

Permisos en Proxmox VE - Roles y Privilegios

Como comentamos en la gestión de [usuarios y grupos](#) en Proxmox VE, el motivo de esto era usar estas configuraciones para asignar determinados permisos a los usuarios o grupos. En este artículo, veremos los permisos disponibles.

Gestión de permisos en Proxmox VE

Para que un usuario pueda realizar una acción (como listar, modificar o eliminar partes de la configuración de una VM), el usuario debe tener los permisos adecuados.

Proxmox VE utiliza un sistema de gestión de permisos basado en roles y rutas. Una entrada en la tabla de permisos permite que un usuario, grupo o token asuma un rol específico al acceder a un objeto o ruta. Esto significa que dicha regla de acceso se puede representar como una tripleta de (ruta, usuario, rol), (ruta, grupo, rol) o (ruta, token, rol), donde el rol contiene un conjunto de acciones permitidas y el camino que representa el objetivo de estas acciones.

Roles

Un rol es simplemente una lista de privilegios. Proxmox VE viene con una serie de funciones predefinidas que satisfacen la mayoría de los requisitos.

- **Administrator:** tiene todos los privilegios
- **NoAccess:** no tiene privilegios (se usa para prohibir el acceso)
- **PVEAdmin:** puede realizar la mayoría de las tareas, pero no tiene derechos para modificar la configuración del sistema (*Sys.PowerMgmt*, *Sys.Modify*, *Realm.Allocate*) o permisos (*Permissions.Modify*)
- **PVEAuditor:** tiene acceso de solo lectura
- **PVEDatastoreAdmin:** crea y asigna plantillas y espacio de respaldo
- **PVEDatastoreUser:** asigna espacio de respaldo y ve el almacenamiento
- **PVEMappingAdmin:** gestionar asignaciones de recursos
- **PVEMappingUser:** ver y usar asignaciones de recursos
- **PVEPoolAdmin:** asignar grupos
- **PVEPoolUser:** ver grupos
- **PVESDNAdmin:** gestionar la configuración SDN
- **PVESDNUser:** acceso a bridges/vnets

- **PVESysAdmin:** auditoría, consola del sistema y registros del sistema
- **PVETemplateUser:** ver y clonar plantillas
- **PVEUserAdmin:** gestionar usuarios
- **PVEVMAdmin:** administrar completamente las máquinas virtuales
- **PVEVMUser:** ver, realizar copias de seguridad, configurar CD-ROM, consola de VM, administración de energía de VM

Puedes ver el conjunto completo de roles predefinidos en la GUI.

Create	Edit	Remove
Built-In	Name ↑	Privileges
Yes	Administrator	Datastore.Allocate Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit Group.Allocate Mapping.Audit Mapping.Modify Mapping.Use Permissions.Modify Pool.Allocate Pool.Audit Realm.Allocate Realm.AllocateUser SDN.Allocate SDN.Audit SDN.Use Sys.Audit Sys.Console Sys.Incoming Sys.Modify Sys.PowerMgmt Sys.Syslog User.Modify VM.Allocate VM.Audit VM.Backup VM.Clone VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Disk VM.Config.HWType VM.Config.Memory VM.Config.Network VM.Config.Options VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback
Yes	NoAccess	-
Yes	PVEAdmin	Datastore.Allocate Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit Group.Allocate Mapping.Audit Mapping.Use Pool.Allocate Pool.Audit Realm.AllocateUser SDN.Allocate SDN.Audit SDN.Use Sys.Audit Sys.Console Sys.Syslog User.Modify VM.Allocate VM.Audit VM.Backup VM.Clone VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Disk VM.Config.HWType VM.Config.Memory VM.Config.Network VM.Config.Options VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback
Yes	PVEAuditor	Datastore.Audit Mapping.Audit Pool.Audit SDN.Audit Sys.Audit VM.Audit
Yes	PVEDatastoreAdmin	Datastore.Allocate Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit
Yes	PVEDatastoreUser	Datastore.AllocateSpace Datastore.Audit
Yes	PVEMappingAdmin	Mapping.Audit Mapping.Modify Mapping.Use
Yes	PVEMappingUser	Mapping.Audit Mapping.Use
Yes	PVEPoolAdmin	Pool.Allocate Pool.Audit
Yes	PVEPoolUser	Pool.Audit
Yes	PVESDNAdmin	SDN.Allocate SDN.Audit SDN.Use
Yes	PVESDNUser	SDN.Audit SDN.Use
Yes	PVESysAdmin	Sys.Audit Sys.Console Sys.Syslog
Yes	PVETemplateUser	VM.Audit VM.Clone
Yes	PVEUserAdmin	Group.Allocate Realm.AllocateUser User.Modify
Yes	PVEVMAdmin	VM.Allocate VM.Audit VM.Backup VM.Clone VM.Config.CDROM VM.Config.CPU VM.Config.Cloudinit VM.Config.Disk VM.Config.HWType VM.Config.Memory VM.Config.Network VM.Config.Options VM.Console VM.Migrate VM.Monitor VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback
Yes	PVEVMUser	VM.Audit VM.Backup VM.Config.CDROM VM.Config.Cloudinit VM.Console VM.PowerMgmt

Puedes agregar nuevos roles a través de la GUI o la línea de comando.

▼ Datacenter

> hv9

Search

Summary

Notes

Cluster

Ceph

Options

Storage

Backup

Replication

Permissions

Users

API Tokens

Two Factor

Groups

Pools

Roles

Realms

Create

Edit

Remove

Built-In	Name ↑
Yes	Administrator
Yes	NoAccess
Yes	PVEAdmin
Yes	PVEAuditor
Yes	PVEDatastoreAc
Yes	PVEDatastoreUs
Yes	PVEMappingAdi
Yes	PVEMappingUse
Yes	PVEPoolAdmin
Yes	PVEPoolUser
Yes	PVESDNAdmin
Yes	PVESDNUser
Yes	PVESysAdmin
Yes	PVETemplateUs
Yes	PVEUserAdmin

Si pulsamos en crear, podremos crear un rol nuevo.

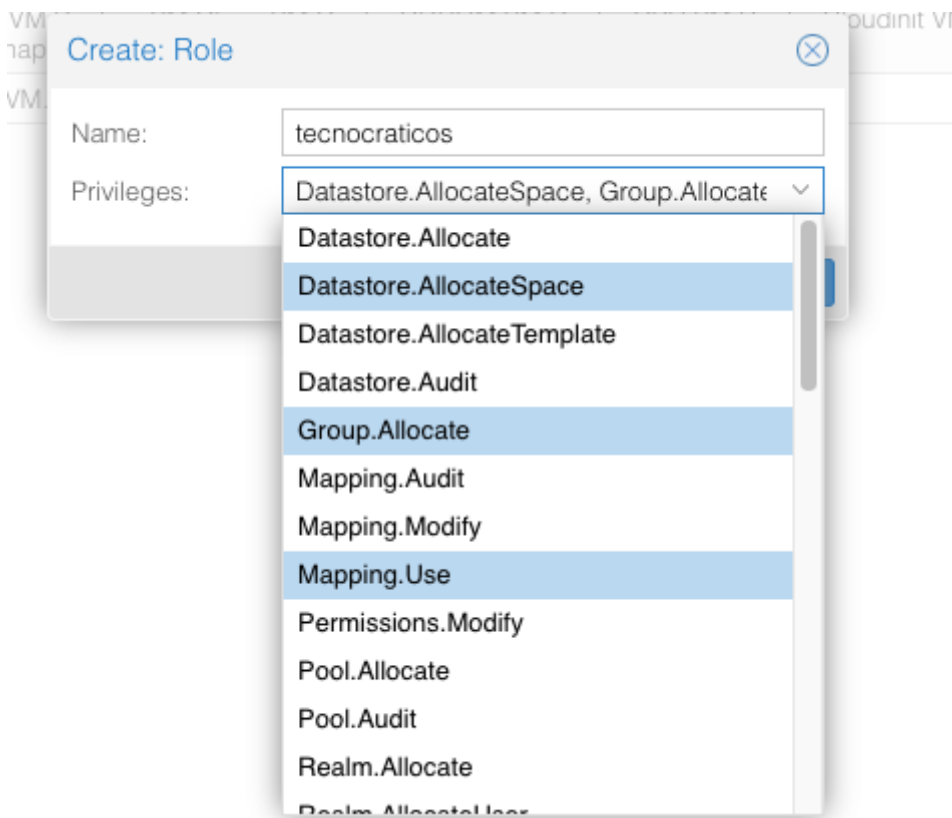
Create: Role

Name:

Privileges:

Create

De esta forma, se pueden asignar uno o más roles predefinidos al un rol nuevo



Para agregar un rol a través de la línea de comando, puede usar la herramienta CLI pveum, por ejemplo:

```
pveum role add VM_Power-only --privs "VM. PowerMgmt VM. Console"
pveum role add Sys_Power-only --privs "Sys. PowerMgmt Sys. Console"
```

Privilegios

Un privilegio es el derecho a realizar una acción específica. Para simplificar la administración, las listas de privilegios se agrupan en roles, que luego se pueden usar en la tabla de permisos. Ten en cuenta que los privilegios no se pueden asignar directamente a usuarios y rutas sin ser parte de un rol.

Actualmente Proxmox VE admite los siguientes privilegios:

Privilegios relacionados con el nodo/sistema

- Group.Allocate: crear/modificar/eliminar grupos
- Mapping.Audit: ver asignaciones de recursos
- Mapping.Modify: gestionar asignaciones de recursos
- Mapping.Use: utilizar asignaciones de recursos
- Permisos.Modificar: modificar permisos de acceso
- Pool.Allocate: crear/modificar/eliminar un grupo
- Pool.Audit: ver un pool

- Realm.AllocateUser: asigna usuario a un realm o dominio de autenticación
- Realm.Allocate: crear/modificar/eliminar dominios de autenticación
- SDN.Allocate: gestionar la configuración de SDN
- SDN.Audit: ver la configuración de SDN
- Sys.Audit: ver el estado/configuración del nodo, la configuración del clúster Corosync y la configuración de HA
- Sys.Console: acceso de consola al nodo
- Sys.Incoming: permite flujos de datos entrantes de otros clústeres (experimental)
- Sys.Modify: crear/modificar/eliminar parámetros de red de nodos
- Sys.PowerMgmt: gestión de energía del nodo (inicio, parada, reinicio, apagado,...)
- Sys.Syslog: ver syslog
- User.Modify: crea/modifica/elimina el acceso y los detalles del usuario.

Privilegios relacionados con la máquina virtual

- SDN.Use: acceda a redes virtuales SDN y los bridges de red local
- VM.Allocate: crear/eliminar VM en un servidor
- VM.Audit: ver la configuración de VM
- VM.Backup: copia de seguridad/restauración de máquinas virtuales
- VM.Clone: clonar/copiar una VM
- VM.Config.CDROM: expulsar/cambiar CD-ROM
- VM.Config.CPU: modificar la configuración de la CPU
- VM.Config.Cloudinit: modificar los parámetros de Cloud-init
- VM.Config.Disk: agregar/modificar/eliminar discos
- VM.Config.HWType: modifica los tipos de hardware emulado
- VM.Config.Memory: modifica la configuración de la memoria
- VM.Config.Network: agregar/modificar/eliminar dispositivos de red
- VM.Config.Options: modifica cualquier otra configuración de VM
- VM.Console: acceso de consola a VM
- VM.Migrate: migre la VM a un servidor alternativo en el clúster
- VM.Monitor: acceso al monitor VM (kvm)
- VM.PowerMgmt: gestión de energía (inicio, parada, reinicio, apagado,...)
- VM.Snapshot.Rollback: revierte la VM a una de sus instantáneas
- VM.Snapshot: crear/eliminar instantáneas de VM

Privilegios relacionados con el almacenamiento

- Datastore.Allocate: crear/modificar/eliminar un almacén de datos y eliminar volúmenes
- Datastore.AllocateSpace: asigna espacio en un almacén de datos
- Datastore.AllocateTemplate: asignar/cargar plantillas e imágenes ISO
- Datastore.Audit: ver/explorar un almacén de datos

Ambos **Permissions.Modify** y **Sys.Modify** deben gestionarse con cuidado, ya que permiten modificar aspectos del sistema y su configuración que son peligrosos o sensibles.

Advertencia Lee atentamente la sección sobre herencia que se detalla a continuación para comprender cómo se propagan los roles asignados (y sus privilegios) a lo largo del árbol de ACL.

Objetos y rutas

Los permisos de acceso se asignan a objetos, como máquinas virtuales, almacenamientos o grupos de recursos. Usamos rutas similares a sistemas de archivos para abordar estos objetos. Estas rutas forman un árbol natural y, opcionalmente, los permisos de niveles superiores (rutas más cortas) se pueden propagar hacia abajo dentro de esta jerarquía.

Los paths pueden tener plantillas. Cuando una llamada API requiere permisos en una ruta con plantilla, la ruta puede contener referencias a parámetros de la llamada API. Estas referencias se especifican entre llaves. Algunos parámetros se toman implícitamente del URI de la llamada API. Por ejemplo, la ruta de permiso **/nodes/{node}** al llamar a **/nodes/mynode/status** requiere permisos en **/nodes/mynode**, mientras que la ruta {path} en una solicitud PUT a **/access/acl** se refiere al parámetro de ruta del método.

Algunos ejemplos son:

- **/nodes/{node}**: Acceso a las máquinas del servidor Proxmox VE
- **/vms**: cubre todas las máquinas virtuales
- **/vms/{vmid}**: acceso a máquinas virtuales específicas
- **/storage/{storeid}**: Acceso a un almacenamiento específico
- **/pool/{poolname}**: acceso a los recursos contenidos en un grupo específico
- **/access/groups**: administración de grupos
- **/access/realms/{realmid}**: acceso administrativo a reinos

Herencia

Como se mencionó anteriormente, las rutas de los objetos forman un sistema de archivos similar a un árbol, y los objetos que se encuentran en ese árbol pueden heredar los permisos (el indicador de propagación está configurado de forma predeterminada). Usamos las siguientes reglas de herencia:

- Los permisos para usuarios individuales siempre reemplazan a los permisos de grupo.
- Los permisos para grupos se aplican cuando el usuario es miembro de ese grupo.
- Los permisos en niveles más profundos reemplazan a los heredados de un nivel superior.
- NoAccess cancela todos los demás roles en una ruta determinada.
- Además, los tokens separados por privilegios nunca pueden tener permisos en una ruta determinada que su usuario asociado no tenga.

Pools

Los pools se pueden utilizar para agrupar un conjunto de máquinas virtuales y almacenes de datos. Luego puedes simplemente establecer permisos en los pools (/pool/{poolid}), que heredan todos los miembros del grupo. Esta es una excelente manera de simplificar el control de acceso.

Revision #1

Created 28 January 2024 08:45:52 by etaboada

Updated 28 January 2024 09:11:16 by etaboada