Dominios de autenticación en Proxmox VE

En Proxmox VE, como comentamos en el apartado de usuarios, disponemos de varios dominios o reinos (realm) de autenticación dependiendo de que opciones usemos para autenticar a los usuarios.

Como los usuarios de Proxmox VE son los homólogos de los usuarios que existen en algún dominio externo, los dominios deben configurarse en **/etc/pve/domains.cfg**. Están disponibles los siguientes dominios (métodos de autenticación):

Autenticación estándar PAM de Linux

Linux PAM es el método para la autenticación de usuarios en todo el sistema. Estos usuarios se crean en el sistema host linux con comandos como **adduser**. Si existen usuarios de PAM en el sistema host de Proxmox VE, se pueden agregar las entradas correspondientes a Proxmox VE para permitir que estos usuarios inicien sesión a través de su nombre de usuario y contraseña del sistema.

Linux PAM corresponde a los usuarios del sistema host, debe existir un usuario del sistema en cada nodo en el que el usuario pueda iniciar sesión. El usuario se autentica con su contraseña habitual del sistema. Este dominio se agrega de forma predeterminada y no se puede eliminar. En términos de configuración, un administrador puede optar por requerir autenticación de dos factores con inicios de sesión desde el dominio y establecer el dominio como el dominio de autenticación predeterminado.

Servidor de autenticación Proxmox VE

Este es un almacén de contraseñas similar al que usa Unix, que almacena contraseñas hash en /**etc/pve/priv/shadow.cfg**. Las contraseñas se codifican mediante el algoritmo hash SHA-256. Este es el mejor sistema para instalaciones de pequeña escala (o incluso de mediana escala), donde los usuarios no necesitan acceso a nada fuera de Proxmox VE. En este caso, los usuarios se administran completamente por Proxmox VE y pueden cambiar sus propias contraseñas a través de la GUI.

El ámbito del servidor de autenticación Proxmox VE es un almacén de contraseñas simple similar a Unix. El dominio se crea de forma predeterminada y, al igual que con Linux PAM, los únicos

elementos de configuración disponibles son la capacidad de requerir autenticación de dos factores para los usuarios del dominio y establecerlo como el dominio predeterminado para iniciar sesión.

A diferencia de otros tipos de dominio de Proxmox VE, los usuarios se crean y autentican completamente a través de Proxmox VE, en lugar de autenticarse contra otro sistema. Por lo tanto, se le solicita que establezca una contraseña para este tipo de usuario al momento de su creación.

LDAP

LDAP (Protocolo ligero de acceso a directorios) es un protocolo abierto multiplataforma para la autenticación mediante servicios de directorio. OpenLDAP es una implementación popular de código abierto del protocolo LDAP.

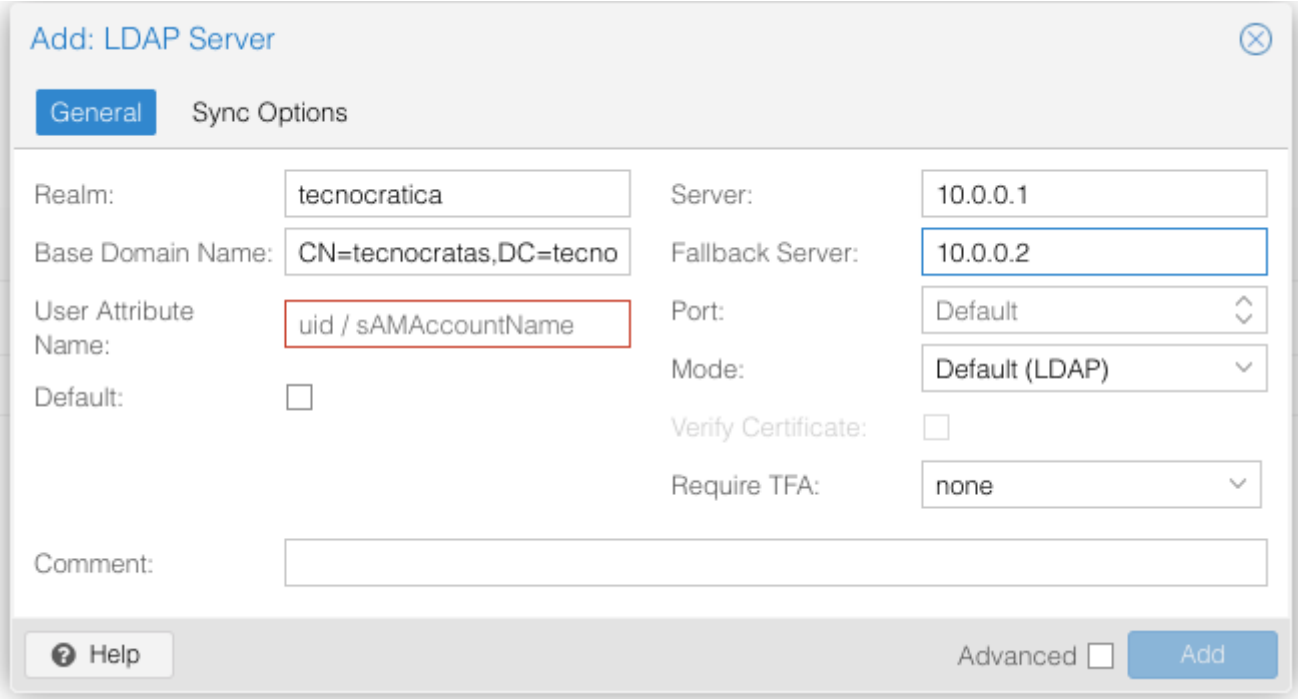
También puede utilizar un servidor LDAP externo para la autenticación de usuarios (por ejemplo, OpenLDAP). En este tipo de dominio, los usuarios se buscan bajo un nombre de dominio base (base_dn), utilizando el atributo de nombre de usuario especificado en el campo Nombre de atributo de usuario (user_attr).

Se puede configurar un servidor y un servidor de backup opcional, y la conexión se puede cifrar mediante SSL. Además, se pueden configurar filtros para directorios y grupos. Los filtros le permiten limitar aún más el alcance del dominio.

Por ejemplo, si un usuario está representado a través del siguiente conjunto de datos LDIF:

```
# etaboada of Group Tecnocratas at tecnocractica.net
dn: uid=user1,ou=Tecnocratas,dc=tecnocratica,dc=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: etaboada
cn: Prueba usuario
sn: Pruebas
description: Usuario de prueba.
```

El nombre de dominio base sería **ou=Tecnocratas,dc=tecnocratica,dc=net** y el atributo de usuario sería uid.



Si Proxmox VE necesita autenticarse (vincularse) al servidor LDAP antes de poder consultar y autenticar usuarios, se puede configurar un nombre de dominio de vinculación a través de la propiedad bind_dn en **/etc/pve/domains.cfg**. Luego, su contraseña debe almacenarse en **/etc/pve/priv/ldap/<realmname>.pw** (por ejemplo, /etc/pve/priv/ldap/tecnocratica.pw). Este archivo debe contener una sola línea con la contraseña sin formato.

Para verificar los certificados, debe configurar capath. Puede configurarlo directamente en el certificado CA de su servidor LDAP o en la ruta del sistema que contiene todos los certificados CA confiables (/etc/ssl/certs). Además, debe configurar la opción de verificación, que también se puede realizar a través de la interfaz web.

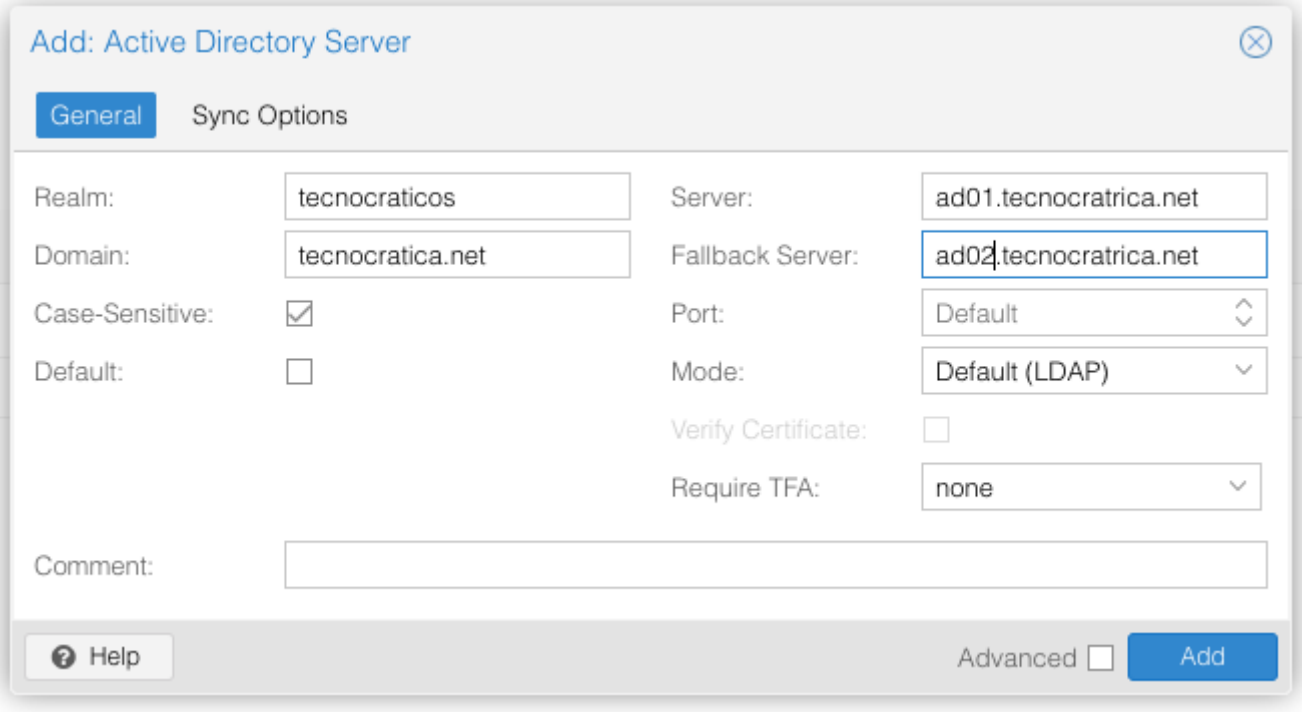
Las principales opciones de configuración para un dominio de servidor LDAP son las siguientes:

- Realm (reino): El identificador de reino para los usuarios de Proxmox VE
- Nombre de dominio base (base_dn): el directorio en el que se buscan los usuarios
- Nombre de atributo de usuario (user_attr): el atributo LDAP que contiene el nombre de usuario con el que los usuarios iniciarán sesión.
- Servidor (servidor1): el servidor que aloja el directorio LDAP
- Servidor alternativo (servidor2): una dirección de servidor alternativo opcional, en caso de que no se pueda acceder al servidor principal
- Puerto (puerto): el puerto en el que escucha el servidor LDAP (normalmente el 389)

> Para permitir que un usuario en particular se autentique utilizando el servidor LDAP, también debe agregarlo como usuario de ese dominio desde el servidor Proxmox VE. Esto se puede realizar automáticamente con la sincronización.

Directorio activo de Microsoft (AD)

Microsoft Active Directory (AD) es un servicio de directorio para redes de dominio de Windows y Proxmox VE lo admite como dominio de autenticación. Soporta LDAP como protocolo de autenticación, ya que es un LDAP extendido.



Como podemos ver la configuración es muy parecida a la de LDAP, ya que al fin y al cabo, AD es compatible con LDAP

Para permitir que un usuario en particular se autentique utilizando el servidor LDAP, también debe agregarlo como usuario de ese dominio desde el servidor Proxmox VE. Esto se puede llevar a cabo automáticamente con la sincronización. Para configurar Microsoft AD como dominio, se debe especificar una dirección de servidor y un dominio de autenticación. Active Directory admite la mayoría de las mismas propiedades que LDAP, como un servidor de respaldo opcional, un puerto y cifrado SSL. Además, los usuarios pueden agregarse a Proxmox VE automáticamente mediante operaciones de sincronización, después de la configuración.

Al igual que con LDAP, si Proxmox VE necesita autenticarse antes de vincularse al servidor AD, debe configurar la propiedad Vincular usuario (bind_dn). Esta propiedad suele ser necesaria de forma predeterminada para Microsoft AD.

Los principales ajustes de configuración de Microsoft Active Directory son:

- Realm (reino): El identificador de reino para los usuarios de Proxmox VE
- Dominio (dominio): el dominio AD del servidor
- Servidor (servidor1): el FQDN o dirección IP del servidor
- Servidor alternativo (servidor2): una dirección de servidor alternativo opcional, en caso de que no se pueda acceder al servidor principal
- Puerto (puerto): el puerto en el que escucha el servidor de Microsoft AD

Sincronización de dominios basados en LDAP

Es posible sincronizar automáticamente usuarios y grupos para dominios basados en LDAP (LDAP y Microsoft Active Directory), en lugar de tener que agregarlos a Proxmox VE manualmente. Puede acceder a las opciones de sincronización desde la ventana Agregar/Editar del panel de Autenticación de la interfaz web o mediante los comandos p**veum realm add/modify**. Luego puede realizar la operación de sincronización desde el panel de Autenticación de la GUI o utilizando el siguiente comando:

```
pveum realm sync <realm>
```

Los usuarios y grupos se sincronizan con el archivo de configuración de todo el cluster en el archivo /etc/pve/user.cfg.

Atributos a propiedades

Si la respuesta de sincronización incluye atributos de usuario, se sincronizarán con la propiedad de usuario correspondiente en user.cfg. Por ejemplo: nombre o apellido.

Si los nombres de los atributos no coinciden con las propiedades de Proxmox VE, puede establecer un mapa personalizado de campo a campo en la configuración utilizando la opción **sync_attributes.**

La forma en que se manejan dichas propiedades si algo desaparece se puede controlar a través de las opciones de sincronización.

Configuración de sincronización

Las opciones de configuración para sincronizar dominios basados en LDAP se pueden encontrar en la pestaña Opciones de sincronización de la ventana Agregar/Editar.

Las opciones de configuración son las siguientes:

- Vincular usuario (bind_dn): se refiere a la cuenta LDAP utilizada para consultar usuarios y grupos. Esta cuenta necesita acceso a todas las entradas deseadas. Si está configurado, la búsqueda se realizará mediante vinculación; en caso contrario, la búsqueda se realizará de forma anónima. El usuario debe tener un nombre distinguido (DN) con formato LDAP completo, por ejemplo, cn=admin,dc=example,dc=com.
- Atributo de nombre de grupo. (group_name_attr): Representa los grupos de usuarios. Sólo se sincronizan las entradas que cumplen con las limitaciones habituales de caracteres del archivo user.cfg. Los grupos se sincronizan con -$realm adjunto al nombre, para evitar conflictos de nombres. Asegúrese de que una sincronización no sobrescriba los grupos creados manualmente.

- Clases de usuario (user_classes): Clases de objetos asociados a los usuarios.
- Clases de grupo (group_classes): Clases de objetos asociados a grupos.
- Atributo de correo electrónico: si el servidor basado en LDAP especifica direcciones de correo electrónico de usuario, estas también se pueden incluir en la sincronización configurando el atributo asociado aquí. Desde la línea de comando, esto se puede lograr mediante el parámetro --sync_attributes.
- Filtro de usuario (filtro): para obtener más opciones de filtro para dirigirse a usuarios específicos.
- Filtro de grupo (group_filter): para obtener más opciones de filtrado para dirigirse a grupos específicos.

Opciones de sincronización

Además de las opciones especificadas en la sección anterior, también puede configurar otras opciones que describen el comportamiento de la operación de sincronización.

Estas opciones se configuran como parámetros antes de la sincronización o como valores predeterminados a través de la opción de reino sync-defaults-options.

Las principales opciones de sincronización son:

- Alcance (**scope**): el alcance de qué sincronizar. Pueden ser usuarios, grupos o ambos.
- Habilitar nuevo (**enable-new**): si se establece, los usuarios recién sincronizados están habilitados y pueden iniciar sesión. El valor predeterminado es verdadero.
- Eliminar no encontrados (**remove-vanished**): esta es una lista de opciones que, cuando se activan, determinan si se eliminan cuando no se devuelven de la respuesta de sincronización. Las opciones son:
  - ACL (**acl**): elimina las ACL de usuarios y grupos que no se devolvieron en la respuesta de sincronización. Esto suele tener sentido junto con Entry.
  - Entrada (**entry**): elimina las entradas (es decir, usuarios y grupos) cuando no se devuelven en la respuesta de sincronización.
  - Propiedades (**properties**): elimina las propiedades de las entradas donde el usuario en la respuesta de sincronización no contenía esos atributos. Esto incluye todas las propiedades, incluso aquellas que nunca se establecen mediante una sincronización. Las excepciones son los tokens y el indicador de habilitación; estos se conservarán incluso con esta opción habilitada.
- Vista previa (**dry-run**): no se escriben datos en la configuración. Esto es útil si desea ver qué usuarios y grupos se sincronizarían con user.cfg.

Carácteres reservados

Ciertos caracteres están reservados (consulta la RFC2253) y no se pueden usar fácilmente en valores de atributos en DN sin utilizar escapes adecuados.

Los siguientes carácteres necesitan secuencia de escape:

- Espacio ( ) al principio o al final
- Signo numérico (#) al principio
- Coma (,)
- Signo más (+)
- Comilla doble ("")
- Barras diagonales (/)
- Corchetes angulares (<>)
- Punto y coma (;)
- Signo igual (=)

Para utilizar dichos caracteres en DN, escribe el valor del atributo entre comillas dobles. Por ejemplo, para vincularse con un usuario con el ejemplo CN (nombre común), usuario, utilice CN="Ejemplo, usuario",OU=people,DC=example,DC=com como valor para bind_dn.

Esto se aplica a los atributos base_dn, bind_dn y group_dn.

> Los usuarios con dos puntos y barras diagonales no se pueden sincronizar ya que son caracteres reservados en los nombres de usuario.

Conexión OpenID

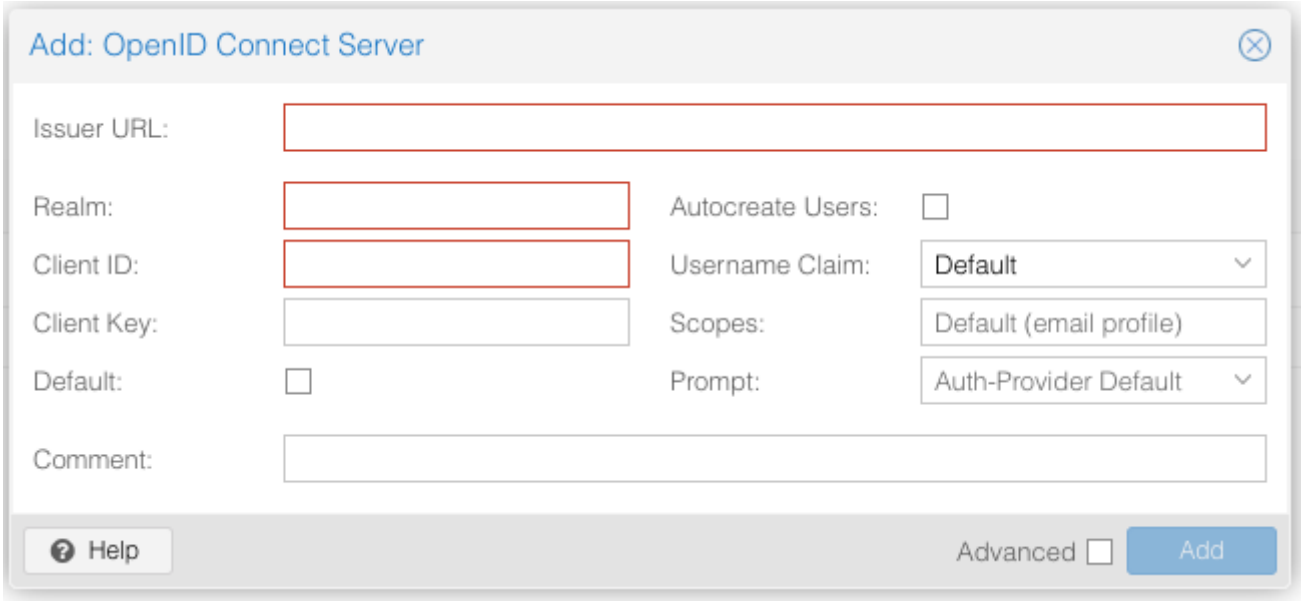
OpenID Connect se implementa como una capa de identidad sobre el protocolo OATH 2.0. Permite a los clientes verificar la identidad del usuario, basándose en la autenticación realizada por un servidor de autorización externo. Existen diferentes productos que proporcionan dicha funcionalidad.

Las principales opciones de configuración de OpenID Connect son:

URL del emisor (**issuer-url**): Esta es la URL del servidor de autorización. Proxmox utiliza el protocolo OpenID Connect Discovery para configurar automáticamente más detalles.

Si bien es posible utilizar URL http:// no cifradas, recomendamos encarecidamente utilizar conexiones https:// cifradas. ya que en la comunicación se intercambian datos confidenciales que pueden ser aprovechados para obtener acceso no autorizado.

- Dominio(**realm**): El identificador de reino o dominio para los usuarios de Proxmox VE
- ID de cliente (**client-id**): ID de cliente OpenID.
- Clave de cliente (**client-key**): Clave de cliente OpenID opcional.
- Autocrear usuarios (**autocreate**): Crea usuarios automáticamente si no existen. Si bien la autenticación se realiza en el servidor OpenID, todos los usuarios aún necesitan una entrada en la configuración de usuario de Proxmox VE. Puede agregarlos manualmente o usar la opción de creación automática para agregar nuevos usuarios automáticamente.
- Reclamación de nombre de usuario (**username-claim**): Opción de OpenID utilizada para generar el nombre de usuario único (asunto, nombre de usuario o correo electrónico).



Mapa de nombres de usuario

La especificación OpenID Connect define un único atributo único (*claim* en términos de OpenID) denominado sujeto. De forma predeterminada, utilizamos el valor de este atributo para generar nombres de usuario de Proxmox VE, simplemente agregando @ y el nombre del dominio: ${subject}@${realm}.

Desafortunadamente, la mayoría de los servidores OpenID usan cadenas aleatorias para el asunto, como

K5ZZI1NADAUCEA0STSB9, por lo que un nombre de usuario típico sería K5ZZI1NADAUCEA0STSB9@yourrealm. Si bien es único, es difícil para los humanos recordar estas cadenas aleatorias, lo que hace imposible asociar a usuarios reales con esto.

La configuración de claim de nombre de usuario le permite usar otros atributos para la asignación del nombre de usuario. Es prefible configurarlo como nombre de usuario si el servidor OpenID Connect proporciona ese atributo y garantiza su singularidad.

Otra opción es utilizar el correo electrónico, que también proporciona nombres de usuario legibles por humanos. Nuevamente, use esta configuración solo es factible, si el servidor garantiza la unicidad de este atributo.

Ejemplos
A continuación se muestra un ejemplo de cómo crear un dominio OpenID usando Google. Debe reemplazar --client-id y --client-key con los valores de su configuración de Google OpenID.

```
pveum realm add myrealm1 --type openid --issuer-url  https://accounts.google.com --client-id
XXXX --client-key YYYY --username-claim email
```

El comando anterior utiliza el correo electrónico --username-claim, de modo que los nombres de usuario en el lado de Proxmox VE se vean como ejemplo.usuario@google.com@myrealm1.

Revision #7
Created 27 January 2024 10:13:48 by etaboada
Updated 28 January 2024 08:15:21 by etaboada