Doble Factor de autenticación en Proxmox VE

En primer lugar y como "disclaimer"

> NO ES ACONSEJABLE PONER UN PROXMOX EN PRODUCCIÓN SIN NINGÚN TIPO DE PROTECCIÓN.

Dicho esto, si necesitas hacerlo, te aconsejamos pone un firewall basado en iptables, o mejor aún en nftables

Hay dos formas de utilizar la autenticación de dos factores:

Puede ser requerido por el dominio o realm de autenticación, ya sea a través de TOTP (contraseña de un solo uso basada en tiempo) o YubiKey OTP. En este caso, a un usuario recién creado se le deben agregar sus claves inmediatamente, **ya que no hay forma de iniciar sesión sin el segundo factor.** En el caso de TOTP, los usuarios también pueden cambiar el TOTP más adelante, siempre que puedan iniciar sesión primero.

Alternativamente, los usuarios pueden optar por optar por la autenticación de dos factores más adelante, incluso si el realmno la aplica.

Segundos factores de autenticación disponibles

Puedes configurar varios segundos factores para evitar una situación en la que perder tu teléfono inteligente o tu llave de seguridad lo bloquee permanentemente de tu cuenta.

Los siguientes métodos de autenticación de dos factores están disponibles además de TOTP aplicado por realm y YubiKey OTP:

TOTP

Contraseña de un solo uso basada en tiempo configurada por el usuario. Un código corto derivado de un secreto compartido y la hora actual, cambia cada 30 segundos.

WebAuthn

Autenticación web. Un estándar general para la autenticación. Se implementa mediante varios dispositivos de seguridad, como claves de hardware o módulos de plataforma confiable (TPM) desde un ordenador o teléfono inteligente.

Claves de recuperación de un solo uso.

Una lista de claves que deben imprimirse y guardarse bajo llave en un lugar seguro o guardarse digitalmente en un vault o sistema de almacenamiento de claves electrónico. Cada clave se puede utilizar sólo una vez. Estos son perfectos para garantizar que no quede bloqueado, incluso si todos los demás factores secundarios se pierden o se corrompen.

Antes de que WebAuthn fuera compatible, el usuario podía configurar U2F. Aún se pueden utilizar los factores U2F existentes, pero se recomienda cambiar a WebAuthn, una vez que esté configurado en el servidor.

Autenticación de dos factores (TFA) reforzada en el Realm

Esto se puede hacer seleccionando uno de los métodos disponibles a través del cuadro desplegable de TFA al agregar o editar un dominio o realm de autenticación. Cuando un dominio tiene TFA habilitado, se convierte en un requisito y solo los usuarios con TFA configurado podrán iniciar sesión.

Actualmente hay dos métodos disponibles:

Time-based OATH (TOTP)

Esto utiliza el algoritmo estándar HMAC-SHA1, donde la hora actual se codifica con la clave configurada por el usuario. Los parámetros de tiempo transcurrido y longitud de la contraseña son configurables.

Un usuario puede tener varias claves configuradas (separadas por espacios) y las claves se pueden especificar en Base32 (RFC3548) o notación hexadecimal.

Proxmox VE proporciona una herramienta de generación de claves (oathkeygen) que imprime una clave aleatoria en notación Base32, que se puede usar directamente con varias herramientas OTP, como la herramienta de línea de comandos oathtool, o en Android Google Authenticator, Authy, FreeOTP, andOTP o aplicaciones similares.

OTP de YubiKey

Para autenticarse a través de una YubiKey, se debe configurar una ID de API de Yubico, una CLAVE de API y una URL del servidor de validación, y los usuarios deben tener una YubiKey disponible. Para obtener la ID de clave de una YubiKey, puede activar la YubiKey una vez después de conectarla a través de USB y copiar los primeros 12 caracteres de la contraseña ingresada en el campo de ID de clave del usuario.

Consulta la documentación de YubiKey OTP para saber cómo utilizar YubiCloud o alojar t propio servidor de verificación.

Límites y bloqueo de la autenticación de dos factores

Un segundo factor está destinado a proteger a los usuarios si su contraseña se filtra o se adivina de alguna manera. Sin embargo, algunos factores aún podrían romperse mediante la fuerza bruta. Por este motivo, los usuarios quedarán bloqueados después de demasiados intentos fallidos de inicio de sesión del segundo factor.

Para TOTP, 8 intentos fallidos desactivarán los factores TOTP del usuario. Se desbloquean al iniciar sesión con una clave de recuperación. Si TOTP era el único factor disponible, se requiere la intervención del administrador y se recomienda encarecidamente solicitar al usuario que cambie su contraseña de inmediato.

Dado que FIDO2/Webauthn y las claves de recuperación son menos susceptibles a ataques de fuerza bruta, el límite es mayor (100 intentos), pero todos los segundos factores se bloquean durante una hora cuando se exceden.

Un administrador puede desbloquear la autenticación de dos factores de un usuario en cualquier momento a través de la lista de usuarios en la interfaz de usuario o mediante el siguiente comando:

```
pveum user tfa unlock etaboada@pve
```

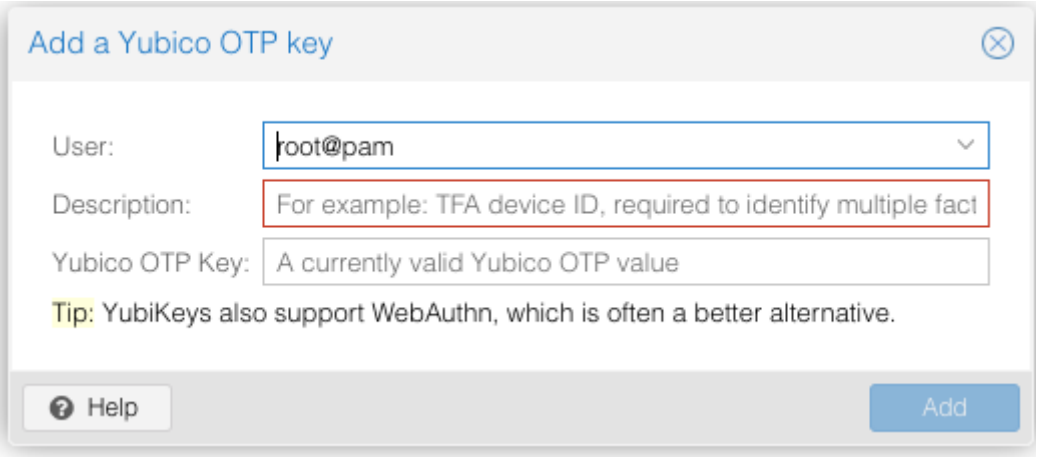
Autenticación TOTP configurada por el usuario

Los usuarios pueden optar por habilitar TOTP o WebAuthn como segundo factor al iniciar sesión, a través del botón TFA en la lista de usuarios (a menos que el realm use YubiKey OTP).

Los usuarios siempre pueden agregar y usar claves de recuperación únicas. Después de abrir la ventana TFA, se presenta al usuario un cuadro de diálogo para configurar la autenticación TOTP. El campo Secreto contiene la clave, que se puede generar aleatoriamente mediante el botón

Aleatorizar. Se puede agregar un nombre de emisor opcional para proporcionar información a la aplicación TOTP sobre a qué pertenece la clave. La mayoría de las aplicaciones TOTP mostrarán el nombre del emisor junto con los valores OTP correspondientes. El nombre de usuario también está incluido en el código QR de la aplicación TOTP.

Después de generar una clave, se mostrará un código QR, que se puede usar con la mayoría de las aplicaciones OTP, como FreeOTP o Authy. Luego, el usuario debe verificar la contraseña de usuario actual (a menos que haya iniciado sesión como root), así como la capacidad de usar correctamente la clave TOTP, escribiendo el valor OTP actual en el campo Código de verificación y presionando el botón Aplicar.



TOTP

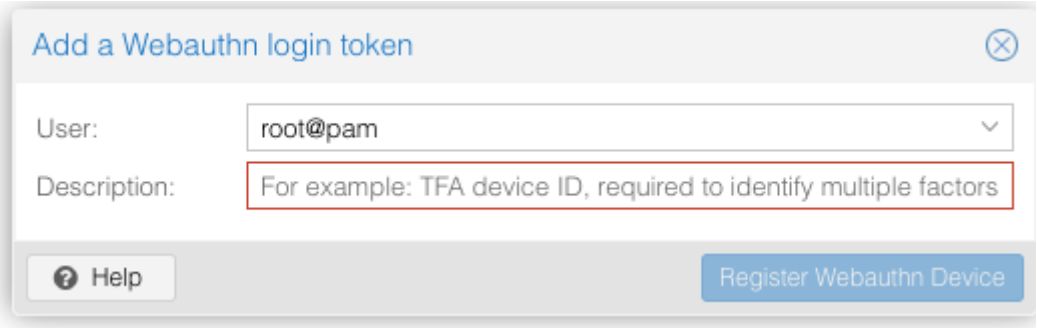
No se requiere configuración del servidor. Simplemente instala una aplicación TOTP en tu teléfono inteligente (por ejemplo, FreeOTP o Authy) y usa la interfaz web de Proxmox Backup Server para agregar un factor TOTP.

WebAuthn

Para que WebAuthn funcione, es necesario tener dos cosas:

1. Un certificado HTTPS confiable (por ejemplo, usando Let's Encrypt). Si bien probablemente funcione con un certificado que no sea de confianza, algunos navegadores pueden advertir o rechazar operaciones de WebAuthn si no es de confianza.
2. Configure la configuración de WebAuthn (Centro de datos → Opciones → Configuración de WebAuthn en la interfaz web de Proxmox VE). Esto se puede completar automáticamente en la mayoría de las configuraciones.

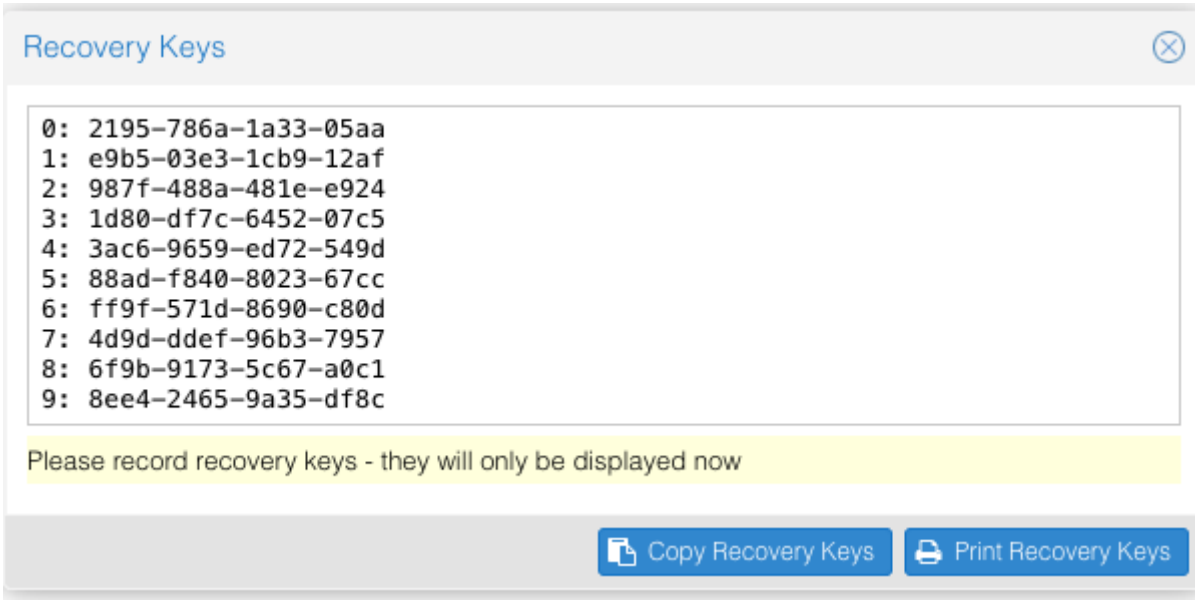
Una vez que se haya cumplido ambos requisitos, puedes agregar una configuración de WebAuthn en el panel Two Factor en Centro de datos → Permisos → Two Factor.



Claves de recuperación

Los códigos de clave de recuperación no necesitan ninguna preparación; simplemente puedes crear un conjunto de claves de recuperación en el panel Two Factor en Centro de datos → Permisos → Two Factor.

> Nota Solo puede haber un conjunto de claves de recuperación de un solo uso por usuario en cualquier momento.



Configuración de Webauthn del lado del servidor

Para permitir a los usuarios utilizar la autenticación WebAuthn, es necesario utilizar un dominio válido con un certificado SSL válido; de lo contrario, algunos navegadores pueden advertir o negarse a autenticarse por completo.

> Nota ¡Cambiar la configuración de WebAuthn puede inutilizar todos los registros de WebAuthn existentes!

Esto se hace a través de /etc/pve/datacenter.cfg. Por ejemplo:

```
webauthn:
rp=hv9.tecnocratica.net,origin=https://hv9.tecnocratica.net:8006,id=hv9.tecnocratica.net
```

Configuración U2F del lado del servidor

> Nota Se recomienda utilizar WebAuthn en su lugar.

Para permitir a los usuarios utilizar la autenticación U2F, puede ser necesario utilizar un dominio válido con un certificado SSL válido; de lo contrario, algunos navegadores pueden imprimir una advertencia o rechazar el uso de U2F por completo. Inicialmente, es necesario configurar un AppId

[1].

> Nota ¡Cambiar el AppId inutilizará todos los registros U2F existentes!

Esto se hace a través de /etc/pve/datacenter.cfg. Por ejemplo:

```
u2f: appid=https://hv9.tecnocratica.net:8006
```

Para un solo nodo, AppId puede ser simplemente la dirección de la interfaz web, exactamente como se usa en el navegador, incluido https:// y el puerto, como se muestra arriba. Ten en cuenta que algunos navegadores pueden ser más estrictos que otros al hacer coincidir los AppIds.

Cuando se utilizan varios nodos, es mejor tener un servidor https independiente que proporcione un archivo **appid.json**, ya que parece ser compatible con la mayoría de los navegadores. Si todos los nodos usan subdominios del mismo dominio de nivel superior, puede ser suficiente usar el TLD como AppId. Sin embargo, cabe señalar que es posible que algunos navegadores no lo acepten.

> Nota Un AppId incorrecto generalmente producirá un error, pero nos hemos encontrado con situaciones en las que esto no sucede, particularmente cuando se usa un AppId de dominio de nivel superior para un nodo al que se accede a través de un subdominio en Chromium. Por este motivo, se recomienda probar la configuración con varios navegadores, ya que cambiar el AppId más adelante inutilizará los registros U2F existentes.

Activando U2F como usuario

Para habilitar la autenticación U2F, abre la pestaña U2F de la ventana TFA, escribe la contraseña actual (a menos que hayas iniciado sesión como root) y presiona el botón Registrar. Si el servidor está configurado correctamente y el navegador acepta el AppId proporcionado por el servidor, aparecerá un mensaje solicitando al usuario que presione el botón en el dispositivo U2F (si es una YubiKey, la luz del botón debe encenderse y apagarse de manera constante, aproximadamente dos veces por segundo).

> Es posible que los usuarios de Firefox necesiten habilitar security.webauth.u2f a través de about:config antes de poder usar un token U2F.

Revision #1
Created 28 January 2024 08:11:14 by etaboada
Updated 28 January 2024 08:44:44 by etaboada