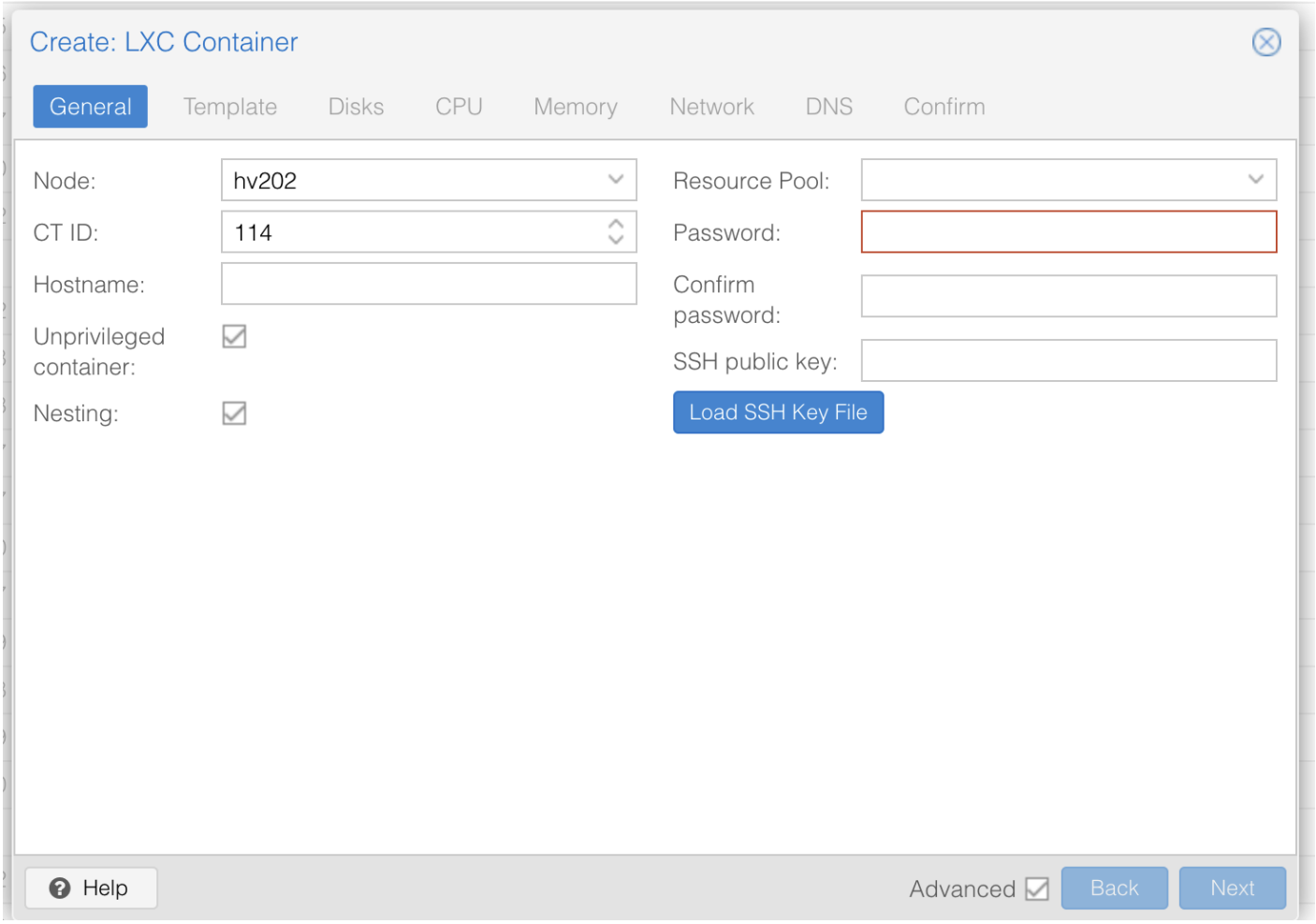
LXC Unprivileged container

Los contenedores sin privilegios son cuando el contenedor se crea y se ejecuta como usuario en lugar de root. Esta es la forma más segura de usar un contenedor porque si la seguridad del contenedor se ve comprometida y el intruso sale del contenedor, se encontrará como un usuario nobody con privilegios extremadamente limitados.

Los contenedores sin privilegios no necesitan ser propiedad del usuario, ya que se ejecutan en espacios de nombres de usuario. Esta es una función del kernel que permite la asignación del UID de un host físico en un espacio de nombres dentro del cual puede existir un usuario con UID 0. Los contenedores sin privilegios también se pueden ejecutar como root. Al asignar un UID y un GID específicos a root, podemos crear contenedores sin privilegios en todo el sistema y ejecutarlos como raíz.
Los contenedores privilegiados son cuando son creados y ejecutados solo por el usuario raíz. Estos contenedores no son seguros porque todos los procesos aún se ejecutan como root. Todos los contenedores creados a través de la GUI de Proxmox o las herramientas PCT son contenedores privilegiados.

> Si la seguridad total o el aislamiento completo de la máquina virtual es la principal preocupación para un entorno, es mejor usar una máquina virtual KVM, porque KVM es una máquina virtual totalmente independiente sin ninguna dependencia del sistema operativo host ni recursos compartidos.



Como podemos ver en la imagen, por defecto los contenedores LXC se crean como Unprivileged container

---

Revision #1
Created 17 May 2022 17:06:56 by Admin
Updated 17 May 2022 17:10:28 by Admin