

Usuarios y Grupos en Proxmox VE

El sistema de usuarios y grupos en Proxmox, nos permite definir permisos granulares, si necesitamos conceder acceso en nuestra organización a diferentes perfiles de cara a que ellos mismos se gestionen sus máquinas y su infraestructura.

Para ello empezaremos a ver como funcionan los usuarios, los grupos y los sistemas de autenticación que soporta Proxmox VE

Sistemas de autenticación

Proxmox VE admite múltiples fuentes de autenticación, por ejemplo Linux PAM (usuarios del sistema Linux subyacente), un servidor de autenticación Proxmox VE integrado, LDAP, Microsoft Active Directory y OpenID Connect. Estas opciones de configuración, [se explican en el siguiente artículo](#).

Al utilizar la administración de permisos y usuarios basada en roles para todos los objetos (VM, almacenamiento, nodos, etc.), se puede definir el acceso granular como hemos comentado antes.

Usuarios

Proxmox VE almacena los atributos del usuario en **/etc/pve/user.cfg**. Las contraseñas no se almacenan aquí; en cambio, los usuarios están asociados con los dominios de autenticación que se describen en los diferentes sistemas de autenticación que explicaremos. Por lo tanto, un usuario suele identificarse internamente por su nombre de usuario y dominio en el formato `<userid>@<realm>`.

Por ejemplo para acceder con un usuario del propio sistema el realm será pam ([eduardo@pam](#)), en el caso de usuarios del servidor de autenticación de Proxmox VE Integrado el realm será pve ([eduardo@pve](#))

Cada entrada de usuario en este archivo contiene la siguiente información:

- Nombre de pila
- Apellido

- Dirección de correo electrónico
- Grupos a los que pertenece
- Fecha de caducidad de la cuenta
- Comentarios o notas sobre este usuario
- Si este usuario está habilitado o deshabilitado
- Claves de autenticación de doble factores (opcional)

Precaución Cuando deshabilitas o eliminas un usuario, o si la fecha de vencimiento establecida ya pasó, este usuario no podrá iniciar sesión, ni iniciar nuevas tareas. Todas las tareas que ya haya iniciado este usuario (por ejemplo, sesiones de terminal) no finalizarán automáticamente por dicho evento, por lo que permanecerán en ejecución.

Usuarios especiales

Administrador del sistema (root/pam)

El usuario root del sistema siempre puede iniciar sesión a través del dominio PAM de Linux y es un administrador ilimitado. Este usuario no se puede eliminar, pero aún se pueden cambiar los atributos. Los correos del sistema se enviarán a la dirección de correo electrónico asignada a este usuario.

Grupos

Cada usuario puede ser miembro de varios grupos. Los grupos son la forma recomendada de organizar los permisos de acceso, ya que de esa forma tendremos mejor control de los que hace cada usuario, sin tener que asignar permisos específicos usuario por usuario, que puede dejar fallos de seguridad. Siempre debes otorgar permisos a grupos en lugar de a usuarios individuales. De esa manera tendrás una lista de control de acceso (ACL) mucho más fácil de mantener.

Revision #2

Created 27 January 2024 09:59:13 by etaboada

Updated 28 January 2024 08:05:28 by etaboada