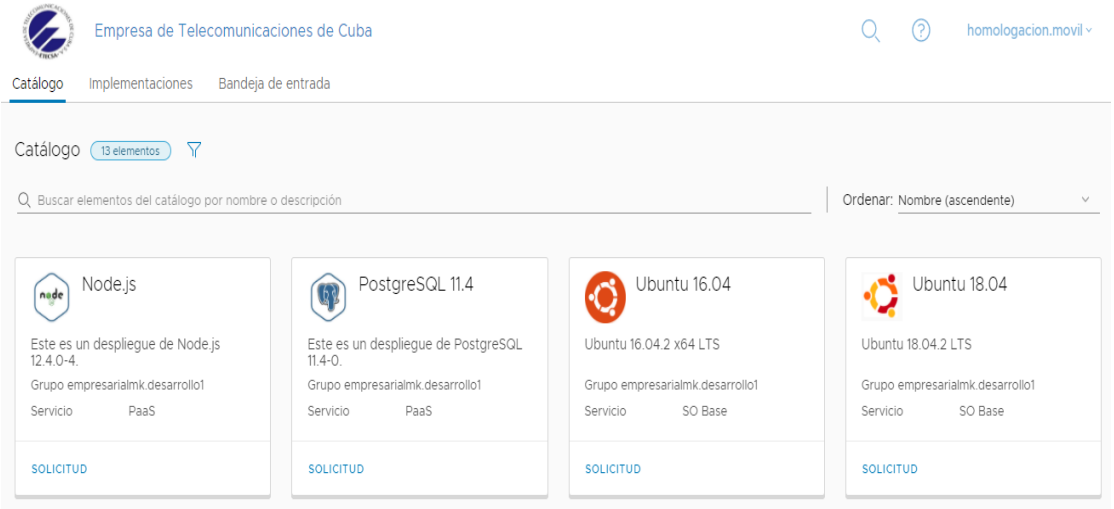
## Instrucciones para configurar y usar el servicio VPS

1. Acceder a la interfaz de gestión desde la **URL:** https://cloud.cd.etecsa.cu/vcac/org/naturales.

   El sitio funcionará con **certificado auto firmado** el que deberá aceptar para continuar, **se recomienda utilizar una versión actualizada de *Google Chrome*** (el idioma del portal dependerá del navegador).
2. Seleccionar el dominio ***nauta.cu*** y hacer clic en **Siguiente**. Se recomienda **recordar esta opción** para que solo se muestre una sola vez

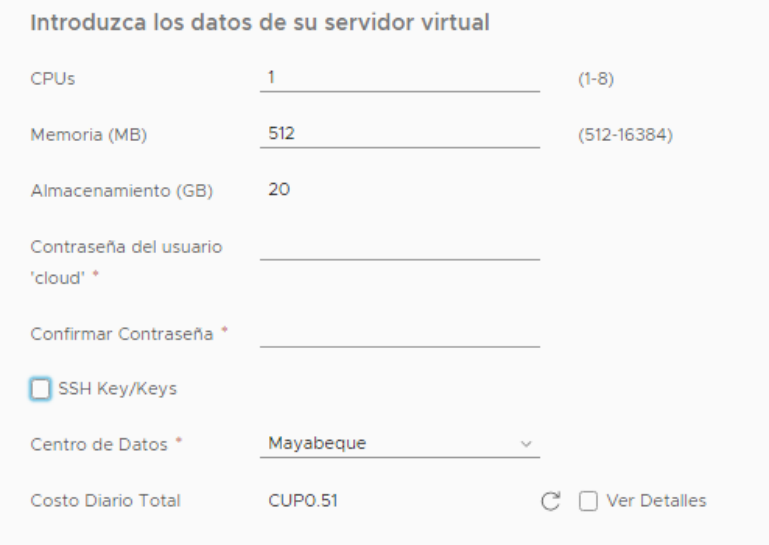

3. Teclear el usuario y la contraseña de la cuenta de correo ***nauta*** y hacer clic en **Iniciar sesión**. En el **nombre de usuario** no es necesario especificar el dominio pues la plataforma asumirá por defecto el que se especifica en el punto anterior.
   El usuario de correo debe coincidir con los datos aportados por el Cliente en la firma del Contrato.


**4.** Una vez autenticado se muestra en la Plataforma el **Catálogo** disponible.

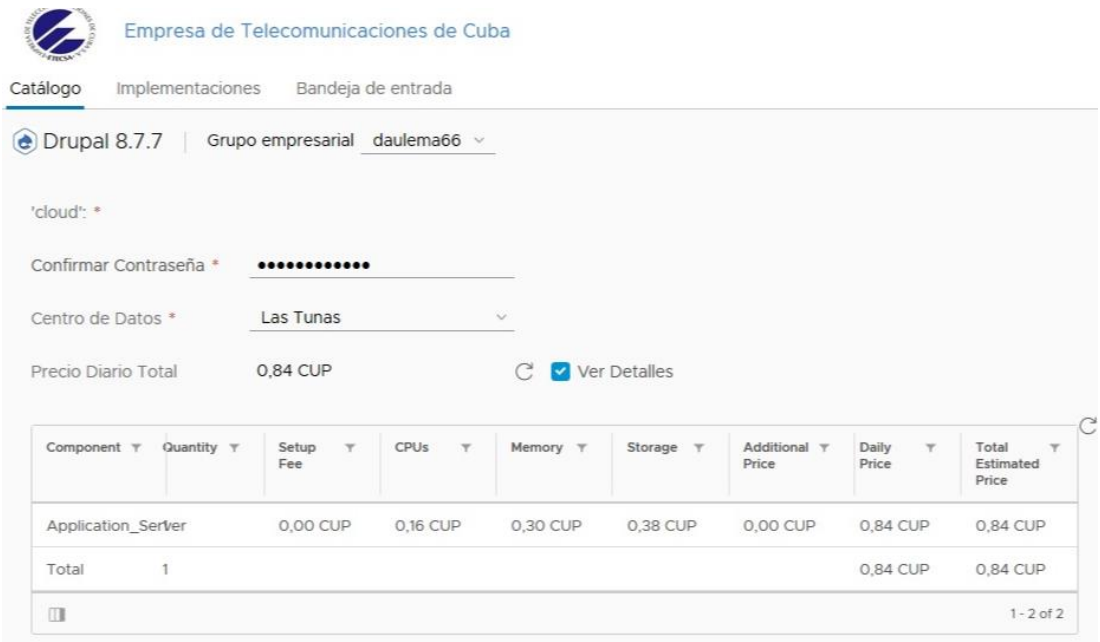



**5.** Para realizar un despliegue a partir del **Catálogo** se hace clic en **SOLICITUD** en el elemento que se desea desplegar.

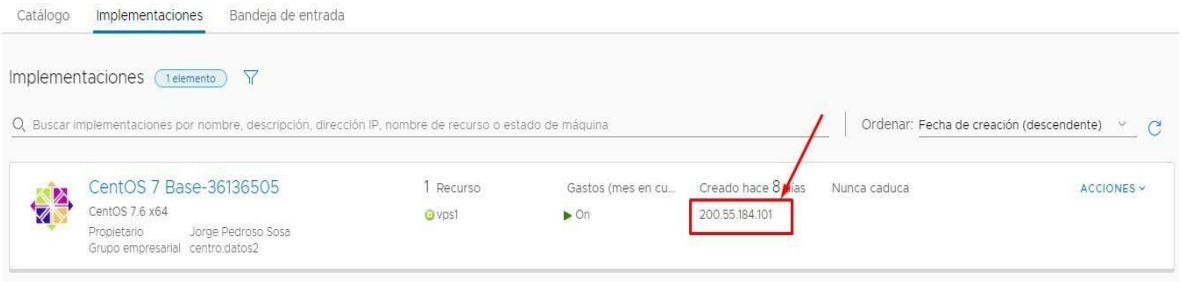
6. Rellenar los **Datos del formulario** con los recursos requeridos.
   Todos los campos son obligatorios. El despliegue de un Sistema Operativo base demora aproximadamente 5 minutos. Se incluye una IP pública con el despliegue.




| Datos | Observaciones |
|---|---|
| CPUs | Rango entre 1 y 8 |
| Memoria | Rango entre 512 MB y 16 GB |
| Almacenamiento | 20 – 500 GB. |
| Contraseña del servidor | Contraseña que se le asigna al usuario "**cloud**". Posteriormente se puede escalar al usuario root ya que el usuario cloud se encuentra en la lista de sudoers. |
| SSH Key/Keys | Si marca esta opción, se mostrará un campo de texto, en el cual si lo desea puede introducir las llaves públicas.<br>Si decide usar esta opción, el proceso de provisión automáticamente deshabilitará la autenticación (*login*) por medio de contraseña (*password*) haciendo más seguro el VPS desplegado. |
| Centro de Datos | Están disponibles 3 regiones para el despliegue del servidor virtual. Por defecto se pueden desplegar 9 servidores, 3 por cada región. |
| Costo/Precio Diario Total. | Este valor es una **referencia del costo diario** del servidor virtual del cliente de acuerdo con los recursos de RAM, CPU y Almacenamiento que haya configurado. Al seleccionar **Ver Detalles** se muestra un desglose del precio por recurso.<br>Una vez concluido el despliegue, esta información no se muestra nuevamente. |



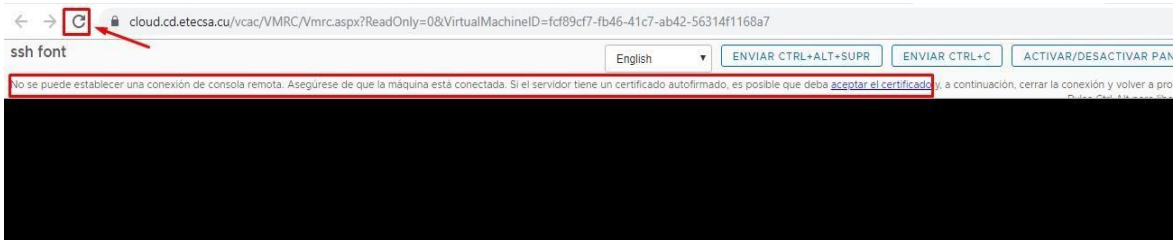

**7.** En la pestaña **Implementaciones** se pueden **visualizar** todos los servidores virtuales desplegados.
Para gestionar el servidor se puede realizar a través de **ssh** o la **consola remota**. Para conectarse por **ssh** debe seleccionar la dirección IP real asignada y establecer una conexión con un cliente ssh. Ejemplo: ssh cloud@200.55.184.101 Si usted escogió la llave pública para el despliegue debe especificar su llave privada para conectarse.




**8.** Para abrir la consola remota utilizar el navegador *Google Chrome* con una versión actualizada y seleccionar el VPS.

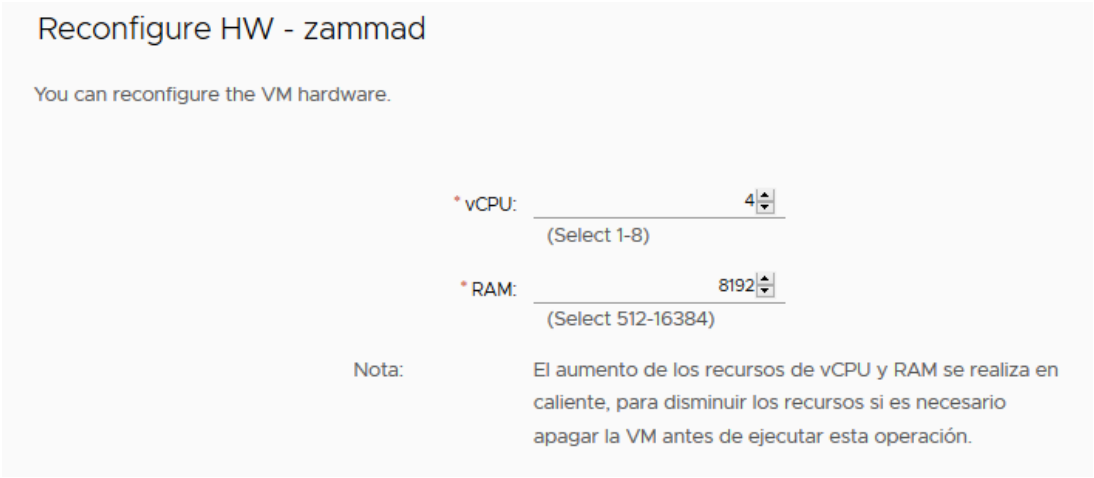

Seleccionar la máquina virtual (1), pinchar en las opciones de configuración (2) y seleccionar la opción **Conectar con la consola remota** (3).


Inmediatamente se abre una nueva ventana en el navegador, debe esperar a que salga el cartel del certificado y posteriormente hacer clic en el botón de **Actualizar**. Ya el certificado está cargado y NO es necesario dar clic en "aceptar el certificado", pinchar solamente **Actualizar**. Después de actualizar la página, se muestra la consola remota.
Autenticarse inicialmente con el usuario "**cloud**" y la contraseña introducida durante el despliegue.

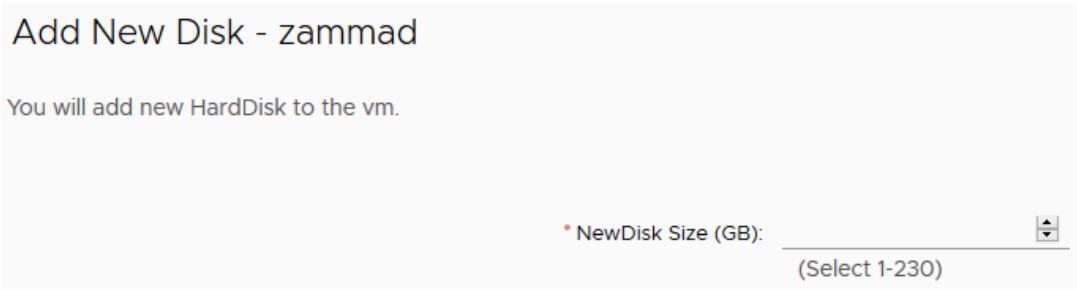



## Operaciones básicas disponibles sobre un servidor virtual.

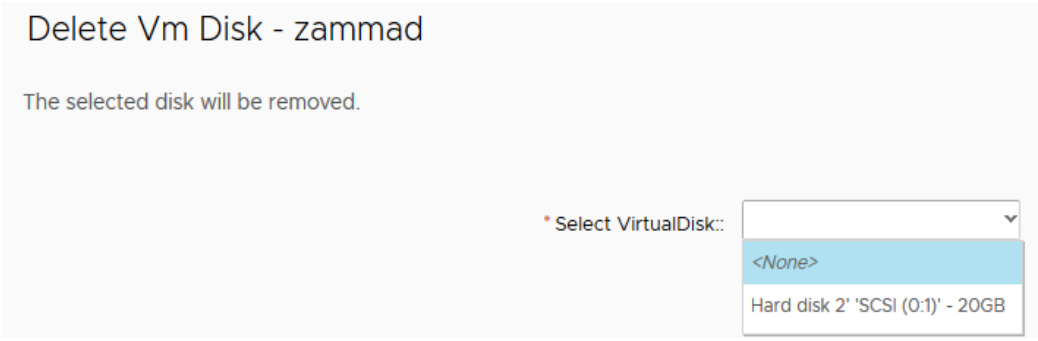
- ✓ **Encender la VM (Power On)-** Esta opción enciende la instancia del VPS.
- ✓ **Apagado brusco e instantáneo de la VM (Power Off)-** Esta opción apaga la instancia del VPS.
- ✓ **Apagado limpio a través de SO (Shutdown)-** Esta opción brinda un apagado suave (graceful shutdown), un apagado desde el sistema operativo, similar a tener configurada la opción de apagado del SO al presionar el botón de power.
- ✓ **Reiniciar VM (Reboot)-** Esta opción reinicia el sistema operativo de la instancia del VPS.
- ✓ **Reconfigurar recursos de la VM, expandir o reducir recursos de CPU, RAM (Reconfigure HW)-** Esta opción permite la modificación de los recursos de procesamiento RAM y CPU. Es una opción que dinámicamente permite la adición en caliente (VPS encendido) de estos recursos, siempre y cuando se encuentren dentro de los valores límites establecidos para el servicio. Cabe destacar que solo se puede en caliente hacer la adición de hardware, para modificar rebajando las cantidades tanto de RAM como CPU es necesario que se realicen estas tareas desde el estado de apagado (Ver nota aclaratoria en la propia página de la opción).




- ✓ **Destruir VM (Destroy)-** Esta opción destruye completamente la instancia del VPS, es importante señalar que con la misma se pierde la posibilidad de restaurar aun teniendo contratado el servicio de salva.
- ✓ **Destruir despliegue (Destroy Deployment)-** Esta opción destruye también la instancia del VPS, pero lo hace desde la vista de Despliegues ahorrándole pasos al usuario. Igual que la opción Destruir VM (Destroy)
- ✓ **Reanudar despliegue (Resume Deployment)-** Esta opción permite reanudar el despliegue de haber ocurrido algún error.
- ✓ **Adicionar nuevo disco (Add New Disk)-** En esta opción el usuario se puede agregar espacio al servidor previamente provisionado en forma de un nuevo disco duro.
  Solo es posible escoger la cantidad de espacio a adicionar y que dinámicamente solo se podrán crear discos hasta sumar el espacio máximo definido para el servicio o hasta que se alcance la máxima configuración de discos para la controladora virtual de discos (máximo 15 HDD). Corre por parte del usuario la extensión del FileSystem del VPS.

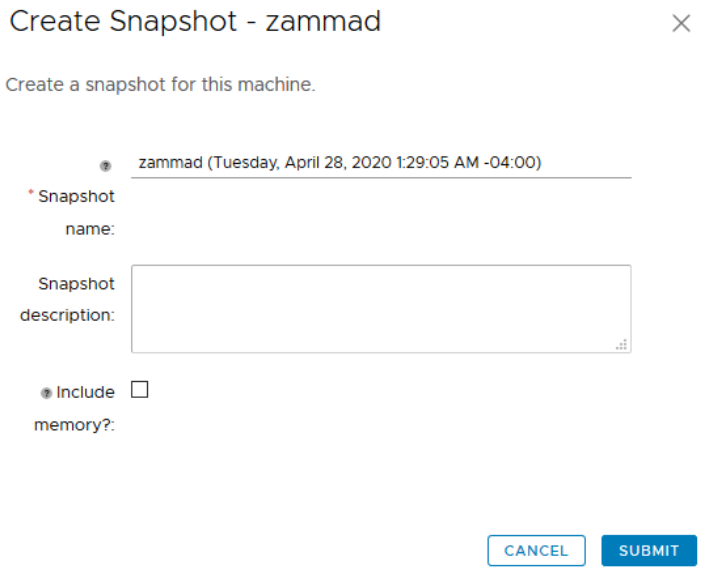



- ✓ **Eliminar Disco (Delete VM Disk)-** Opción que va dirigida a eliminar el disco previamente añadido al VPS (solo se mostraran los discos añadidos mediante la opción “Add New Disk”).
  Es importante señalar que cada cliente es responsable de hacer las tareas pertinentes al filesystem de su VPS previas a la eliminación del disco. El disco de sistema con el que se provisionó el VPS solo es posible eliminarlo usando la opción “Destroy” o “Destroy Deployment”.




- ✓ **Crear instantánea de la VM en el tiempo (Create Snapshot)-** En esta opción el usuario puede crear una instantánea de su VPS. La instantánea está dirigida a hacer una rápida restaura de la condición de la máquina virtual.
  Ejemplo de casos de empleo: Cuando se necesita hacer cambios drásticos en el sistema o probar una nueva funcionalidad.

  **Las características más notables son**:
  - Período de longevidad de 48 horas, después de pasado este tiempo es eliminada automáticamente.
  - Si se incluye la memoria se restaura el tiempo de ejecución (snapshot con VPS encendido y se salva la memoria, entonces al finalizar la restaura el estado es encendida y en ejecución).
  - Solo se puede crear una instantánea por VPS, si necesita crear otra debe borrar primero la ya existente.



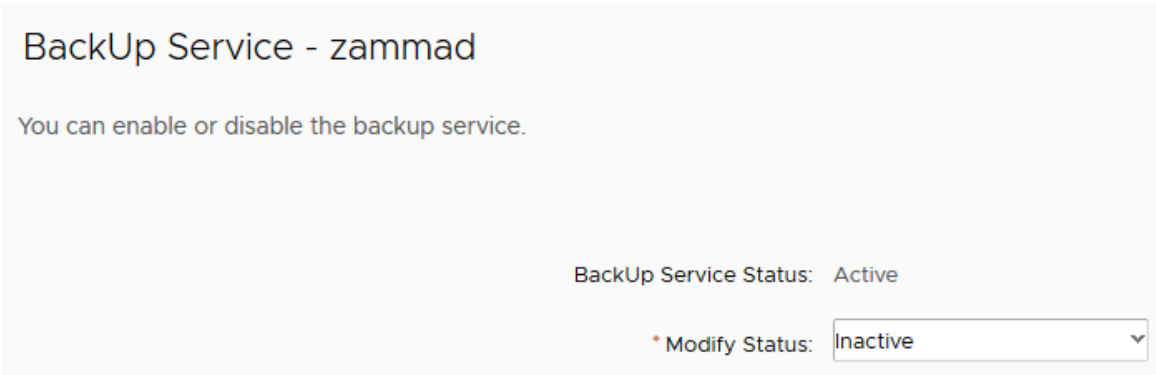

- ✓ **Revertir instantánea (Revert to Snapshot-)** Esta opción proporciona la posibilidad de restaurar la máquina inmediatamente a un estado anterior (no mayor a 48 horas).
- ✓ **Eliminar instantánea (Delete Snapshot-)** Esta opción proporciona la posibilidad de eliminar la instantánea creada para el VPS, dando así la posibilidad de crease uno nuevo.

- ✓ **Abrir la consola gráfica de la VM (Connect to Remote Console-)** Esta opción le proporciona al usuario la ventaja de tener conectados los periféricos al VPS (mv). En dicha opción se observará una consola web que permite la interacción con el servidor (homologo a tener un monitor conectado a la PC).

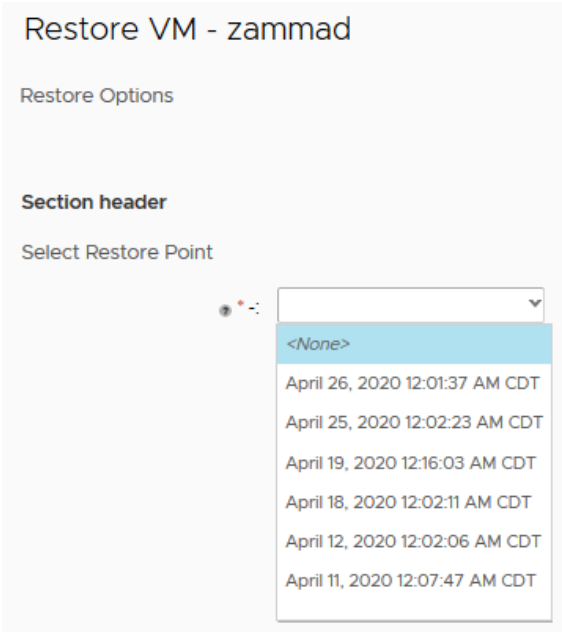
## Servicios adicionales de pago.

**Estos servicios estarán siempre disponibles desde la plataforma tecnológica y su habilitación desde la Unidad Comercial no conlleva costos.**
En la Plataforma **su estado por defecto es disponible e inactivo**, **solo se activan con operaciones que ejecute y configure el cliente desde la interfaz de gestión, haciendo uso de las operaciones del Panel de Control.** Una vez activados por el cliente, la Plataforma es capaz de identificarlos y generar los cargos correspondientes a su facturación mensual. El pago del servicio se realiza al finalizar el mes.

- ✓ **Servicio de salva con dos opciones**- El cliente tendrá la posibilidad de **activar** o no el servicio en la opción (***BackUp Service***) y la posibilidad de **Restaurar** su máquina a un estado anterior en la opción (***Restore VM)*** mediante la interfaz de gestión.
  - **Salva (BackUp Service)**
    **Características:**
    - Se realiza una vez a la semana.
    - Se guardan hasta 5 puntos de restaura (por lo que garantiza un mes)
    - Se realiza en función de la disponibilidad de los recursos de infraestructura.
    - Debe esperar como máximo una semana para poder disfrutar del punto de restauración.
    - El cliente tiene la opción de **desactivar** el servicio desde la interfaz de gestión. La inhabilitación del servicio no propicia que sea eliminado el punto de restaura que se realizó durante el tiempo que estuvo habilitado el servicio, solo este caducara a las 5 semanas de haberse realizado el mismo.




  - **Restaurar VM (Restore VM)-** Esta opción permite restaurar la instancia VPS al estado vigente en el momento de la Salva.
    Solo se mostrará los puntos de restaura que no sean más antiguos a 5 semanas. Cada punto de restaura tiene grabado el instante de tiempo en la que fue realizada la salva. Estar o no suscrito el servicio de salva no impide la restaura del VPS.




- ✓ **Transferencia mensual adicional (GB) (Add Transf)-** Este servicio le permite al cliente habilitar un volumen adicional de Transferencia Mensual (GB) al que se incluye en la oferta comercial.
  El volumen de Transferencia adicional tiene validez o podrá ser usado **solo durante el mes en curso.** El primer día del mes siguiente el volumen de Transferencia mensual toma el valor que está incluido en la oferta, es decir **250 GB.**

    - **Avisos por umbral de Transferencia:** ETECSA enviará al cliente mediante correo electrónico una notificación cuando el consumo de Transferencia mensual del servidor virtual contratado alcance el 80 % del volumen incluido en la oferta de servicio. El cliente decidirá si activa el servicio adicional o no. En caso de consumir todo el volumen de Transferencia mensual incluida en la oferta y no contratar el valor adicional, se procederá a deshabilitar el acceso a internet del servidor virtual después que el cliente sea notificado.

## Asistencia técnica

ETECSA garantizará para la asistencia y respuesta al cliente **como vía prioritaria** el **correo electrónico**, a través de la dirección ayuda.cdatos@etecsa.cu disponible las 24 horas de atención. El cliente debe especificar en el asunto del correo ante cualquier interrupción **"*Reporte VPS*"** para poder facilitar su clasificación.

# Tratamiento y uso del DNS y los registros

- ✓ **Características del servicio VPS con respecto al Servicio de Nombres de Dominio:**

El Servicio de VPS que se oferta en los Centros de Datos de ETECSA, brinda a los clientes los recursos necesarios para la creación y mantenimiento de las Máquinas Virtuales (MV) creadas por los mismos. Como parte del proceso de creación del VPS, se genera de manera automática, un nombre de ***host*** (HostName) único en la Plataforma con el siguiente formato: *srv4to3er-2do1er.**vps.etecsa.cu***

Donde:

- **srv**: prefijo
- **4to**: 4to. Octeto de la IP asignada a la MV
- **3er-**: 3er. Octeto de la IP asignada a la MV
- **2do**: 2do. Octeto de la IP asignada a la MV
- **1er**: 1er. Octeto de la IP asignada a la MV
- **vps.etecsa.cu**: Dominio bajo el cual se registra el nombre del host para el servicio.

Este nombre de **host**, se genera y registra (registro tipo A) en el servicio de DNS de los Centros de Datos de ETECSA, bajo el dominio ***"vps.etecsa.cu"*** y en las zonas reversas de los segmentos de red de los cuales se asignan las IPs a las MVs (registro tipo PTR) del servicio VPS.

Los registros **tipo A** y **PTR** serán eliminados automáticamente, en el momento en el que destruya la MV. El mantenimiento de los registros **tipo A** y **PTR**, solo puede llevarse a cabo por los procesos de creación y destrucción de las VPS. No es posible realizar (ni está previsto) la intervención humana en dichos procesos.

No es posible que el cliente o servicios de terceros, intenten "responder" a las preguntas sobre las IPs que como parte del servicio VPS se asignaron. Esas IPs, están bajo la autoridad de los Centros de Datos de ETECSA y dicha autoridad no se transfiere, ni se subdelega.

Nota: *Estos registros* (**tipo A** y **PTR**), ***"NO"*** *se* ***"subdelegan"****, ni se* ***"transfieren"****.*

Existe la posibilidad de que el cliente desee realizar por sí mismo, el manejo de su zona de dominio ya sea con los recursos (MV) del servicio de VPS y con recursos de un tercero. En este caso, no existe inconveniente alguno, siempre y cuando se haga referencia a los registros **tipo A** automáticamente asignados, bajo el dominio **"*vps.etecsa.cu*"**.

- ✓ **Escenarios:**

Para el manejo de los servicios de nombre existen 2 escenarios posibles, ambos le brindan al servicio VPS la flexibilidad necesaria para el uso de casi cualquier aplicación:

1- Servicio DNS **"Administrado por un Tercero"**, este caso incluye el servicio administrado por ETECSA u otro proveedor.
2- Servicio DNS **"Auto administrado",** donde el cliente administra su DNS delegando con su proveedor de Dominio la zona contratada hacia la IP asignada a su VPS u otro recurso que posea.

Tanto en el caso de que el cliente desee que su zona de dominio esté alojada en un servicio de terceros o desee alojarla en sus propios servicios, deberá tener en cuenta que:

Para reconocer cualquier tipo de registro DNS se debe crear primeramente la zona DNS correspondiente al dominio contratado.

Para referirse a su VPS por otro nombre distinto al asignado automáticamente, deberá crear (o solicitar al servicio de terceros) un registro **tipo CNAME** (alias) haciendo la referencia explícita al nombre generado automáticamente durante el proceso de creación de su MV (***srv4to3ro-2do1er.vps.etecsa.cu***)

**Ejemplo:** Para referirse con otro nombre (ejemplo **www**) al host ***srv5177-206152.vps.etecsa.cu***, bajo el dominio ***"MI.DOMINIO.CU"***:

www IN CNAME ***srv5177-206152.vps.etecsa.cu*.**

- ✓ **Aplicación**

Comúnmente usado para aplicaciones y sitios web, donde el cliente hace referencia a su VPS con un nombre de dominio contratado. Cuando se desee obtener el nombre del host a partir de su IP, como resultado se obtendrá el nombre generado automáticamente.

**Ejemplo:** Si se deseara obtener el nombre correspondiente a la IP 152.206.177.5, se obtendrá como respuesta: 5.177.206.152.addr.arpa. IN PTR ***srv5177-206152.vps.etecsa.cu.***

*"Si desea alojar un servicio de correos, deberá crear los registros **tipo TXT (SPF, DKIM, DMARC)** y **MX** correspondientes a los dominios a aceptar en entrada y/o salida, indicando los nombres automáticamente generados durante la creación de la MV"*

**Ejemplo:** Registro **SPF** para el dominio "***MI.DOMINIO.CU"***:

***mi.dominio.cu****. 3600 IN TXT "v=spf MX a a:****srv5177-206152.vps.etecsa.cu*** *-all"*

**Ejemplo:** Registro **DKIM** para el dominio "***MI.DOMINIO.CU"***:

***Selector: KEY2048***
***Key:*** *p=**
***KEY2048._domainkey.mi.dominio.cu****. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCYFzuCksBxMyqnc+Y4grmNIjyBnK2JcKg HuZrn4m5Cfm2yy1Es0y3P0y2R4iHuWwqhP7UOo/vMcDzf4cQ+aa/V1jBYB5sM/nB6olBBcBXnm1pdjt mkpBH7Hc4y/yBBNBF/f6vEN+iZN9zEE9PkEXHomm0DRfEZgn563CUUK9o8+QIDAQAB"*

**Ejemplo:** Registro **MX** para el dominio "***MI.DOMINIO.CU"***:

*@ IN MX 10* ***srv5177-206152.vps.etecsa.cu.***

Adicionalmente, el servidor emisor de correos, deberá anunciarse al servidor destino, con el nombre generado automáticamente durante la creación de la MV. Según el ejemplo anterior, **srv5177-206152.vps.etecsa.cu**

- ✓ **Descripción de los registros DNS más comúnmente usados:**

**Registro tipo NS**:
Un registro NS hace referencia al servidor de nombres de un archivo de zona y determina dónde recae la responsabilidad de una zona concreta. Es, por ello, un registro obligatorio en todo archivo de zona. Este registro de recurso indica al servidor DNS si es responsable de una solicitud o no, es decir, si tiene que organizar la zona en cuestión, o bien a quién tiene que reenviar la solicitud.

**Registro tipo A**:
La mayor parte de resoluciones de nombres de dominio en Internet se producen mediante registros tipo A, que contienen una dirección IPv4 en su campo de datos. Gracias a ellos, los usuarios de Internet pueden introducir un nombre de dominio en el navegador y hacer que el cliente envíe automáticamente una solicitud HTTP a la dirección IP correspondiente. Puesto que el tamaño de las direcciones IP siempre es de 4 bytes, el valor de rdlength también es siempre 4, si es que aparece.

**Registro tipo PTR**:
El registro PTR (pointer) es un registro DNS que permite una búsqueda inversa o reverse lookup. Con ella, el servidor DNS puede indicar qué nombres de host pertenecen a una dirección IP concreta. Para cada dirección IP usada en registros tipo A o AAAA existe, por consiguiente, un registro PTR. La dirección IP se forma en este caso en orden opuesto y se le añade, además, el nombre de una zona.

**Registro tipo CNAME**:
Un registro CNAME (canonical name record) contiene un alias, es decir, un nombre alternativo para un dominio, y remite a otro registro A o AAAA ya existente. El campo rdata en este tipo de registros lo ocupa, por lo tanto, un nombre de dominio previamente enlazado con una dirección IP. Así se pueden remitir varias direcciones diferentes al mismo servidor.

**Registro tipo TXT**:
Los registros TXT contienen texto, ya sea como fuente de información para usuarios humanos o para ser leído maquinalmente. En estos registros DNS, el administrador puede alojar texto no estructurado (a diferencia de los datos estructurados de otros registros DNS). Se pueden añadir también, por ejemplo, detalles sobre la empresa a la que pertenece el dominio. Dentro de este tipo de registro se encuentran DMARC,SPF y DKIM utilizados en servicios de mensajería.

**Registro tipo MX**:
El nombre del registro MX es una abreviación de mail exchange, intercambio que se produce mediante un servidor SMTP de correo electrónico. Aquí se definen uno o varios servidores de correo electrónico que pertenezcan al dominio en cuestión. Si se usan varios servidores de correo, por ejemplo, para compensar fallos, se establecen niveles de prioridad. De esta manera, el DNS reconoce en qué orden debe realizar las solicitudes de contacto.

- ✓ **Como proceder si quiero que ETECSA administre mis Nombres de Dominio para el servicio VPS:**

**Detalles del Proceder:**

I. Solicitar a la autoridad reguladora (CITMATEL), su dominio bajo ***"NAT.CU"*** y que delegue el mismo hacia los DNS públicos de ETECSA.

Por lo que, cuando el cliente le solicite a CITMATEL (o la entidad reguladora) la creación del dominio deseado, adicionalmente deberá indicar los nombres de host (o las IPs) de los servidores de DNS.

II. Una vez creado el dominio y se verifique su correcto funcionamiento, el cliente procederá a solicitar los registros requeridos para poder alcanzar sus servicios.

Una manera de comprobar que este proceso ya fue hecho es mediante los siguientes comandos:
Sistema Operativo Windows:
*~>nslookup -type=NS*
Sistema Operativo Linux:
*$: dig*

Esta solicitud de registros DNS se tramitarán mediante el área Comercial y deberá el cliente proveer todos los datos necesarios para la creación de dichos registros.

| CASOS | El CLIENTE debe proveer |
|---|---|
| Creación de la zona **DNS** | Nombre de dominio contratado Ej: ***midominio.nat.cu*** |
| Creación de registro **CNAME** | FQDN autogenerado del VPS desplegado donde reside el servicio a referenciar Ej: ***srv5177-206152.vps.etecsa.cu***<br>Alias dentro del dominio contratado Ej: ***www*** |
| Creación de registro **MX** | FQDN autogenerado del VPS desplegado donde reside el servicio Ej: ***srv5177-206152.vps.etecsa.cu*** |
| Creación de registro **TXT (SPF)** | En este caso, de no proveer los datos, se creará por defecto con los datos provistos para el Registro MX. |
| Creación de registro **TXT (DKIM)** | Selector Llave (key) |
| Creación de registro **TXT (DMARC)** | Este es un registro opcional y se forma a partir de los registros SPF + DKIM, pero si es requerido por el cliente, este deberá proveer todos sus elementos. |

Cualquiera sea el caso, es importante recalcar que, las referencias a los hosts creados en nuestro servicio de VPS, se realizara únicamente por el nombre generado automáticamente durante la provisión del VPS Ej: ***srv5177-206152.vps.etecsa.cu***.

## Recomendaciones de seguridad en el servicio VPS

Cada servicio VPS desplegado posee una IP real que le brinda la posibilidad de publicar una aplicación de alcance internacional, pero no queda exento de ataques constantes para hacerse de las credenciales de su despliegue o explotar vulnerabilidades de algún servicio que tenga corriendo sobre el mismo.

Por eso le proponemos los siguientes **consejos de seguridad**:

- ✓ **Mantenga actualizada la paquetería:**

Mantener el software actualizado es la una de las mejores prácticas que se pueden considerar a nivel de sistema operativo. Las actualizaciones de Software van desde el “PATCH” de las vulnerabilidades

críticas del sistema hasta las correcciones de bugs menores y de poca importancia. Muchas de las vulnerabilidades son parchadas en el momento en que se hacen públicas.

- ✓ **Actualizaciones automáticas**

Si son convenientes o no, depende de su aplicación, sistema y servicio en general. Pero son una ventaja si comparamos los riesgos de quedar expuestos y los males que puedan traer. Existe una muy buena discusión en la Wiki de Fedora.

CentOS - Use *yum-cron* para las actualizaciones automáticas.

Ubuntu - Use *unattended upgrades*.

- ✓ **Cree usuarios con privilegios limitados:**

Por defecto cuando crea el VPS, este ya tiene un usuario con los privilegios limitados.

Si es necesario para hacer todas las tareas administrativas, este usuario puede hacer uso del comando "sudo" que le permite elevar los privilegios de ***"root"*** temporalmente.

Si usted desea crear nuevos usuarios puede hacerlo mediante los comandos:

CentOS

1. Crear el usuario, reemplazando `nuevo_usuario` por el nombre de usuario deseado y proporcione la contraseña.

   ```
   $: useradd nuevo_usuario && passwd nuevo_usuario
   ```

2. Añada el usuario al grupo "Wheel" para que pueda obtener los permisos para ejecutar el comando "sudo":

   ```
   $: usermod -aG wheel nuevo_usuario
   ```

Ubuntu

1. Crear el usuario, remplazando `nuevo_usuario` por el nombre de usuario deseado y proporcione la contraseña.

   ```
   $: adduser nuevo_usuario
   ```

2. Añada el usuario al grupo "sudo" para que pueda obtener los permisos para ejecutar el comando **"sudo"**:

   ```
   $: adduser nuevo_usuario sudo
   ```

- ✓ **Fortificar el Acceso SSH**

Por defecto el acceso al VPS es por medio de la combinación usuario/contraseña usando el servicio SSH. El empleo de una llave criptográfica es mucho más seguro porque esta llave toma el lugar de la contraseña y en general es mucho más difícil de romper mediante ataques de fuerza bruta.

Para generar una llave criptográfica basta con abrir una terminal en su computador local, y ejecutar:

```
$: ssh-keygen -b 4096
```

**Nota:** Este comando se puede ejecutar desde las últimas versiones Window10, cualquier Linux y OS X. Si no posee una versión de sistema que se lo permita, puede usar la utilidad PuTTY.

Puede dejar los nombres por defecto para las llaves generadas, `id_rsa` y `id_rsa.pub`.

- `id_ rsa` es la llave privada que usted y solo usted debe tener para conectarse al servidor.
- `id_rsa.pub` es la llave pública que deberá tener el servidor.

Nuestro servicio de VPS permite que desde el despliegue usted provea esta llave pública (id_rsa.pub) y automáticamente esta sea insertada en `/home/nombre_usuario/.ssh/authorized_keys` que tiene el rol de mantener la lista de llaves autorizadas a iniciar sesión usando **SSH**.

- ✓ **Opciones para el Demonio del servicio SSH**

Es aconsejable **desactivar el inicio de sesión del usuario *"root"*** por el servicio **SSH**. Esto requiere el inicio de sesión por **SSH** usando cualquier otro usuario diferente a **"*root*"**. Una vez que un usuario con permisos limitados se conecte puede ejecutar tareas que requieren privilegios elevados usando el comando `$: sudo` o puede cambiar al SHELL de **"*root*"** usando el comando `$: su -`.

El demonio del servicio SSH es configurable haciendo cambios en el fichero `/etc/ssh/sshd_config`.

/etc/ssh/sshd_config

```
# Authentication:
...
PermitRootLogin no
```

Es aconsejable **desactivar el inicio de sesión por usuario y contraseña** si está usando llave criptográfica. Si usted escoge hacerlo desde el momento de despliegues este cambio se ejecutará automáticamente durante el proceso de provisión del VPS.

/etc/ssh/sshd_config

```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no
```

Si realizo algún cambio en la configuración del demonio de **SSH** usted debe reiniciarlo para que los cambios surtan efecto.

```
$: sudo systemctl restart sshd
```

- ✓ **Use Fail2Ban para proteger el inicio de sesión por servicio SSH**

Fail2Ban es una aplicación que banea las direcciones IPs que hacen muchos intentos de conexión por el protocolo **SSH**, es completamente configurable y extensible a mas que el protocolo **SSH**, actualmente se integra con más aplicaciones cada día. Es una herramienta muy útil para contrarrestar los ataques de fuerza bruta que se perpetren contra su VPS. Al desplegar el VPS este ya viene configurado solo para el servicio **SSH** desde el proceso de provisión. Puede encontrar su configuración bajo el directorio `/etc/fail2ban/`.

- ✓ **Elimine los servicios expuestos a internet y no utilice**

Desde que se instancia la provisión de su VPS usted será dueño del Sistema Operativo que se desplego y es una buena práctica deshabilitar los servicios que innecesariamente se encuentran expuestos hacia internet. Obligatoriamente usted tendrá que convivir con el servicio **SSH** ya que es su modo de acceso remoto, pero puede encontrar que en ocasiones existen otros servicios que se encuentran escuchando en puertos aceptando conexiones externas.

Una buena forma de encontrar estos servicios es ejecutando en el VPS el comando:

```
$: sudo ss -atpu
```

**Nota:** Existen 2 procesos java que corren contra una dirección privada **172.27.6.23:https** que no deben eliminarse y deben permanecer intactos para garantizar el correcto funcionamiento del VPS.

- ✓ **Configure el Cortafuego de su distribución**

Usar el cortafuegos para bloquear el tráfico de entrada no deseado al VPS le provee una capa de seguridad muy efectiva. Siendo muy específico en cuanto al tráfico que desea permitir de entrada, usted prevendrá muchos ataques y evitará intrusiones no deseadas. Las mejor practica en el uso de cortafuegos es denegar todo el tráfico y permitir solo lo necesario. Los VPS se desplegarán con el Cortafuegos habilitado y solo permitiendo el servicio **SSH** de entrada.

- FirewallD es el cortafuegos usado en los VPS basados en CentOS.

- UFW es el cortafuegos usado en los VPS basados en Ubuntu.

- ✓ **Como debo proceder si haciendo cambios me quede fuera del VPS**

Si por cualquier razón se encuentra que no se puede conectar a su VPS por medio de **SSH**, existe una vía por la cual usted puede acceder al despliegue sin necesidad de este protocolo.

- Usted puede acceder a su VPS desplegado por la consola de administración fuera de banda que se provee en el portal de administración. Y que se detalla al principio de esta guía.
- Usted puede una vez conectado revertir los cambios realizados en el fichero de configuración del demonio de **SSH** para habilitar nuevamente el inicio de sesión por contraseña y/o el inicio usando el usuario ***"root"***.

/etc/ssh/sshd_config

```
# Authentication:
...
PermitRootLogin yes
...
PasswordAuthentication yes
```

Si realizo algún cambio en la configuración del demonio de **SSH** usted debe reiniciarlo para que los cambios surtan efecto.

```
$: sudo systemctl restart sshd
```

- Si usted desea eliminar o modificar la llave publica que inserto en el VPS, edite el fichero que se encuentra `/home/nombre_usuario/.ssh/autorized_keys` o si no lo necesita puede borrarlo usando:

```
$: rm ~/.ssh/authorized_keys
```