## How to vitalinux cliente AD.

**Escenario inicial:**

Se cuenta con un Dominio instalado en un servidor con Windows 2016 nivel funcional Windows 2016. (supongo que en versiones anteriores funcionará igualmente)

Un cliente vitalinux instalado. El cual tiene en su configuración de Red como DNS la IP del servidor mencionado.

**Referencias:**

El procedimiento que se describe a continuación está basado en la documentación que se encuentra en la Ubuntu Server Guide (lo he tomado para la versión 16.04, pero no cambia de la 14.04) )concretamente en el apartado de Autentificación de Redes -> SSSD and Active Directory

ver el enlace <https://help.ubuntu.com/lts/serverguide/sssd-ad.html>

A continuación comento en cada apartado del manual de Ubuntu los cambios o comentarios sobre cada paso.

**Pasos a seguir**

## Prerequisites, Assumptions, and Requirements

Revisar que se cumplan todos los requerimientos, como estoy haciendo la prueba sobre un dominio recién instalado no hay ningún problema.

En este paso sobre todo comprobar que la resolución de nombres desde el cliente la realiza el servidor.

Lo mas sencillo es un ping a iespiramide.es (nombre del domino). con esta comprobación suele bastar. Nos tendría que contestar el Servidor de AD.

También es importante comprobar la hora del servidor para evitar problemas de autentificación si la hora está desincronizada.

## Instalación de software

ejecuto sudo apt install krb5-user samba sssd ntp

En una primera prueba he eliminado ntp por simplificar, pero más adelante lo añadiré. Si el cliente también sincroniza bien la hora no es problema.

## Kerberos Configuration

Al ejecutar la instalación anterior de krb5-user nos pregunta por el reino kerberos (realm) coincide con nuestro nombre de domini OJO hay que ponerlo en mayúsculas. En mi caso solo pregunta eso y el resto lo detecta automático.

Solo queda comprobar que el archivo /etc/krb5.conf coincide con lo que debería ser. Yo no he tocado nada. Me falta comprobar que el tiempo de vida de los ticket realmente es la que va por defecto.

Al haberme saltado la instalación de ntp no he añadido en /etc/ntp.conf el servidor de hora. Más adelante si sería interesante hacerlo.

## Configuración Samba

Modificó el contenido de /etc/samba/smb.conf como se indica. En mi caso el Workgroup lo cambio pero el resto de opciones no estaban y las añado en la sección [Global]

## SSSD Configuration

Creo el archivo con copy paste y cambiando el nombre de dominio. No olvidarse de cambiar el propietario y permisos como se indica

## Verify nsswitch.conf Configuration

Simplemente lo verifico.

## Modify /etc/hosts

Este punto no lo tengo claro . Yo siempre lo había hecho de otra forma. No lo hago como indica, pero veo que para que haya actualizaciones dinámicas en el DNS debería ser así.

De momento no he añadido la línea con la IP del equipo sino en la linea que ya existe como 127.0.0.1, el resto igual.

## Join the Active Directory

Reinicio los servicios (ntp no por no haberlo configurado)

Testeo con kinit y verificar el ticket con klist

por último uno el equipo con sudo net ads join -k

me aparece el warning que avisa la documentación No DNS domain configured. Unable to perform DNS Update.

Compruebo con getent password y no salen los de dominio, pero si le pregunto por uno concreto sí sale.

## Test Authentication

Pruebo y funciona.

## Home directories with pam\_mkhomedir (optional)

añado la linea que indica al /etc/pam-d/common-session.

Aquí tengo el problema que falta de pulir.

Se refiere a los permisos por defecto (umask) de los usuarios de dominio. Los usuarios de dominio van todos al mismo grupo principal “Usuarios del dominio” lo que provoca que el home de cada usuari sea accesible por todos. He probado a cambiar en la línea el umask=0022 por umask=0066 pero no va. Cuando ejecuto umask desde el usuario veo que sigue siendo 0022. y los permisos al crear el home son 644 como corresponde a esa máscara.

He probado a cambiar en /etc/defs el umask para todos y eso provoca un daño colateral en el escritorio y en más sitios supongo. Ya no he probado mas cosas ya que no quiero que interfiera con la configuración que tenga puesta vitalinux.

## Desktop Ubuntu Authentication

No es necesario en vitalinux.

Una vez finalizado solo queda probarlo para ello la primera vez iniciar sesión con iespiramide\nombreusuario y para dentro.

## Conclusion

A falta de probarlo con fuego real hay dos detalles que aun no me gusta como me quedan.

* Lo de los permisos en home
* Que no cachea las credenciales para usuarios que ya hubieran iniciado sesión en el equipo, por si el servidor está fuera de servicio como ocurre en windows. Al menos en la prueba que he realizado