**GERENCIA DE SISTEMAS  
INFORME / NOTIFICACIÓN INTERNA**

**INFINT-13122022-JZ-00003-Informe SRV Host SERVER**

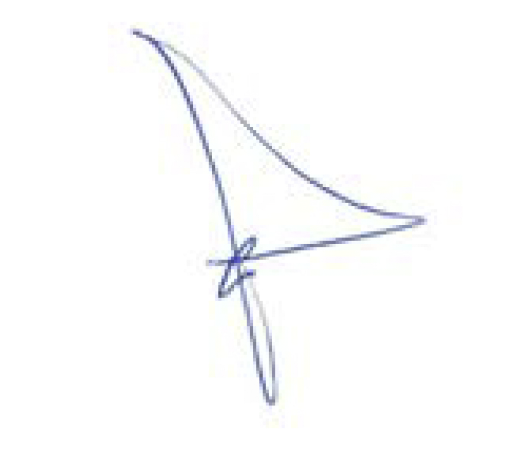
|  |  |  |
| --- | --- | --- |
| **DE:** | Julián Marcelo Zappia | |
| **A:** | Ing. Juan Julián Callegari | Gerente IT | |
| **FECHA:** | 13 de Diciembre de 2022 | |
| **Breve descripción del asunto:** | Informe de Análisis General de Servidor de Red host “SERVER”. | |
| **Autoriza: --** | **Sector: GERENCIA IT** | **Asignado a:** |
|  |  |  |

**INFORME / NOTIFICACIÓN**

De mi mayor consideración:

Por intermedio del presente, me dirijo a Ud. respetuosamente a efectos de informar análisis general realizado sobre servidor de red Windows Server 2012 R2 Standard, host “SERVER” (físico).

Sin más, lo saludo atte.



Julián Marcelo Zappia  
Administrador de Sistemas

Limpiolux S.A.

**ANÁLISIS DE SERVIDOR DE RED. HOST “SERVER” (FÍSICO).**

**server.limpiolux.local**

**Unidades de disco.**

El servidor físico server.limpiolux.local se encuentra 100% virtualizado. Como le comenté verbalmente en el día de ayer, sinceramente no entiendo la necesidad de realizar tal acción, como tampoco la comparto plenamente.

La arquitectura de un servidor físico es bastante simple. Cada servidor tiene su propio hardware: recursos de memoria, red, procesamiento y almacenamiento. En este hardware, el sistema operativo del servidor está cargado. Desde el SO se pueden ejecutar las aplicaciones. Muy claro.

Con una infraestructura virtual, se tiene el mismo que un servidor físico con todos los recursos, pero en lugar del sistema operativo del servidor, hay un hipervisor como vSphere, VMWARE o Hyper-V (entre otros) ejecutándose en él.

Los beneficios de la virtualización son obvios: En lugar de tener solo una aplicación por servidor, ahora puede ejecutar varios sistemas operativos “Guest” y una serie de aplicaciones con el mismo hardware físico. La virtualización es muy rentable, muchísimo más que el hardware físico.

Una máquina virtual puede ser portátil en máquinas físicas que ejecutan el mismo hipervisor. Cada máquina virtual tiene su propio hardware virtual. Por lo que el sistema operativo “Invitado” cargado en una VM solo conoce esta configuración del hardware y no la del servidor físico.

En otras palabras, una VM es completamente independiente del hardware. El sistema operativo instalado en una VM ya no está vinculado a un determinado hardware, y así pueden moverse fácilmente máquinas virtuales desde un servidor físico a otro.

Esto hace que las VM sean absolutamente portátiles Puede copiarse a una unidad flash, es “transportable” y replicable.

**Características extra de las máquinas virtuales.**

Una de las características clave de la virtualización, como expresé anteriormente, es la portabilidad de máquinas virtuales, que es posible gracias a la independencia de hardware.

Permite migrar fácilmente una VM a cualquier sitio que desee: Es posible realizar copias de respaldo y restaurarla en otro servidor, puede colocarse en una unidad flash como también existen muchas características útiles creadas a partir de la independencia de hardware y la portabilidad de VM:

vMotion es una tecnología de VMware que otorga portabilidad de VM e independencia de hardware, permitiendo a una VM en ejecución migrar de un servidor a otro sin tiempo de inactividad para el usuario final.

Distributed Resource Scheduler (o DRS, por sus siglas en inglés), también de VMware, permite equilibrar la infraestructura virtual en el aspecto del consumo de recursos.

DRS puede mover una VM en ejecución desde un host a otro (mediante vMotion) para poder brindarle todos los recursos que necesita para funcionar con eficacia.

VMware High Availability (o VMHA, por sus siglas en inglés) es una opción que le permite restaurar VM desde un servidor fallido a otro para que pueda volver a ejecutarla de inmediato.

Distributed Power Management (o DPM, por sus siglas en inglés) es otra excelente característica de VMware que puede ayudar a reducir el consumo de energía. Con esta característica, puede mantenerse bajo control el consumo de energía de la infraestructura.

DPM consolida a las VM en menos servidores físicos cuando el consumo de recursos en la infraestructura virtual es bajo. Mientras tanto, aquellos servidores que no sean necesarios se desactivarán.

La virtualización también facilita la recuperación ante desastres. Gracias a la independencia de hardware, si una VM dentro de su infraestructura virtual falla, puede ejecutar las VM a las que se les realizó un backup en cualquier servidor ya que los sistemas operativos “Guest” ya no están vinculados al hardware.

Sin embargo, para aprovechar al máximo esta funcionalidad que otorga la virtualización, deberían usarse las herramientas adecuadas para el monitoreo, la administración y, por supuesto, la protección de datos.

Dado que las máquinas virtuales difieren notablemente de los servidores físicos, las herramientas designadas para estos últimos no sirven para las primeras. Esto aplica en especial para las copias de respaldo; por esto, el nacimiento de Veeam, una solución de copias de respaldo muy confiable.

*Pero en la infraestructura de Limpiolux S.A., basándome en los análisis realizados en mis pocos días de desempeño como Administrador de Sistemas, no existe implementación de nada de lo mencionado anteriormente.*

**Ventajas de los servidores físicos.**

* Más seguridad.
* Mejor control de la temperatura.
* Centralización de las gestiones de los usuarios y contraseñas.
* Reduce el número de credenciales dentro de la red.
* Establece políticas en los ordenadores Windows
* Es más fácil gestionar las copias de seguridad.
* Brinda exclusividad.
* Administración.
* Seguridad.
* Mantenimiento.
* Versatilidad.
* Sistema Operativo.

**Desventajas de los servidores físicos.**

* Los servidores físicos son más costosos que los virtuales.
* Estos servidores suelen ser gestionados mediante paneles de control, pero siempre es recomendable tener conocimientos previos acerca de estos paneles de control.
* Si se decide optar por los físicos siempre recomiendo sobre la efectividad de las medidas de seguridad.

**Ventajas de los Servidores virtuales.**

* Las instalaciones se pueden simplificar de tal manera que puedes ahorrar espacio, tiempo y dinero.
* Su gestión es centralizada y es compatible con todas las aplicaciones.
* Tiene mayor disponibilidad y recuperación en caso de que ocurra un desastre.
* Posee una capacidad superior de ejecutar copias de seguridad y además puede utilizar muchos entornos de sistemas operativos en la misma computadora.
* Por otra parte, tiene acceso controlado a datos confidenciales y propiedad intelectual, manteniéndolos seguros dentro del centro de datos.
* Mejor uso de los espacios.
* Tiene una mejor utilización del hardware.

**Desventajas de las VM.**

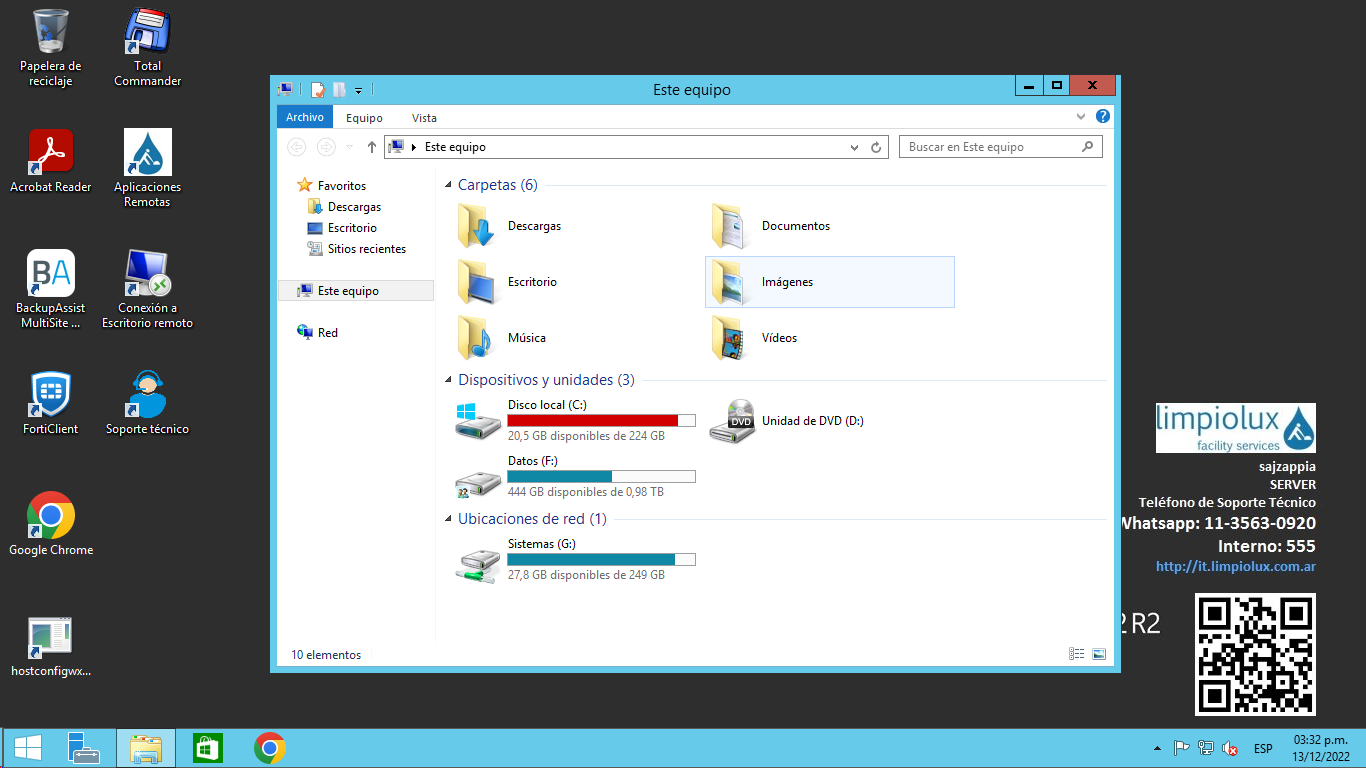
* Si los servidores virtuales se desconectan todos los servicios y aplicaciones alojadas se cerrarán, por lo tanto, la Empresa deberá configurar un grupo de servidores físicos de respaldo.
* La administración de estos servidores debe ser monitoreados exclusivamente a través de máquinas virtuales.
* Cuando varios equipos virtuales se están ejecutando en el mismo host. el rendimiento por lo general se ve afectado.
* Gran consumo de RAM, ya que cada VM ocupa un área separada de la misma.
* Los servidores virtuales requieren de múltiples enlaces en una cadena que deben trabajar juntos de manera coherente.
* Por último, tenemos un gran uso del espacio en un disco, porque toma los archivos para cada sistema operativo instalado en cada VM.

**Espacio de almacenamiento disponible en limpiolux.local.**

Disco C: (Sistema): 20,5 GB libres (aproximadamente entre 10% y 15% del tamaño asignado).

Disco F: (Datos): disponibilidad aproximada del 40% (poco más de 440 GB).

Disco G: (Sistemas): casi 28 GB libres (entre 10-15% del espacio asignado).



**Firewall de Windows.**

Si bien la protección de Fortinet es correcta, la configuración completa del Firewall de Windows se encuentra desactivada. Por el momento, no se comprende el motivo.

Todas las redes del servidor analizado se encuentran sin protección; la red local, de dominio y pública están completamente liberadas.

Una captura de pantalla de una computadora

Descripción generada automáticamente

Una captura de pantalla de una computadora

Descripción generada automáticamente

Una captura de pantalla de una computadora

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Dispositivos e impresoras.**

No evaluados en el presente análisis, si bien podría existir algún tipo de redundancia en base a los altos resultados de tiempo y timeout de “Ping”. Es necesario un análisis funcional y presencial para poder afirmarlo.

Una captura de pantalla de una computadora

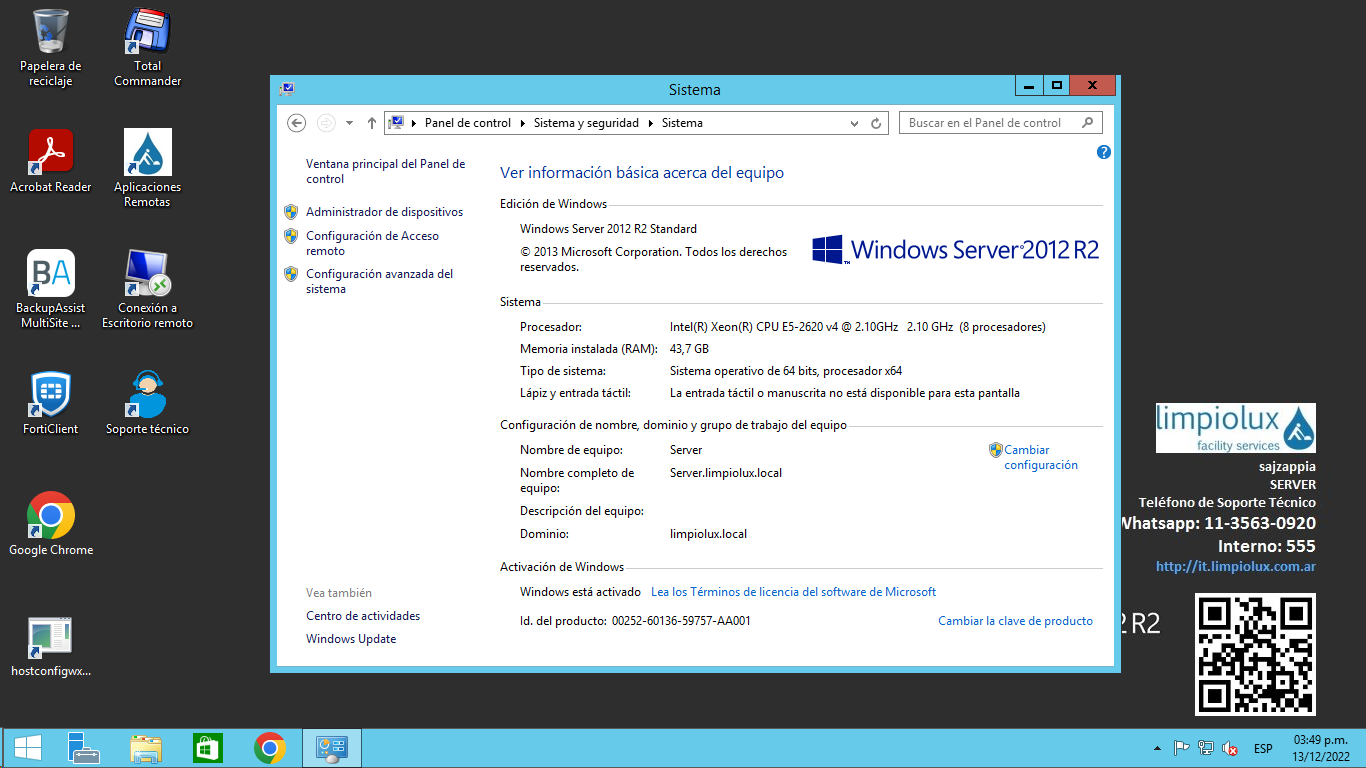
Descripción generada automáticamente

Captura de pantalla de computadora

Descripción generada automáticamente

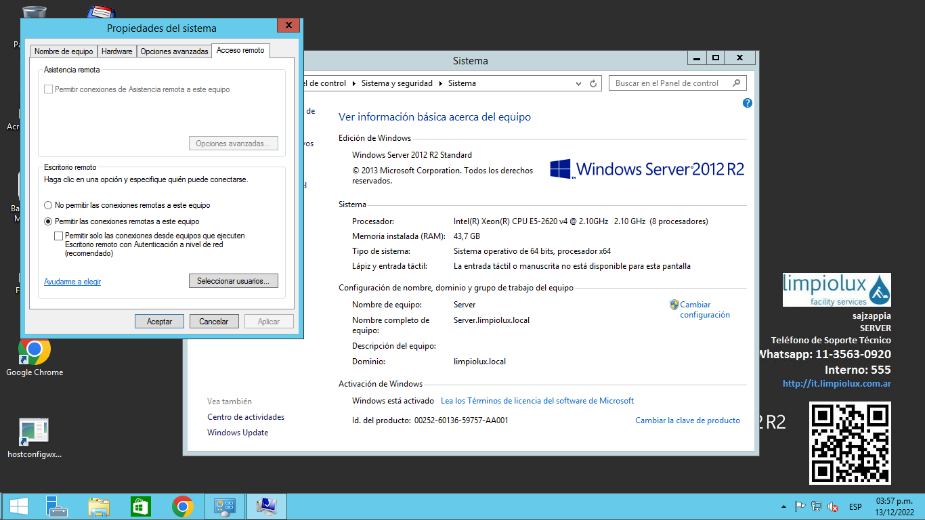
**Sistema.**

No hay comentarios por el momento; pero debido a evaluaciones de rendimiento y capacidad de uso, sería necesaria la ampliación de su memoria y discos. La instalación podría presentar inconsistencias.

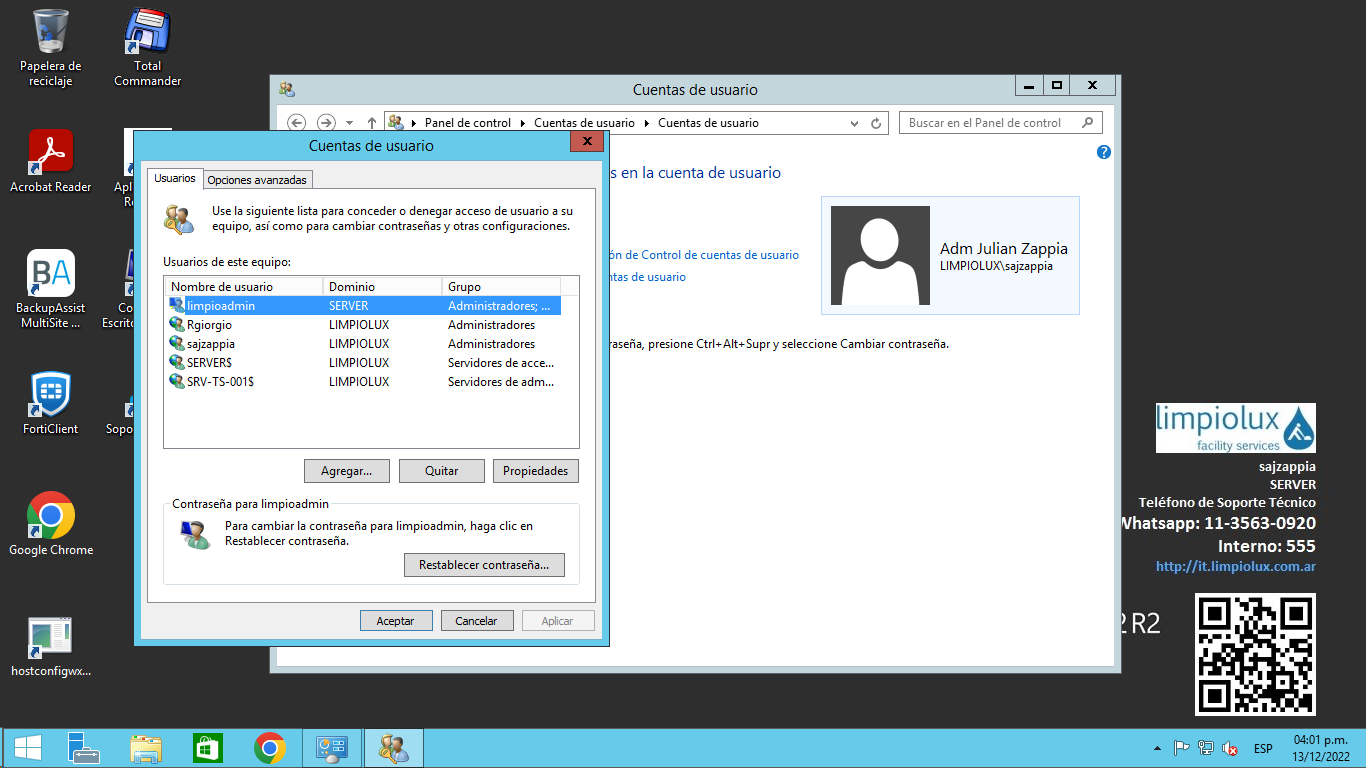


**Acceso remoto.**

Permitido para todo usuario.



**Cuentas de usuario definidas.**



**Advertencias del servidor.**

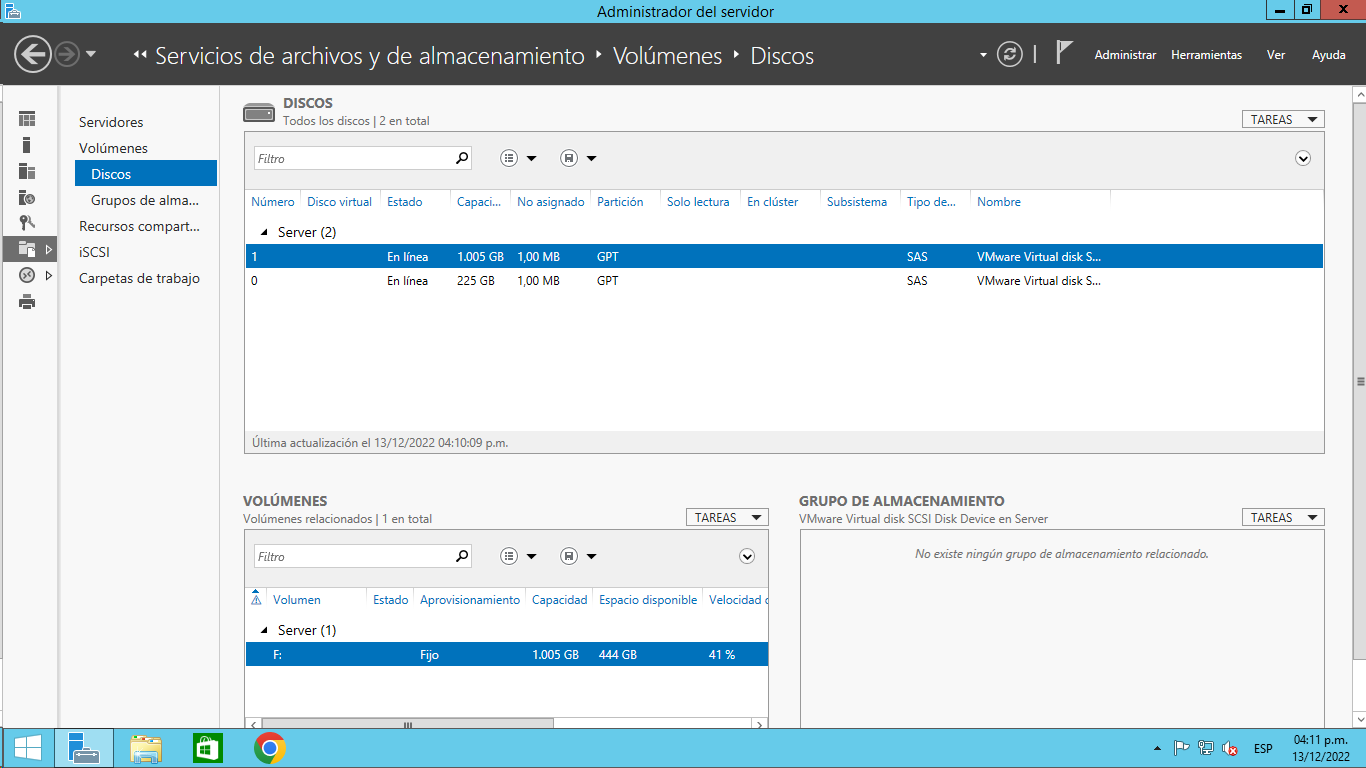
Importante cantidad de advertencias del servicio Group Policy Services relacionados con la configuración de Fortinet VPN. Esto podría haber ocurrido previo a la caída de los accesos ocurridos en el día de la fecha, o en momentos posteriores. Se desconoce el motivo de la incidencia. A simple vista, podría ser una caída del servicio, o un reinicio del servidor no notificado.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Volúmenes / Discos.**

Por el momento, se concluye escasa cantidad de espacio disponible en los volúmenes del servidor analizado.



Perfiles de usuario con múltiples errores.

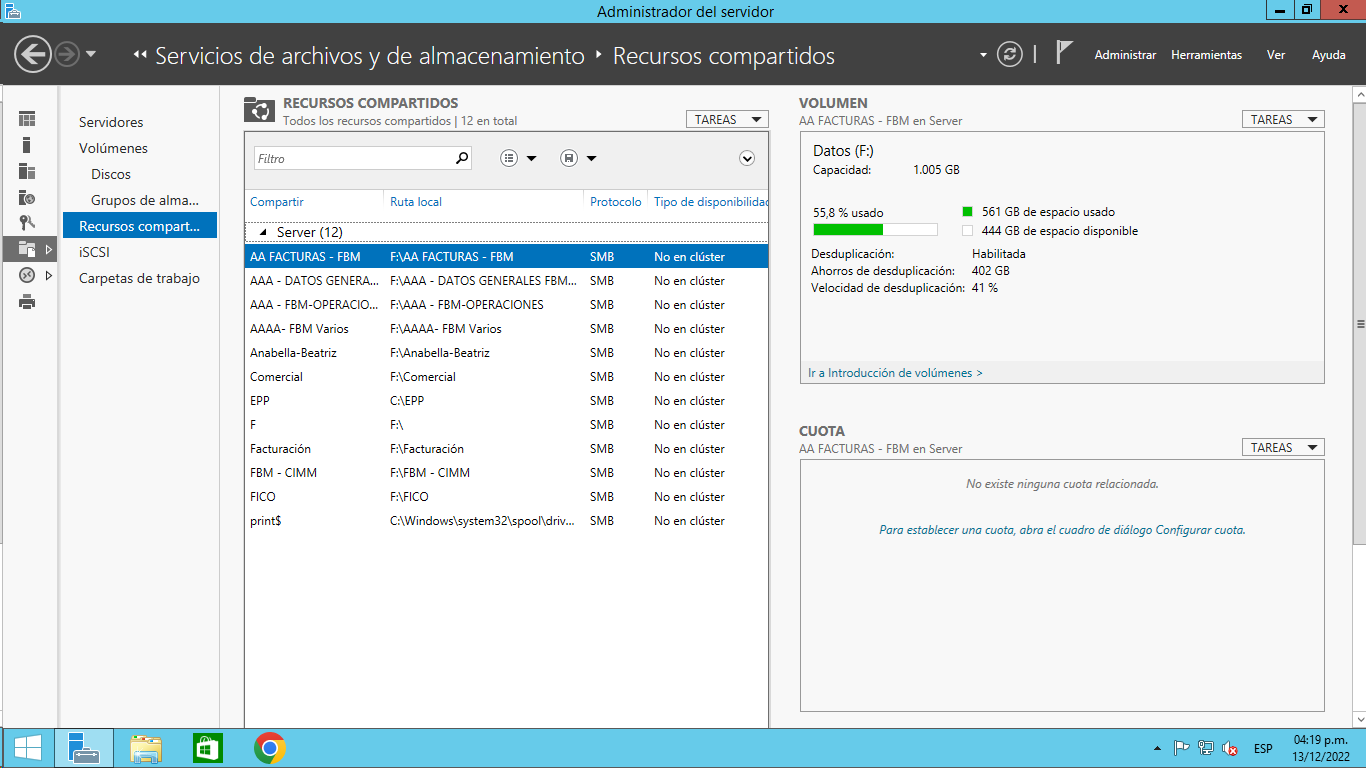
Se han observado perfiles de usuario de “Cuentas desconocidas”; podría ser producto de un fallo del sistema, de un error de almacenamiento en disco o de eliminación de perfiles directamente desde su carpeta compartida.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

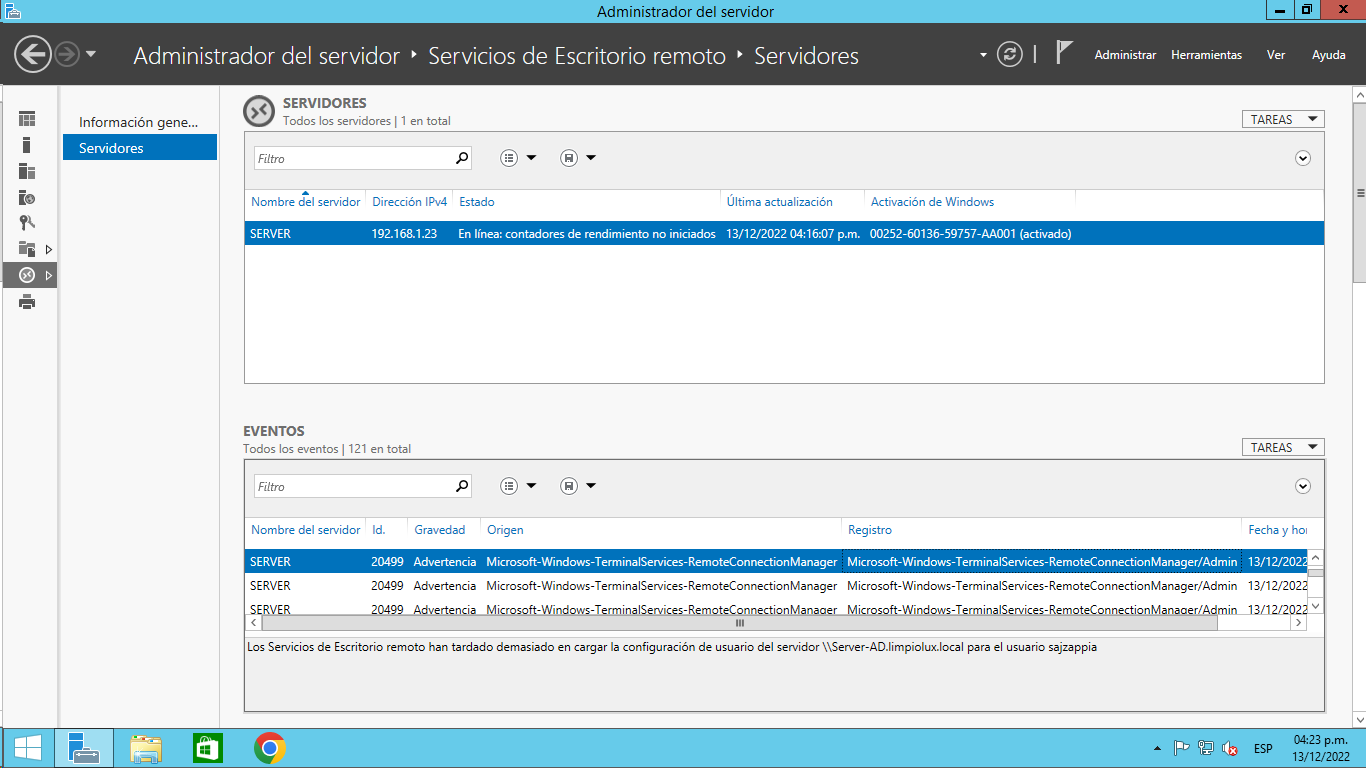
**Recursos compartidos.**

Muchos no se comprenden debido a su denominación (por ejemplo “//AAAAAA…”). Se verificarán en análisis funcional.



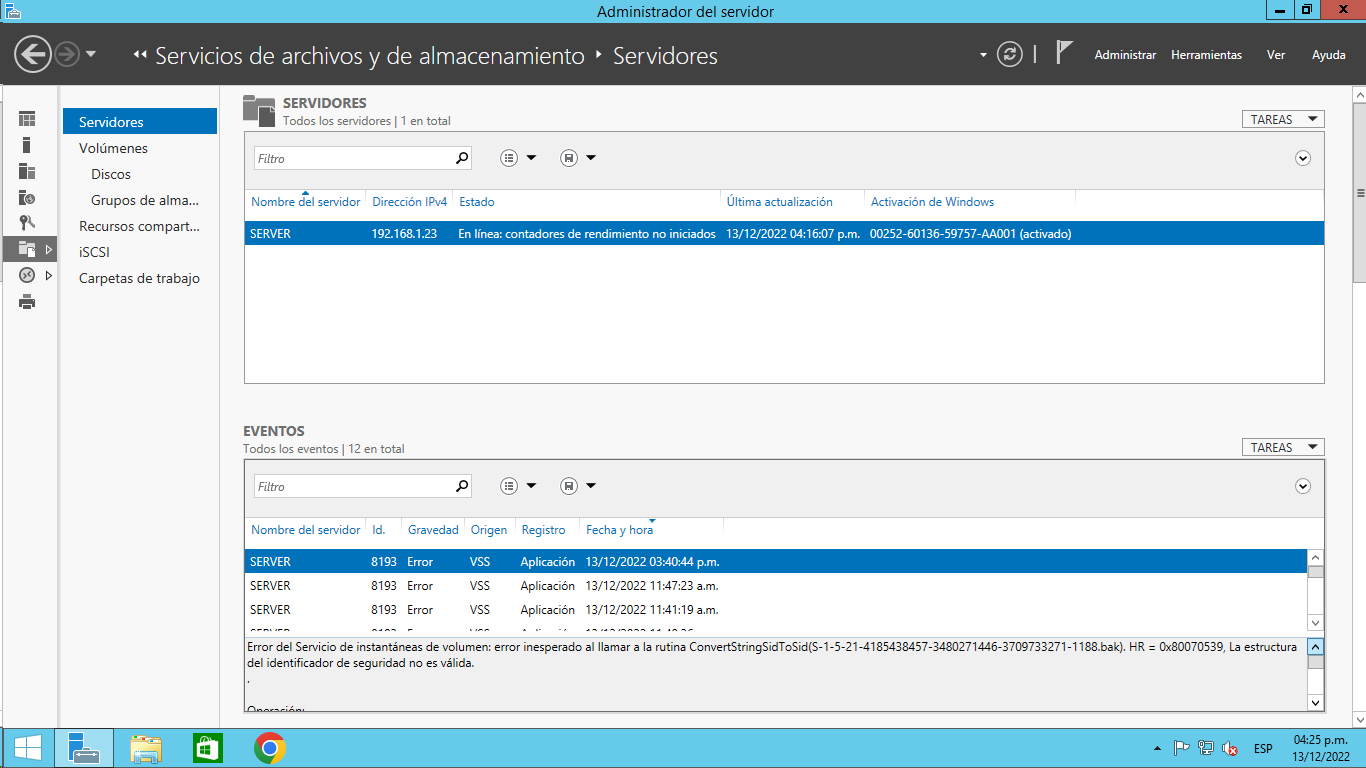
**Advertencias del Servicio de Escritorio Remoto.**

Múltiples advertencias del servicio Microsoft Windows Terminal Services. Podría ser una ocurrencia conjunta a lo mencionado al respecto del servicio Fortinet VPN.



**Errores en servicios de archivos y almacenamiento.**

Se han detectado, ya desde días atrás, errores reiterativos y no identificados de una rutina ConnectionString. Podría ser efecto de la implementación de sistema SAP y/o de sus bases de datos SQL que lo produce.



**Alta exigencia, caídas de rendimiento con consecuentes picos de consumo de recursos.**

**Interfaz de usuario gráfica, Texto, Aplicación

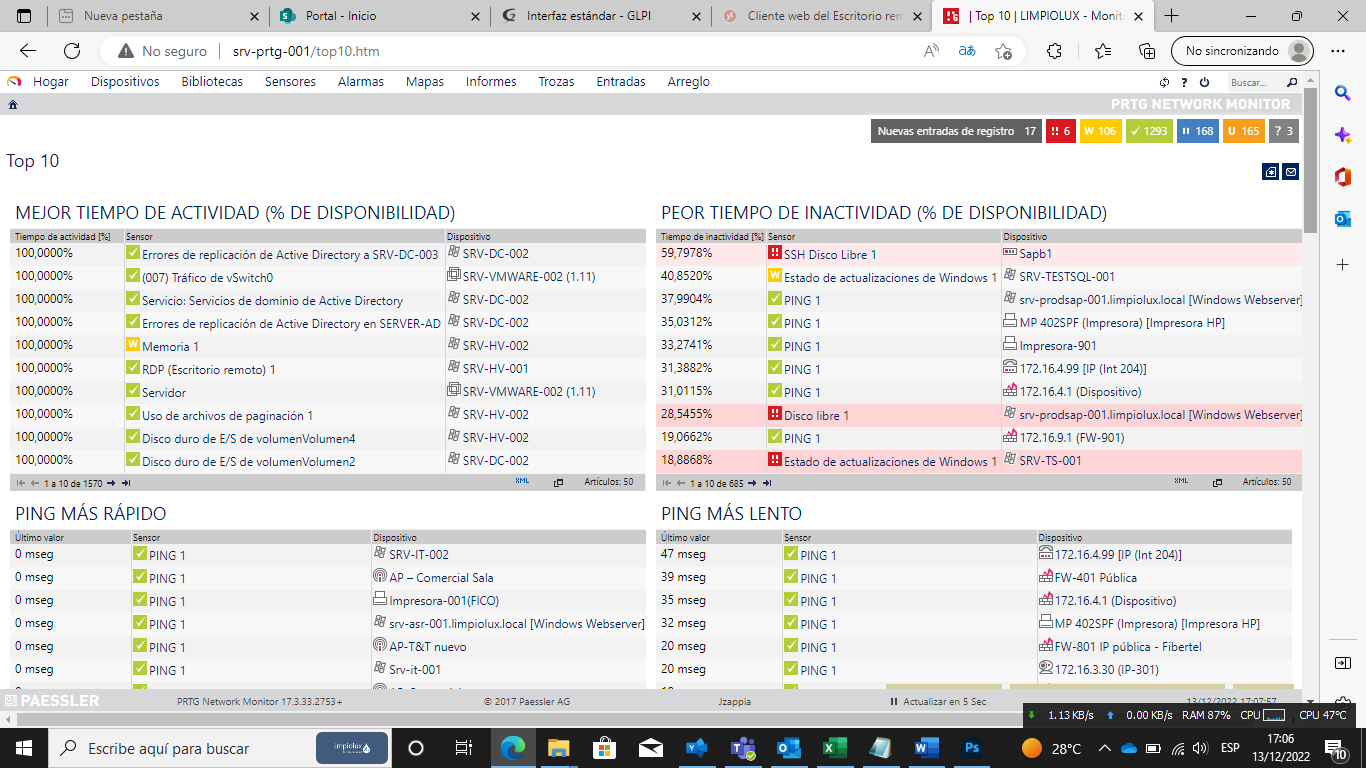
Descripción generada automáticamente**

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

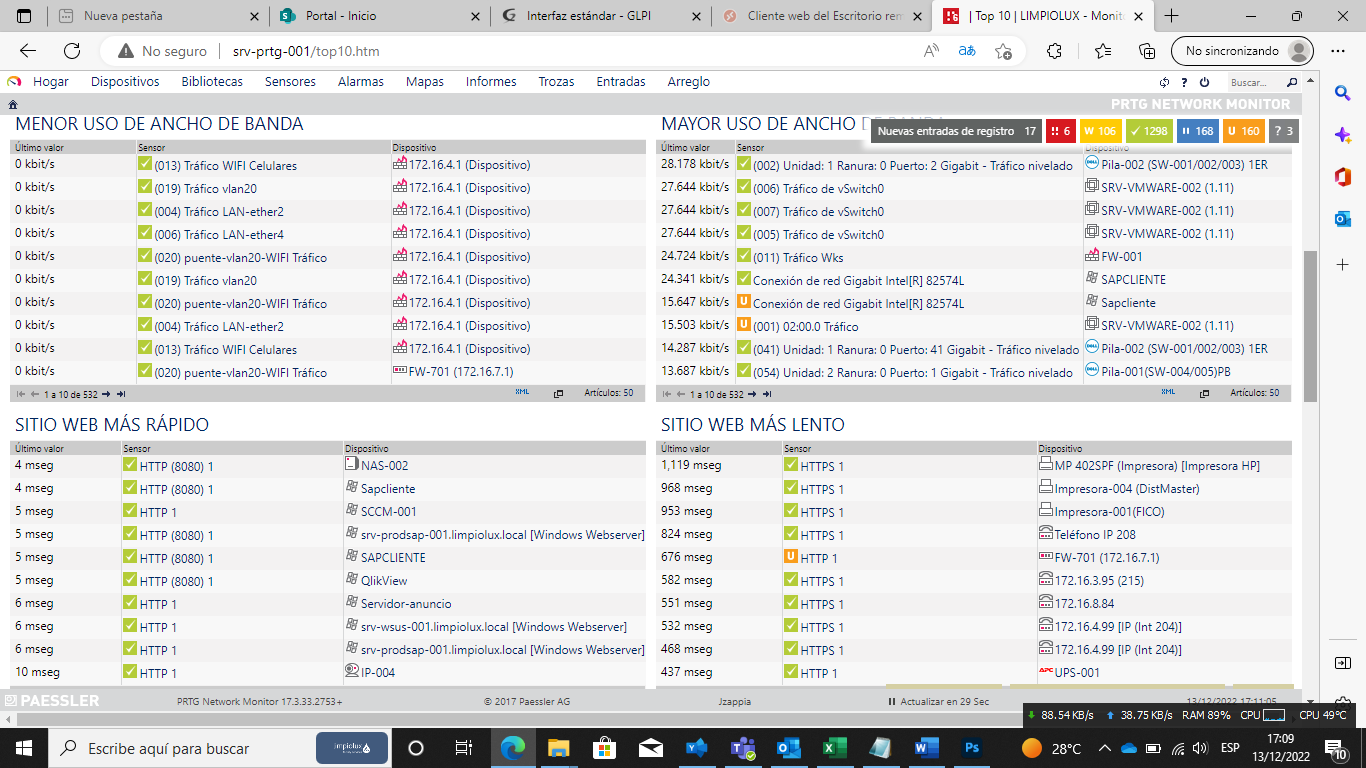
**PRTG Network Monitor con Alertas.**

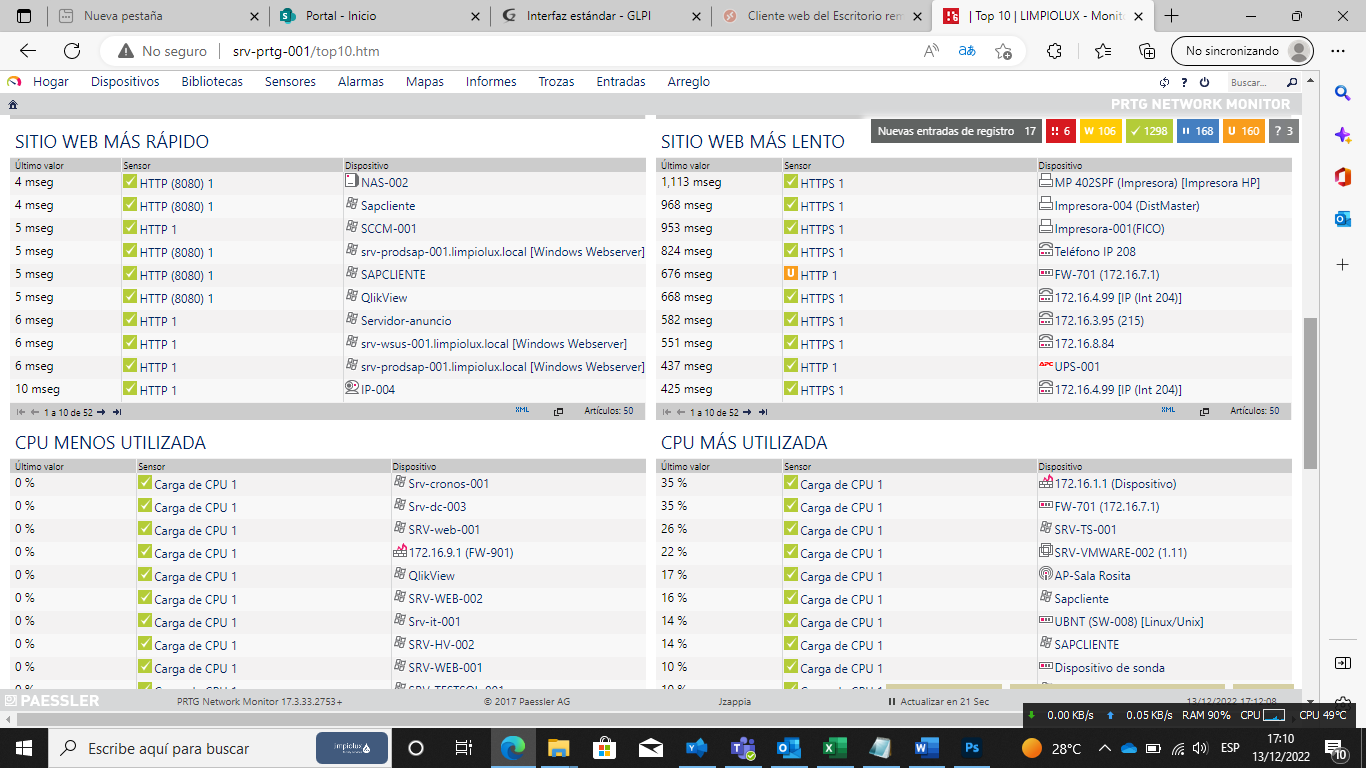
En software PRTG continúan alertas de alto consumo de espacio en disco, actualizaciones de Windows no implementadas, alto consumo de memoria, entre otros.



Una captura de pantalla de una computadora

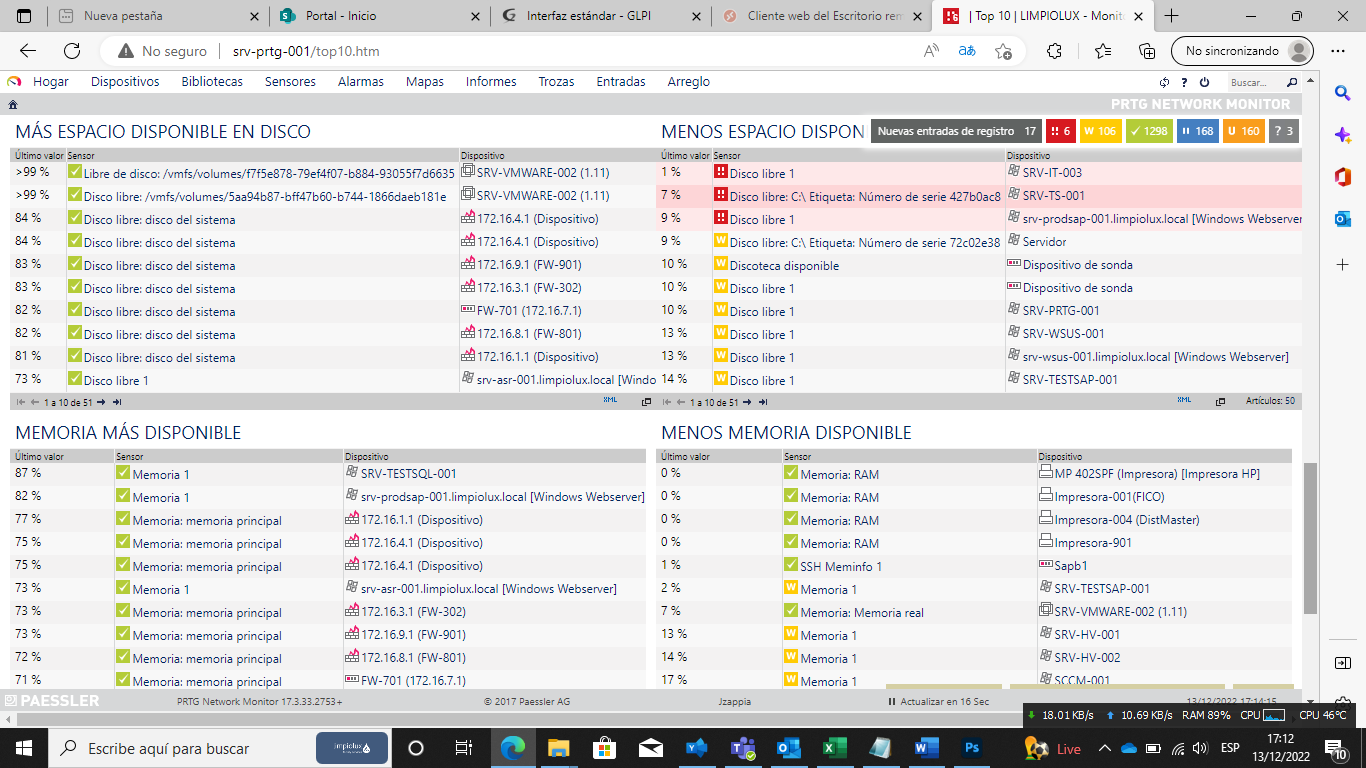
Descripción generada automáticamente





Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



**IPCONFIG.**

Configuraci¢n IP de Windows

Adaptador de Ethernet Ethernet 2:

Estado de los medios. . . . . . . . . . . : medios desconectados

Sufijo DNS espec¡fico para la conexi¢n. . :

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . . . . . . . : medios desconectados

Sufijo DNS espec¡fico para la conexi¢n. . :

Adaptador de Ethernet Ethernet0 2:

Sufijo DNS espec¡fico para la conexi¢n. . :

Direcci¢n IPv4. . . . . . . . . . . . . . : 192.168.1.23

M scara de subred . . . . . . . . . . . . : 255.255.0.0

Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de t£nel isatap.{E0C656D1-ADC0-421D-9865-98D9F9DC222F}:

Estado de los medios. . . . . . . . . . . : medios desconectados

Sufijo DNS espec¡fico para la conexi¢n. . :

**NETSTAT.**

Conexiones activas

Proto Direcci¢n local Direcci¢n remota Estado

TCP 127.0.0.1:51773 Server:51774 ESTABLISHED

TCP 127.0.0.1:51774 Server:51773 ESTABLISHED

TCP 127.0.0.1:54545 Server:54546 TIME\_WAIT

TCP 127.0.0.1:54555 Server:54556 TIME\_WAIT

TCP 127.0.0.1:54582 Server:54583 TIME\_WAIT

TCP 127.0.0.1:54584 Server:54585 TIME\_WAIT

TCP 127.0.0.1:54587 Server:54588 TIME\_WAIT

TCP 127.0.0.1:54608 Server:54609 TIME\_WAIT

TCP 127.0.0.1:54611 Server:54612 TIME\_WAIT

TCP 127.0.0.1:54619 Server:54620 TIME\_WAIT

TCP 127.0.0.1:54621 Server:54622 ESTABLISHED

TCP 127.0.0.1:54622 Server:54621 ESTABLISHED

TCP 192.168.1.23:445 srv-prodsap-001:58806 ESTABLISHED

TCP 192.168.1.23:445 SRV-SIAP-001:65260 ESTABLISHED

TCP 192.168.1.23:445 SRV-IT-004:59765 ESTABLISHED

TCP 192.168.1.23:445 srv-veeam-002:56250 ESTABLISHED

TCP 192.168.1.23:445 WKS-008:62546 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.1:49910 ESTABLISHED

TCP 192.168.1.23:445 NB-033:64039 ESTABLISHED

TCP 192.168.1.23:445 NB-149:59374 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.5:64287 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.7:50499 ESTABLISHED

TCP 192.168.1.23:445 NB-155:62378 ESTABLISHED

TCP 192.168.1.23:445 NB-108:49774 ESTABLISHED

TCP 192.168.1.23:445 NB-015:55414 ESTABLISHED

TCP 192.168.1.23:445 NB-044:65491 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.13:54203 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.14:62481 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.15:50299 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.16:52285 ESTABLISHED

TCP 192.168.1.23:445 NB-100:56201 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.21:54012 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.24:56074 ESTABLISHED

TCP 192.168.1.23:445 NB-189:59156 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.28:63307 ESTABLISHED

TCP 192.168.1.23:445 NB-103:56195 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.30:58035 ESTABLISHED

TCP 192.168.1.23:445 NB-134:50974 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.36:51482 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.37:57767 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.38:62441 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.39:65140 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.40:59230 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.41:60741 ESTABLISHED

TCP 192.168.1.23:445 NB-116:50899 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.43:57713 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.44:64463 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.46:53855 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.51:58136 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.52:55025 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.53:53082 ESTABLISHED

TCP 192.168.1.23:445 NB-045:63148 ESTABLISHED

TCP 192.168.1.23:445 NB-117:54736 ESTABLISHED

TCP 192.168.1.23:445 NB-048:65362 ESTABLISHED

TCP 192.168.1.23:445 172.30.22.71:64546 ESTABLISHED

TCP 192.168.1.23:445 Server-AD:50809 ESTABLISHED

TCP 192.168.1.23:445 SRV-DC-002:52153 ESTABLISHED

TCP 192.168.1.23:445 srv-prtg-001:63446 ESTABLISHED

TCP 192.168.1.23:445 srv-wsus-001:49310 ESTABLISHED

TCP 192.168.1.23:445 SRV-TS-001:62275 ESTABLISHED

TCP 192.168.1.23:445 192.168.50.146:56329 ESTABLISHED

TCP 192.168.1.23:445 NB-116:49756 ESTABLISHED

TCP 192.168.1.23:445 WKS-016:56005 ESTABLISHED

TCP 192.168.1.23:445 NB-018:62721 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.7:51459 ESTABLISHED

TCP 192.168.1.23:3389 NB-015:49906 ESTABLISHED

TCP 192.168.1.23:3389 NB-044:62424 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.13:52983 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.21:53807 ESTABLISHED

TCP 192.168.1.23:3389 NB-189:60893 ESTABLISHED

TCP 192.168.1.23:3389 NB-218:51549 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.36:51513 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.39:65178 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.40:60245 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.41:59075 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.52:55126 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.54:62080 ESTABLISHED

TCP 192.168.1.23:3389 NB-045:49774 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.56:63512 ESTABLISHED

TCP 192.168.1.23:3389 NB-117:51010 ESTABLISHED

TCP 192.168.1.23:3389 NB-048:54617 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.71:64555 ESTABLISHED

TCP 192.168.1.23:3389 172.30.22.73:50680 ESTABLISHED

TCP 192.168.1.23:3389 NB-170:63556 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:51576 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:52731 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:53443 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:55746 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:57007 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:58416 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:58443 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:58643 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:58667 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:59411 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:61302 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:62239 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:62660 ESTABLISHED

TCP 192.168.1.23:3389 SRV-TS-001:63198 ESTABLISHED

TCP 192.168.1.23:49155 srv-prtg-001:64112 ESTABLISHED

TCP 192.168.1.23:49227 SRV-TS-001:49728 ESTABLISHED

TCP 192.168.1.23:49508 40.102.34.194:https ESTABLISHED

TCP 192.168.1.23:50519 52.114.132.55:https ESTABLISHED

TCP 192.168.1.23:50651 whatsapp-cdn-shv-01-eze1:https ESTABLISHED

TCP 192.168.1.23:50845 52.114.132.17:https ESTABLISHED

TCP 192.168.1.23:50960 192.168.51.93:8008 ESTABLISHED

TCP 192.168.1.23:50986 ce-in-f188:5228 ESTABLISHED

TCP 192.168.1.23:51009 52.97.2.130:https ESTABLISHED

TCP 192.168.1.23:51538 40.102.34.194:https ESTABLISHED

TCP 192.168.1.23:51776 srv-asr-001:9443 ESTABLISHED

TCP 192.168.1.23:51845 192.168.51.93:8008 ESTABLISHED

TCP 192.168.1.23:51868 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:51878 52.115.92.12:https ESTABLISHED

TCP 192.168.1.23:52379 srv-prodsap-001:8100 ESTABLISHED

TCP 192.168.1.23:52926 Server-AD:microsoft-ds ESTABLISHED

TCP 192.168.1.23:53118 srv-dc-003:microsoft-ds ESTABLISHED

TCP 192.168.1.23:53245 52.111.225.2:https ESTABLISHED

TCP 192.168.1.23:53655 52.111.225.2:https TIME\_WAIT

TCP 192.168.1.23:53773 srv-it-001:microsoft-ds ESTABLISHED

TCP 192.168.1.23:53775 Qlikview:microsoft-ds ESTABLISHED

TCP 192.168.1.23:54229 SRV-PTR-001:49670 ESTABLISHED

TCP 192.168.1.23:54392 152.199.52.147:https TIME\_WAIT

TCP 192.168.1.23:54399 52.97.28.194:https TIME\_WAIT

TCP 192.168.1.23:54400 52.97.28.194:https TIME\_WAIT

TCP 192.168.1.23:54402 52.97.28.194:https TIME\_WAIT

TCP 192.168.1.23:54541 srv-dc-003:epmap TIME\_WAIT

TCP 192.168.1.23:54542 srv-dc-003:49667 TIME\_WAIT

TCP 192.168.1.23:54551 52.109.108.96:https ESTABLISHED

TCP 192.168.1.23:54557 Server-AD:epmap ESTABLISHED

TCP 192.168.1.23:54558 Server-AD:49672 ESTABLISHED

TCP 192.168.1.23:54563 20.189.173.10:https ESTABLISHED

TCP 192.168.1.23:54570 52.97.28.194:https TIME\_WAIT

TCP 192.168.1.23:54571 20.189.173.10:https TIME\_WAIT

TCP 192.168.1.23:54576 52.109.108.25:https TIME\_WAIT

TCP 192.168.1.23:54579 srv-dc-003:epmap TIME\_WAIT

TCP 192.168.1.23:54580 srv-dc-003:49667 TIME\_WAIT

TCP 192.168.1.23:54589 98:https TIME\_WAIT

TCP 192.168.1.23:54590 52.104.88.39:https TIME\_WAIT

TCP 192.168.1.23:54594 srv-dc-003:epmap TIME\_WAIT

TCP 192.168.1.23:54595 srv-dc-003:49667 ESTABLISHED

TCP 192.168.1.23:54596 srv-prodsap-001:8100 TIME\_WAIT

TCP 192.168.1.23:54597 srv-prodsap-001:8100 ESTABLISHED

TCP 192.168.1.23:54602 srv-wsus-001:8530 ESTABLISHED

TCP 192.168.1.23:54605 srv-asr-001:https TIME\_WAIT

TCP 192.168.1.23:54606 srv-dc-003:49667 TIME\_WAIT

TCP 192.168.1.23:54614 73-145-30-181:https ESTABLISHED

TCP 192.168.1.23:54615 a23-55-76-39:https ESTABLISHED

TCP 192.168.1.23:54618 srv-wazuhmanager-001:1514 SYN\_SENT

TCP 192.168.1.23:54623 srv-asr-001:9443 ESTABLISHED

TCP 192.168.1.23:54631 40.102.32.146:https ESTABLISHED

TCP 192.168.1.23:54766 52.97.3.130:https ESTABLISHED

TCP 192.168.1.23:56784 52.109.108.63:https ESTABLISHED

TCP 192.168.1.23:57154 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57177 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57227 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57233 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57235 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57260 192.168.51.93:8008 ESTABLISHED

TCP 192.168.1.23:57265 192.168.51.93:8009 ESTABLISHED

TCP 192.168.1.23:57299 40.102.33.226:https ESTABLISHED

TCP 192.168.1.23:59837 52.109.108.97:https TIME\_WAIT

TCP 192.168.1.23:61166 52.109.108.96:https ESTABLISHED

TCP 192.168.1.23:62568 52.114.128.84:https ESTABLISHED

TCP 192.168.1.23:63953 52.97.23.130:https TIME\_WAIT

TCP 192.168.1.23:64085 52.111.225.2:https ESTABLISHED

TCP 192.168.1.23:64971 52.109.108.97:https ESTABLISHED

TCP 192.168.1.23:65312 192.168.51.93:8008 ESTABLISHED

TCP [::1]:135 Server:49207 ESTABLISHED

TCP [::1]:445 Server:49336 ESTABLISHED

TCP [::1]:5504 Server:49330 ESTABLISHED

TCP [::1]:5504 Server:49334 ESTABLISHED

TCP [::1]:49207 Server:epmap ESTABLISHED

TCP [::1]:49330 Server:5504 ESTABLISHED

TCP [::1]:49334 Server:5504 ESTABLISHED

TCP [::1]:49336 Server:microsoft-ds ESTABLISHED

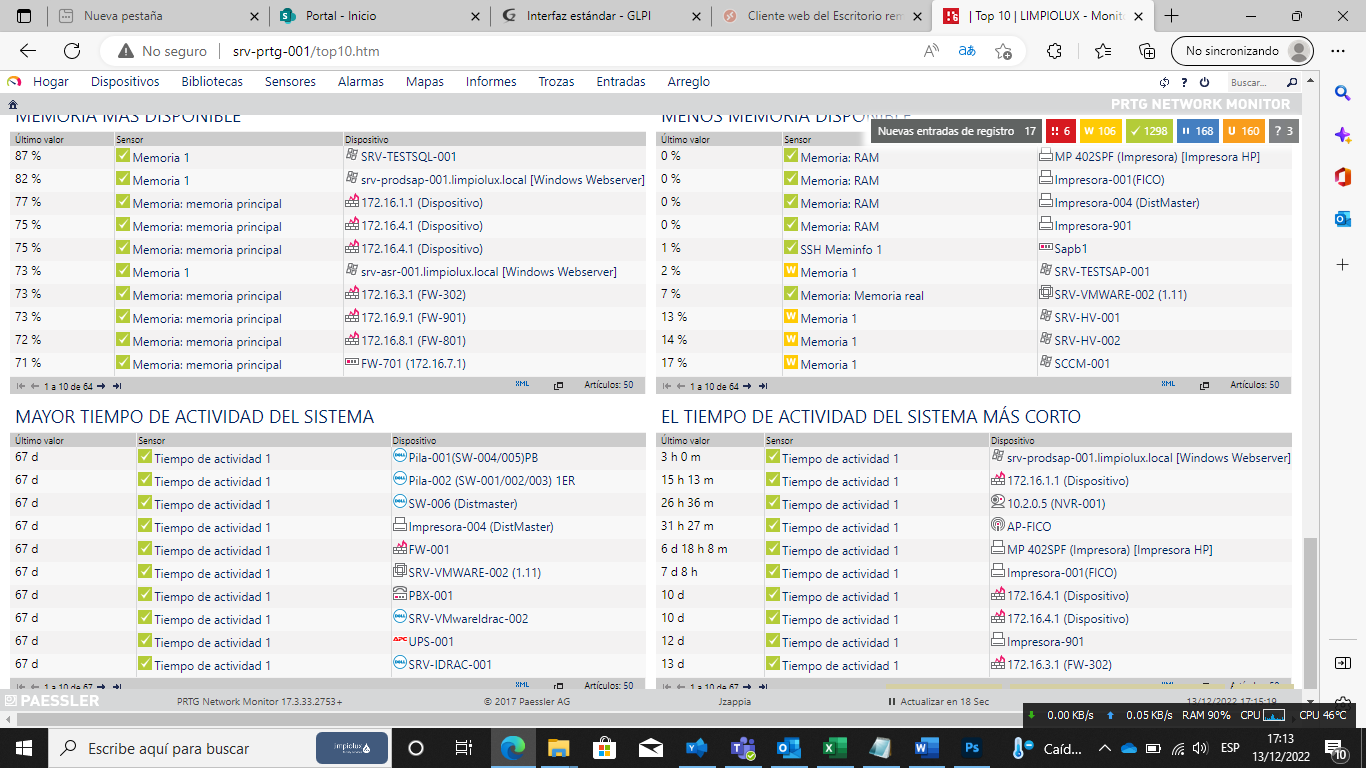
TCP [::1]:54772 Server:epmap TIME\_WAIT

**Conclusiones iniciales.**

Creo necesaria la necesidad de realizar las correspondientes acciones de mantenimiento preventivo / correctivo y configuraciones adicionales, intentando no alterar ni interrumpir el normal funcionamiento del sistema.

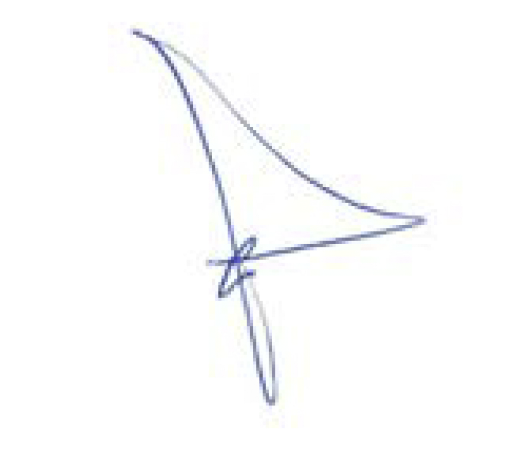
También, podría incluir ampliación de memoria RAM e inclusión de nuevas unidades de almacenamiento.

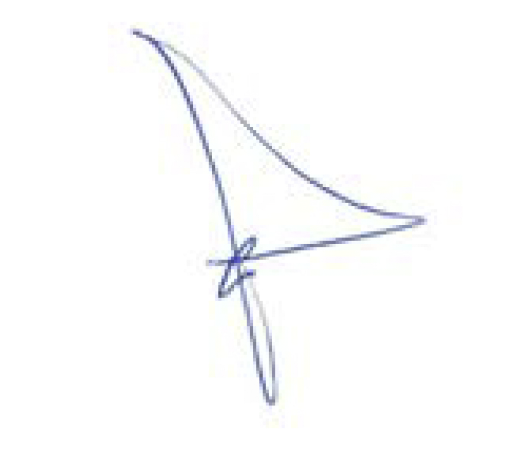
Las configuraciones de seguridad, tanto Firewall, acceso remoto, como también de usuarios y accesos a recursos compartidos, debería ser configurada previo análisis, todo a efectos de mejorar su rendimiento y estabilidad.



**Evaluaciones / Análisis pendientes.**

De acuerdo a listado obtenido realizado previamente por administración anterior, restaría la evaluación / análisis de 31 servidores.



Julián Marcelo Zappia  
Administrador de Sistemas  
Limpiolux S.A.