

vcenter, SSO, VCSA, AD

Vcenter Server Appliance VCSA

El nuevo vcenter appliance elimina la necesidad de contar con una licencia de windows para instalar el vcenter. Además permite manejar más objetos que la base de datos sqllite que incluye la versión para windows.

Entre las limitaciones tenemos <http://kb.vmware.com/kb/2002531>

Validación en AD con Vcenter Appliance 5.5

En vsphere 5.5 la validación SSO ha sido reescrita y se han añadido nuevos tipos de validación.

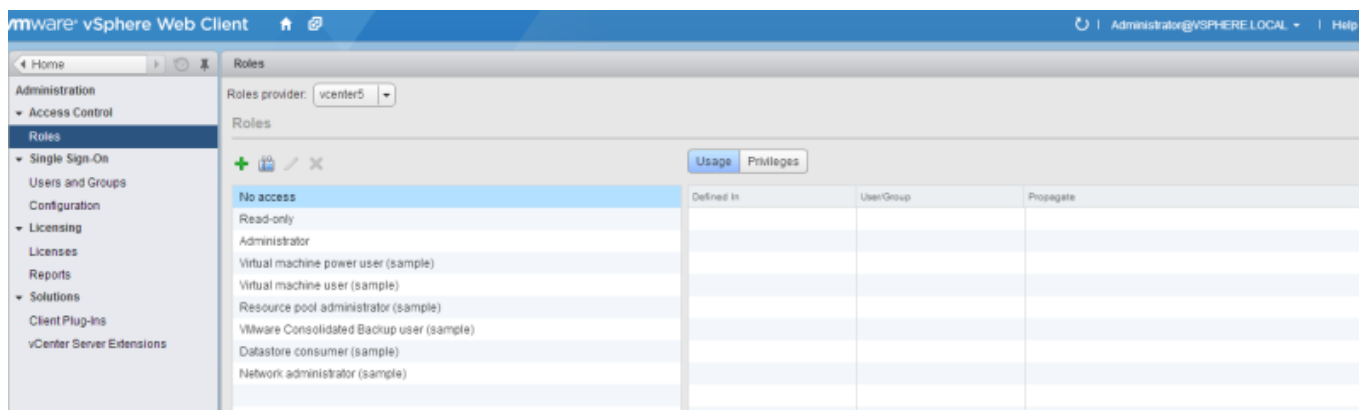
Para configurar nuestro VCSA y utilizar la validación de nuestros usuario y grupos integrada con nuestro Active Directory vamos a seguir los siguientes pasos:

- Nos conectamos a nuestro cliente web <https://xxx.xxx.xxx.xxx:9443/vsphere-client> con el usuario **administrator@vsphere.local** y como contraseña **vmware**



En el cliente para escritorio no aparece la opción de configuración y tampoco aparece si entramos con el usuario root aunque entremos al cliente web

- Pinchamos en Administration → Single Sign-On → **Configuration**



Si no aparece la opción de configuration es que no te has validado como administrator@vsphere.local

Al pulsar sobre **Configuration** la pantalla que aparece es la siguiente

Policies Identity Sources Certificates				
Name	Server URL	Type	Domain	Alias
--	--	--	vsphere.local	--
--	--	Local OS	locals (default)	--

- En la pestaña **Identity Sources** pulsamos sobre el + de color verde para añadir un nuevo origen de identificación

The screenshot shows the 'Add identity source' dialog box. The 'Identity source type' section has four radio buttons: 'Active Directory (Integrated Windows Authentication)', 'Active Directory as a LDAP Server', 'Open LDAP' (which is selected), and 'Local OS'. The 'Identity source settings' section contains several text input fields: 'Name', 'Base DN for users', 'Domain name', 'Domain alias', 'Base DN for groups', 'Primary server URL', 'Secondary server URL', 'Username', and 'Password'. A 'Test Connection' button is positioned below the 'Username' and 'Password' fields. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Si estamos en el vcenter basado en windows elegiríamos como opción de Identity source type la primera **Active Directory (Integrated Windows Authentication)**. En nuestro caso como lo estamos instalando desde el appliance que incluye una distribución de linux Suse, tenemos que elegir la segunda opción **Active Directory as LDAP Server** y configurar los parámetros según nuestro AD.

Add identity source

Identity source type:

- ☐ Active Directory (Integrated Windows Authentication)
- ☒ Active Directory as a LDAP Server
- ☐ Open LDAP
- ☐ Local OS

Identity source settings

Name: miad.local

Base DN for users: DC=miad,DC=local

Domain name: miad.local

Domain alias: miad

Base DN for groups: DC=miad,DC=local

Primary server URL: ldap://domaincontroller1.miad.local:3268

Secondary server URL: ldap://domaincontroller2.miad.local:3268

Username: miad\usuariovalidacion

Password: *****

Test Connection

OK Cancel

Al pulsar sobre el botón **OK** nos aparecerá el nuevo origen de identificación que acabamos de crear. Si queremos que sea el origen por defecto, lo seleccionamos y pulsamos sobre el icono

SSO Configuration for 172.19.3.205

Policies Identity Sources Certificates

Filter

Name	Server URL	Type	Domain	Alias
miad.local	---	---	vsphere.local	---
Local OS	---	Local OS	localos (default)	---

Al cambiarla validación por defecto aparecerá una ventana de aviso

Renovar los certificados

- Para renovar los certificados del vcenter appliance o bien lo hacemos desde <https://mivcenter:5480> →pestaña Admin y seleccionamos la opción de Certificate regeneration enabled→ Submit
- Otra opción es conectarnos por ssh al vcenter y ejecutamos creamos un fichero llamado

allow_regeneration en el directorio /etc/vmware-vpx/ssl directory

```
touch /etc/vmware-vpx/ssl/allow_regeneration
```



Después de hacer cualquiera de los dos cambios hay que reiniciar el appliance ya que es en el reinicio cuando genera los nuevos certificados



Tenía un problema que seguía sin poder conectar al cliente web aún habiendo renovado los certificados, para solucionarlo conecté por ssh al vcenter y ejecuté el siguiente script **/opt/vmware/share/vami/vami_config_net** revisé los parámetros de configuración de hostname e ip y aunque los parámetros eran los mismos volvió a funcionar

Referencias

- <http://www.virten.net/2013/09/howto-ad-authentication-in-vcenter-sso-5-5/>

From:
<https://intrusos.info/> - LCWIKI

Permanent link:
<https://intrusos.info/doku.php?id=virtualizacion:vmware:version5:vcenterappliance&rev=1403183132>

Last update: 2023/01/18 14:41

