VERACRYPT

FUENTE ABIERTA - LIBRE - EN - LA - ENCRIPCIÓN DE FLYENCRYPTION

GUÍA DEL USUARIO

veracrypt.codeplex.com

Información de la versión

Guía del usuario de VeraCrypt, versión 1.18
Lanzado por IDRIX el 17 de agosto , (2016)

CONTENIDO

Tenga en cuenta que, si bien la mayoría de los capítulos de esta documentación se aplican a todas las versiones de VeraCrypt, algunas secciones están dirigidas principalmente a los usuarios de las versiones de VeraCrypt para Windows. Por lo tanto, dichas secciones pueden contener información inapropiada para las versiones de VeraCrypt para Mac OS X y Linux.

Introducción

VeraCrypt es un sistema de software para establecer y mantener un volumen (dispositivo de almacenamiento de datos) cifrado sobre la marcha. El cifrado sobre la marcha significa que los datos se cifran automáticamente justo antes de guardarlos y se descifran justo después de cargarlos, sin intervención del usuario. Ningún dato almacenado en un volumen cifrado se puede leer (descifrar) sin usar la contraseña, el archivo o los archivos de claves correctos o las claves de cifrado correctas. Todo el sistema de archivos está cifrado (por ejemplo, nombres de archivos, nombres de carpetas, contenido de cada archivo, espacio libre, metadatos, etc.).

Los archivos se pueden copiar hacia y desde un volumen VeraCrypt montado, igual que se copian hacia o desde cualquier disco normal (por ejemplo, con simples operaciones de arrastrar y soltar). Los archivos se descifran automáticamente sobre la marcha (en memoria/RAM) mientras se leen o copian desde un volumen VeraCrypt cifrado. De igual forma, los archivos que se escriben o copian en el volumen VeraCrypt se cifran automáticamente sobre la marcha (justo antes de escribirse en el disco) en RAM. Tenga en cuenta que esto no significa que todo el archivo que se va a cifrar/descifrar deba almacenarse en RAM antes de poder cifrarlo/descifrarlo. VeraCrypt no requiere memoria RAM adicional. Para ver cómo se realiza esto, consulte el siguiente párrafo.

Supongamos que hay un archivo de vídeo .avi almacenado en un volumen VeraCrypt (por lo tanto, el archivo de vídeo está completamente cifrado). El usuario proporciona la contraseña correcta (y/o el archivo de claves) y monta (abre) el volumen VeraCrypt. Al hacer doble clic en el icono del archivo de vídeo, el sistema operativo inicia la aplicación asociada al tipo de archivo, normalmente un reproductor multimedia. El reproductor empieza a cargar una pequeña parte inicial del archivo de vídeo desde el volumen cifrado con VeraCrypt a la RAM para reproducirlo. Mientras se carga la parte, VeraCrypt la descifra automáticamente (en RAM). El reproductor reproduce la parte descifrada del vídeo (almacenada en RAM). Mientras se reproduce esta parte, el reproductor empieza a cargar otra pequeña parte del archivo de vídeo desde el volumen cifrado con VeraCrypt a la RAM y el proceso se repite. Este proceso se llama cifrado/descifrado sobre la marcha y funciona para todos los tipos de archivos (no solo para archivos de vídeo).

Tenga en cuenta que VeraCrypt nunca guarda los datos descifrados en un disco; solo los almacena temporalmente en la memoria RAM. Incluso cuando el volumen está montado, los datos almacenados en él siguen cifrados. Al reiniciar Windows o apagar el ordenador, el volumen se desmontará y los archivos almacenados en él serán inaccesibles (y estarán cifrados). Incluso si se interrumpe repentinamente el suministro eléctrico (sin apagar el sistema correctamente), los archivos almacenados en el volumen serán inaccesibles (y estarán cifrados). Para volver a acceder a ellos, debe montar el volumen (y proporcionar la contraseña o el archivo de claves correctos). Para obtener una guía de inicio rápido, consulte el capítulo " Tutorial para principiantes".

Tutorial para principiantes

Cómo crear y utilizar un contenedor VeraCrypt

Este capítulo contiene instrucciones paso a paso sobre cómo crear, montar y usar un volumen VeraCrypt. Le recomendamos encarecidamente que lea también las demás secciones de este manual, ya que contienen información importante.

PASO 1:

Si aún no lo ha hecho, descargue e instale VeraCrypt. A continuación, inícielo haciendo doble clic en el archivo VeraCrypt.exe o haciendo clic en el acceso directo de VeraCrypt en el menú Inicio de Windows.

PASO 2:

Debería aparecer la ventana principal de VeraCrypt. Haga clic en Crear volumen (marcado con un rectángulo rojo para mayor claridad).

PASO 3:

Debería aparecer la ventana del Asistente de creación de volumen de VeraCrypt.

En este paso, debe elegir dónde desea crear el volumen VeraCrypt. Un volumen VeraCrypt puede residir en un archivo, también llamado contenedor, en una partición o unidad. En este tutorial, elegiremos la primera opción y crearemos un volumen VeraCrypt dentro de un archivo.

Como la opción está seleccionada de forma predeterminada, puedes simplemente hacer clic en Siguiente.

Nota: En los siguientes pasos, las capturas de pantalla mostrarán solo la parte derecha de la ventana del Asistente.

PASO 4:

En este paso, debe elegir si desea crear un volumen VeraCrypt estándar u oculto. En este tutorial, elegiremos la primera opción y crearemos un volumen VeraCrypt estándar.

Como la opción está seleccionada de forma predeterminada, puedes simplemente hacer clic en Siguiente.

PASO 5:

En este paso, debe especificar dónde desea crear el volumen VeraCrypt (contenedor de archivos). Tenga en cuenta que un contenedor VeraCrypt es como cualquier archivo normal. Puede, por ejemplo, moverse o eliminarse como cualquier archivo normal. También necesita un nombre de archivo, que elegirá en el siguiente paso.

Haga clic en Seleccionar archivo.

Debería aparecer el selector de archivos estándar de Windows (mientras la ventana del Asistente de creación de volumen de VeraCrypt permanece abierta en segundo plano).

PASO 6:

En este tutorial, crearemos nuestro volumen VeraCrypt en la carpeta F:\Data\ y el nombre del archivo (contenedor) será Mi Volumen (como se puede ver en la captura de pantalla anterior). Por supuesto, puede elegir cualquier otro nombre de archivo y ubicación que desee (por ejemplo, en una memoria USB).
Tenga en cuenta que el archivo Mi Volumen aún no existe: VeraCrypt lo creará.

IMPORTANTE: Tenga en cuenta que VeraCrypt no cifrará ningún archivo existente (al crear un contenedor de archivos VeraCrypt).
Si selecciona un archivo existente en este paso, se sobrescribirá y será reemplazado por el volumen recién creado (por lo tanto, el archivo sobrescrito se perderá , no se cifrará).
Podrás cifrar archivos existentes (más adelante) moviéndolos al volumen VeraCrypt que estamos creando ahora.*

Seleccione la ruta deseada (donde desea que se cree el contenedor) en el selector de archivos.

Escriba el nombre del archivo contenedor deseado en el cuadro Nombre de archivo .

Haga clic en Guardar.

La ventana del selector de archivos debería desaparecer.

En los siguientes pasos, regresaremos al Asistente de creación de volumen de VeraCrypt.

---

* Tenga en cuenta que, tras copiar archivos sin cifrar a un volumen VeraCrypt, debe borrar de forma segura los archivos originales sin cifrar. Existen herramientas de software que permiten el borrado seguro (muchas de ellas gratuitas).

PASO 7:

En la ventana del Asistente para creación de volumen, haga clic en Siguiente.

PASO 8:

Aquí puede elegir un algoritmo de cifrado y un algoritmo hash para el volumen. Si no está seguro de qué seleccionar, puede usar la configuración predeterminada y hacer clic en Siguiente (para más información, consulte los capítulos Algoritmos de cifrado y Algoritmos hash).

PASO 9:

Aquí especificamos que el tamaño de nuestro contenedor VeraCrypt debe ser de 250 megabytes. Por supuesto, puede especificar un tamaño diferente. Después de escribir el tamaño deseado en el campo de entrada (marcado con un rectángulo rojo), haga clic en Siguiente.

PASO 10:

Este es uno de los pasos más importantes. Aquí debes elegir una buena contraseña de volumen.

Lea atentamente la información que se muestra en la ventana del Asistente sobre lo que se considera una buena contraseña.

Después de elegir una contraseña adecuada, escríbala en el primer campo de entrada. Luego, vuelva a escribirla en el campo de entrada debajo de la primera y haga clic en Siguiente.

Nota: El botón Siguiente estará deshabilitado hasta que las contraseñas en ambos campos de entrada sean las mismas.

PASO 11:

Mueva el ratón de la forma más aleatoria posible dentro de la ventana del Asistente de creación de volúmenes, al menos hasta que el indicador de aleatoriedad se ponga verde. Cuanto más tiempo mueva el ratón, mejor (se recomienda moverlo durante al menos 30 segundos). Esto aumenta significativamente la solidez criptográfica de las claves de cifrado (lo que aumenta la seguridad).

Haga clic en Formato.

Debería comenzar la creación del volumen. VeraCrypt creará un archivo llamado Mi Volumen en la carpeta F: \Data\ (como especificamos en el paso 6). Este archivo será un contenedor de VeraCrypt (contendrá el volumen cifrado de VeraCrypt). Dependiendo del tamaño del volumen, la creación del volumen puede tardar bastante. Al finalizar, aparecerá el siguiente cuadro de diálogo:

Haga clic en Aceptar para cerrar el cuadro de diálogo.

PASO 12:

Acabamos de crear con éxito un volumen VeraCrypt (contenedor de archivos).

En la ventana del Asistente de creación de volumen de VeraCrypt, haga clic en Salir.

La ventana del asistente debería desaparecer.

En los pasos restantes, montaremos el volumen que acabamos de crear. Regresaremos a la ventana principal de VeraCrypt (que debería seguir abierta, pero si no lo está, repita el paso 1 para iniciar VeraCrypt y luego continúe desde el paso 13).

PASO 13:

Seleccione una letra de unidad de la lista (marcada con un rectángulo rojo). Esta será la letra de unidad donde se montará el contenedor de VeraCrypt.

Nota: En este tutorial, elegimos la letra de unidad M, pero por supuesto puedes elegir cualquier otra letra de unidad disponible.

PASO 14:

Haga clic en Seleccionar archivo.

Debería aparecer la ventana del selector de archivos estándar.

PASO 15:

En el selector de archivos, busque el archivo contenedor (que creamos en los pasos 6 a 11) y selecciónelo.

Haga clic en Abrir (en la ventana del selector de archivos).

La ventana del selector de archivos debería desaparecer.

En los siguientes pasos, regresaremos a la ventana principal de VeraCrypt.

PASO 16:

En la ventana principal de VeraCrypt, haga clic en Montar. Contraseña

Debería aparecer una ventana de diálogo de aviso.

PASO 17:

Escriba la contraseña (que especificó en el paso 10) en el campo de ingreso de contraseña (marcado con un rectángulo rojo).

PASO 18:

Seleccione el algoritmo PRF utilizado durante la creación del volumen (SHA-512 es el PRF predeterminado que usa VeraCrypt). Si no recuerda qué PRF se utilizó, simplemente déjelo en "detección automática", pero el proceso de montaje tardará más. Haga clic en "Aceptar" después de introducir la contraseña.

VeraCrypt intentará montar el volumen. Si la contraseña es incorrecta (por ejemplo, si la escribió mal), VeraCrypt le notificará y deberá repetir el paso anterior (volver a escribir la contraseña y hacer clic en Aceptar). Si la contraseña es correcta, el volumen se montará.

PASO FINAL :

Acabamos de montar con éxito el contenedor como un disco virtual M:

El disco virtual está completamente cifrado (incluidos los nombres de archivo, las tablas de asignación, el espacio libre, etc.) y se comporta como un disco real. Puede guardar (o copiar, mover, etc.) archivos en este disco virtual y se cifrarán automáticamente a medida que se escriben.

Si abre un archivo almacenado en un volumen VeraCrypt, por ejemplo, en un reproductor multimedia, el archivo se descifrará automáticamente en RAM (memoria) sobre la marcha mientras se lee.

Importante: Tenga en cuenta que al abrir un archivo almacenado en un volumen VeraCrypt (o al escribir/copiar un archivo en/desde el volumen VeraCrypt), no se le solicitará que vuelva a introducir la contraseña. Solo deberá introducir la contraseña correcta al montar el volumen.

Puede abrir el volumen montado, por ejemplo, seleccionándolo en la lista como se muestra en la captura de pantalla anterior (selección azul) y luego haciendo doble clic en el elemento seleccionado.

También puede acceder al volumen montado como lo haría normalmente con cualquier otro tipo de volumen. Por ejemplo, abra la lista "Equipo" (o "Mi PC") y haga doble clic en la letra de unidad correspondiente (en este caso, la M).

Puede copiar archivos (o carpetas) hacia y desde el volumen VeraCrypt tal como lo haría a cualquier disco normal (por ejemplo, con simples operaciones de arrastrar y soltar). Los archivos que se leen o copian desde el volumen VeraCrypt cifrado se descifran automáticamente sobre la marcha en la RAM (memoria). De igual forma, los archivos que se escriben o copian en el volumen VeraCrypt se cifran automáticamente sobre la marcha en la RAM (justo antes de escribirse en el disco).

Tenga en cuenta que VeraCrypt nunca guarda los datos descifrados en un disco; solo los almacena temporalmente en la memoria RAM. Incluso cuando el volumen está montado, los datos almacenados en él siguen cifrados. Al reiniciar Windows o apagar el equipo, el volumen se desmontará y todos los archivos almacenados en él serán inaccesibles (y estarán cifrados). Incluso si se interrumpe repentinamente el suministro eléctrico (sin apagar el sistema correctamente), todos los archivos almacenados en el volumen serán inaccesibles (y estarán cifrados). Para volver a tenerlos accesibles, debe montar el volumen. Para ello, repita los pasos 13 a 18.

Si desea cerrar el volumen y hacer que los archivos almacenados en él sean inaccesibles, reinicie el sistema operativo o desmonte el volumen. Para ello, siga estos pasos:

Seleccione el volumen de la lista de volúmenes montados en la ventana principal de VeraCrypt (marcado con un rectángulo rojo en la captura de pantalla anterior) y haga clic en Desmontar (también marcado con un rectángulo rojo en la captura de pantalla anterior). Para que los archivos almacenados en el volumen vuelvan a ser accesibles, deberá montarlo. Para ello, repita los pasos 13-18.

Cómo crear y utilizar una partición o dispositivo cifrado con VeraCrypt

En lugar de crear contenedores de archivos, también puede cifrar particiones o unidades físicas (es decir, crear volúmenes VeraCrypt alojados en dispositivos). Para ello, repita los pasos 1 a 3, pero en el paso 3 seleccione la segunda o la tercera opción. A continuación, siga las instrucciones restantes del asistente. Al crear un volumen VeraCrypt alojado en dispositivos dentro de una partición o unidad que no sea del sistema , puede montarlo haciendo clic en "Montar dispositivos automáticamente" en la ventana principal de VeraCrypt. Para obtener información sobre particiones o unidades del sistema cifradas , consulte el capítulo "Cifrado del sistema".

Importante: Le recomendamos encarecidamente que lea también los demás capítulos de este manual, ya que contienen información importante que se ha omitido en este tutorial para simplificar.

Volumen de VeraCrypt

Hay dos tipos de volúmenes de VeraCrypt: • Alojado en
archivos (contenedor) • Alojado en
particiones/dispositivos (no sistema)

Nota: Además de crear los tipos de volúmenes virtuales mencionados anteriormente, VeraCrypt puede cifrar una partición/unidad física donde esté instalado Windows (para obtener más información, consulte el capítulo Cifrado del sistema).

Un volumen alojado en archivos de VeraCrypt es un archivo normal que puede residir en cualquier tipo de dispositivo de almacenamiento. Contiene (aloja) un dispositivo de disco virtual cifrado completamente independiente.

Una partición VeraCrypt es una partición de disco duro cifrada con VeraCrypt. También puede cifrar discos duros completos, discos duros USB, memorias USB y otros tipos de dispositivos de almacenamiento.

Creación de un nuevo volumen de VeraCrypt

Para crear un nuevo volumen alojado en archivos de VeraCrypt o cifrar una partición/dispositivo (requiere privilegios de administrador), haga clic en "Crear volumen" en la ventana principal del programa. Debería aparecer el Asistente para la creación de volúmenes de VeraCrypt. En cuanto aparezca, el Asistente comenzará a recopilar datos que se utilizarán para generar la clave maestra, la clave secundaria (modo XTS) y la sal del nuevo volumen.
Los datos recopilados, que deben ser lo más aleatorios posible, incluyen los movimientos del ratón, las pulsaciones de teclas y otros valores obtenidos del sistema (para más información, consulte la sección " Generador de números aleatorios"). El asistente proporciona la ayuda y la información necesarias para crear correctamente un nuevo volumen de VeraCrypt. Sin embargo, varios elementos requieren una explicación más detallada:

Algoritmo hash

Permite seleccionar el algoritmo hash que VeraCrypt utilizará. El algoritmo hash seleccionado es utilizado por el generador de números aleatorios (como una función de mezcla pseudoaleatoria), que genera la clave maestra, la clave secundaria (modo XTS) y la sal (para más información, consulte la sección " Generador de Números Aleatorios"). También se utiliza para derivar la nueva clave de encabezado de volumen y la clave de encabezado secundaria (consulte la sección " Derivación de Clave de Encabezado, Sal y Número de Iteraciones").

Para obtener información sobre los algoritmos hash implementados, consulte el capítulo Algoritmos hash.

Tenga en cuenta que la salida de una función hash nunca se utiliza directamente como clave de cifrado. Para más información, consulte el capítulo " Detalles técnicos".

Algoritmo de cifrado

Esto le permite seleccionar el algoritmo de cifrado con el que se cifrará su nuevo volumen.
Tenga en cuenta que el algoritmo de cifrado no se puede modificar una vez creado el volumen. Para más información, consulte el capítulo "Algoritmos de cifrado".

Formato rápido

Si no está marcada, se formateará cada sector del nuevo volumen. Esto significa que el nuevo volumen se llenará completamente con datos aleatorios. El formato rápido es mucho más rápido, pero puede ser menos seguro, ya que hasta que el volumen esté lleno de archivos, es posible determinar la cantidad de datos que contiene (si el espacio no se llenó previamente con datos aleatorios). Si no está seguro de si debe activar o desactivar el formato rápido, le recomendamos que deje esta opción sin marcar. Tenga en cuenta que el formato rápido solo se puede activar al cifrar particiones o dispositivos.
Importante: al cifrar una partición/dispositivo dentro del cual posteriormente desea crear un volumen oculto, deje esta opción sin marcar.

Dinámica

El contenedor dinámico VeraCrypt es un archivo disperso NTFS preasignado cuyo tamaño físico (espacio en disco real utilizado) aumenta a medida que se le añaden nuevos datos. Tenga en cuenta que el tamaño físico del contenedor (espacio en disco real que utiliza) no disminuye al eliminar archivos del volumen VeraCrypt. El tamaño físico del contenedor solo puede aumentar hasta el valor máximo especificado por el usuario durante la creación del volumen. Una vez alcanzado el tamaño máximo especificado, el tamaño físico del contenedor se mantendrá constante.

Tenga en cuenta que los archivos dispersos solo se pueden crear en el sistema de archivos NTFS. Si crea un contenedor en el sistema de archivos FAT, la opción Dinámica estará deshabilitada ("atenuada").

Tenga en cuenta que el tamaño de un volumen dinámico de VeraCrypt (alojado en archivos dispersos) informado por Windows y por VeraCrypt siempre será igual a su tamaño máximo (que se especifica al crear el volumen). Para conocer el tamaño físico actual del contenedor (el espacio en disco real que ocupa), haga clic con el botón derecho en el archivo contenedor (en una ventana del Explorador de Windows, no en VeraCrypt), seleccione Propiedades y consulte el valor de Tamaño en disco .

ADVERTENCIA: El rendimiento de los volúmenes dinámicos de VeraCrypt (alojados en archivos dispersos) es significativamente inferior al de los volúmenes regulares. Además, estos volúmenes son menos seguros, ya que es posible identificar qué sectores del volumen no se utilizan. Además, si se escriben datos en un volumen dinámico cuando no hay suficiente espacio libre en el sistema de archivos que lo aloja, el sistema de archivos cifrado podría dañarse.

Tamaño del clúster

Un clúster es una unidad de asignación. Por ejemplo, se asigna un clúster en un sistema de archivos FAT para un archivo de un byte. Cuando el archivo supera los límites del clúster, se asigna otro clúster.
En teoría, esto significa que cuanto mayor sea el tamaño del clúster, más espacio en disco se desperdicia; sin embargo, mejor será el rendimiento. Si no sabe qué valor usar, utilice el predeterminado.

Volúmenes de VeraCrypt en CD y DVD

Si desea almacenar un volumen de VeraCrypt en un CD o un DVD, primero cree un contenedor de VeraCrypt alojado en un disco duro y luego grábelo en un CD/DVD usando cualquier software de grabación de CD/DVD (o, en Windows XP o posterior, usando la herramienta de grabación de CD proporcionada con el sistema operativo).
Recuerde que si necesita montar un volumen VeraCrypt almacenado en un medio de solo lectura (como un CD/DVD) en Windows 2000, debe formatearlo como FAT. Esto se debe a que Windows 2000 no puede montar el sistema de archivos NTFS en medios de solo lectura (Windows XP y versiones posteriores sí pueden).

RAID de hardware/software, volúmenes dinámicos de Windows

VeraCrypt admite RAID de hardware/software, así como volúmenes dinámicos de Windows.

Windows Vista o posterior: los volúmenes dinámicos se muestran en la ventana de diálogo "Seleccionar dispositivo" como \Device\HarddiskVolumeN.

Windows XP/2000/2003: Si desea formatear un volumen dinámico de Windows como un volumen VeraCrypt, tenga en cuenta que, tras crearlo (con la herramienta Administración de discos de Windows), debe reiniciar el sistema operativo para que el volumen esté disponible o se muestre en el cuadro de diálogo "Seleccionar dispositivo" del Asistente para la creación de volúmenes VeraCrypt. Tenga en cuenta también que, en el cuadro de diálogo "Seleccionar dispositivo", un volumen dinámico de Windows no se muestra como un único dispositivo (elemento). En su lugar, se muestran todos los volúmenes que lo componen, y puede seleccionar cualquiera de ellos para formatearlo por completo .

Notas adicionales sobre la creación de volúmenes

Tras hacer clic en el botón "Formatear" en la ventana del Asistente de Creación de Volumen (el último paso), se producirá una breve demora mientras se sondea el sistema para obtener datos aleatorios adicionales. Posteriormente, se generarán la clave maestra, la clave de encabezado, la clave secundaria (modo XTS) y la sal del nuevo volumen, y se mostrará el contenido de ambas.

Para mayor seguridad, se puede evitar que se muestren las partes del grupo de aleatoriedad, la clave maestra y la clave de encabezado desmarcando la casilla de verificación en la esquina superior derecha del campo correspondiente:

Tenga en cuenta que solo se muestran los primeros 128 bits del grupo/claves (no todo el contenido).

Puede crear volúmenes FAT (FAT12, FAT16 o FAT32, que se determina automáticamente según el número de clústeres) o NTFS (sin embargo, los volúmenes NTFS solo pueden ser creados por usuarios con privilegios de administrador). Los volúmenes VeraCrypt montados se pueden reformatear a FAT12, FAT16, FAT32 o NTFS en cualquier momento. Funcionan como dispositivos de disco estándar, por lo que puede hacer clic con el botón derecho en la letra de la unidad del volumen VeraCrypt montado (por ejemplo, en la lista "Equipo" o "Mi PC") y seleccionar "Formatear".

Para obtener más información sobre la creación de volúmenes VeraCrypt, consulte también la sección Volumen oculto.

Volúmenes favoritos

Los volúmenes favoritos son útiles, por ejemplo, en cualquiera de los siguientes casos:

- Tiene un volumen que siempre debe montarse en una letra de unidad particular.
- Tiene un volumen que necesita montarse automáticamente cuando su dispositivo host se conecta a la computadora (por ejemplo, un contenedor ubicado en una unidad flash USB o un disco duro USB externo).
- Tiene un volumen que debe montarse automáticamente cuando inicia sesión en el sistema operativo.
- Tiene un volumen que siempre debe montarse como medio de solo lectura o extraíble.

Para configurar un volumen de VeraCrypt como volumen favorito, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic con el botón derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione 'Añadir a favoritos'.
3. Debería aparecer la ventana Organizador de Volúmenes Favoritos. En esta ventana, puede configurar varias opciones para el volumen (ver más abajo).
4. Haga clic en Aceptar.

Los volúmenes favoritos se pueden montar de varias maneras: Para montar todos los volúmenes favoritos, seleccione Favoritos > Montar volúmenes favoritos o pulse la tecla de acceso rápido "Montar volúmenes favoritos" (Configuración > Teclas de acceso rápido). Para montar solo uno de los volúmenes favoritos, selecciónelo de la lista del menú Favoritos . Al hacerlo, se le solicitará su contraseña (y/o archivos de claves) (a menos que esté en caché) y, si es correcta, se montará el volumen. Si ya está montado, se abrirá una ventana del Explorador.

Se pueden montar automáticamente los volúmenes favoritos seleccionados o todos al iniciar sesión en Windows. Para configurarlo, siga estos pasos:

1. Monte el volumen que desea que se monte automáticamente al iniciar sesión (móntelo) a la letra de unidad en la que desea que se monte cada vez).
2. Haga clic derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione “Agregar a favoritos”.
3. Debería aparecer la ventana Organizador de favoritos. En esta ventana, active la opción 'Montar el volumen seleccionado al iniciar sesión' y haga clic en Aceptar.

Luego, cuando inicie sesión en Windows, se le solicitará la contraseña del volumen (y/o los archivos de clave) y, si es correcta, se montará el volumen.

Nota: VeraCrypt no le solicitará una contraseña si ha habilitado el almacenamiento en caché de la contraseña de autenticación previa al arranque (Configuración > 'Cifrado del sistema') y los volúmenes usan la misma contraseña que la partición/unidad del sistema.

Se pueden montar automáticamente algunos o todos los volúmenes favoritos al conectar su dispositivo host al ordenador. Para configurarlo, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic con el botón derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione 'Añadir a favoritos'.
3. Debería aparecer la ventana Organizador de Favoritos. En esta ventana, active la opción "Montar el volumen seleccionado al conectar su dispositivo host" y haga clic en Aceptar.

Luego, cuando inserta, por ejemplo, una unidad flash USB que contiene un volumen VeraCrypt en el puerto USB, se le solicitará la contraseña del volumen (y/o los archivos de clave) (a menos que esté almacenado en caché) y, si es correcta, se montará el volumen.

Nota: VeraCrypt no le solicitará una contraseña si ha habilitado el almacenamiento en caché de la contraseña de autenticación previa al arranque (Configuración > 'Cifrado del sistema') y el volumen usa la misma contraseña que la partición/unidad del sistema.

Se puede asignar una etiqueta especial a cada volumen favorito. Esta etiqueta no es la misma que la del sistema de archivos y se muestra en la interfaz de usuario de VeraCrypt en lugar de la ruta del volumen. Para asignar dicha etiqueta, siga estos pasos:

1. Seleccione Favoritos > 'Organizar volúmenes favoritos'.
2. Debería aparecer la ventana "Organizador de Volúmenes Favoritos". En esta ventana, seleccione el volumen cuya etiqueta desea editar.
3. Ingrese la etiqueta en el campo de entrada 'Etiqueta del volumen favorito seleccionado' y haga clic en Aceptar.

Tenga en cuenta que la ventana Organizador de Volúmenes Favoritos (Favoritos > Organizar Volúmenes Favoritos) le permite configurar otras opciones para cada volumen favorito. Por ejemplo, cualquiera de ellos puede montarse como de solo lectura o como medio extraíble. Para configurar cualquiera de estas opciones, siga estos pasos:

1. Seleccione Favoritos > 'Organizar volúmenes favoritos'.
2. Debería aparecer la ventana "Organizador de Volúmenes Favoritos". En esta ventana, seleccione el volumen cuyas opciones desea configurar.
3. Configure las opciones y haga clic en Aceptar.

El orden en que se muestran los volúmenes favoritos del sistema en la ventana Organizador de Favoritos (Favoritos > Organizar Volúmenes Favoritos) es el mismo en que se montan al seleccionar Favoritos > Montar Volúmenes Favoritos o al pulsar la tecla de acceso rápido "Montar Volúmenes Favoritos" (Configuración > Teclas de acceso rápido). Puede usar los botones Subir y Bajar para cambiar el orden de los volúmenes.

Tenga en cuenta que un volumen favorito también puede ser una partición dentro del alcance de la clave de cifrado del sistema, montada sin autenticación previa al arranque (por ejemplo, una partición ubicada en la unidad de sistema cifrada de otro sistema operativo que no se esté ejecutando). Al montar dicho volumen y añadirlo a favoritos, ya no tendrá que seleccionar Sistema > Montar sin autenticación previa al arranque ni habilitar la opción de montaje "Montar partición usando cifrado del sistema sin autenticación previa al arranque". Puede montar el volumen favorito (como se explicó anteriormente) sin configurar ninguna opción, ya que el modo de montaje se guarda en el archivo de configuración que contiene la lista de sus volúmenes favoritos.

Advertencia: cuando la letra de unidad asignada a un volumen favorito (guardado en el archivo de configuración) no está libre, el volumen no se monta y no se muestra ningún mensaje de error.

Para eliminar un volumen de la lista de volúmenes favoritos, seleccione Favoritos > Organizar volúmenes favoritos, seleccione el volumen, haga clic en Eliminar y haga clic en Aceptar.

Volúmenes favoritos del sistema

Los favoritos del sistema son útiles, por ejemplo, en los siguientes casos:

- Tiene volúmenes que deben montarse antes de que se inicien los servicios del sistema y de la aplicación y antes de que los usuarios comiencen a iniciar sesión.

Existen carpetas compartidas de red en los volúmenes de VeraCrypt. Si configura estos volúmenes como favoritos del sistema, se asegurará de que el sistema operativo restaure automáticamente las carpetas compartidas de red cada vez que se reinicie.

- Es necesario que cada uno de estos volúmenes se monte con la misma letra de unidad cada vez que se inicie el sistema operativo.

Tenga en cuenta que, a diferencia de los favoritos normales (no del sistema), los volúmenes favoritos del sistema utilizan la contraseña de autenticación previa al arranque y, por lo tanto, requieren que la partición o unidad del sistema esté cifrada (no es necesario habilitar el almacenamiento en caché de la contraseña de autenticación previa al arranque). Además, dado que la contraseña previa al arranque se escribe con la distribución de teclado estadounidense (requisito de la BIOS), la contraseña del volumen favorito del sistema debe introducirse durante su creación con la distribución de teclado estadounidense , utilizando las mismas teclas que para la contraseña de autenticación previa al arranque. Si la contraseña del volumen favorito del sistema no es idéntica a la de la distribución de teclado estadounidense, no se podrá montar.

Al crear un volumen que más tarde desee convertir en favorito del sistema, debe configurar explícitamente la distribución del teclado asociada con VeraCrypt en distribución de EE. UU. y debe escribir las mismas teclas que escribe cuando ingresa la contraseña de autenticación previa al arranque.

Los volúmenes favoritos del sistema se pueden configurar para que solo estén disponibles en VeraCrypt para usuarios con privilegios de administrador (seleccione Configuración > Volúmenes favoritos del sistema > Permitir que solo los administradores vean y desmonten los volúmenes favoritos del sistema en VeraCrypt). Esta opción debe estar habilitada en los servidores para garantizar que los usuarios sin privilegios de administrador no puedan desmontar los volúmenes favoritos del sistema. En sistemas que no sean servidores, esta opción puede usarse para evitar que las acciones habituales de los volúmenes de VeraCrypt (como "Desmontar todo", desmontaje automático, etc.) afecten a los volúmenes favoritos del sistema. Además, cuando VeraCrypt se ejecuta sin privilegios de administrador (opción predeterminada en Windows Vista y versiones posteriores), los volúmenes favoritos del sistema no se mostrarán en la lista de letras de unidad de la ventana principal de la aplicación VeraCrypt.

Para configurar un volumen de VeraCrypt como volumen favorito del sistema, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic con el botón derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione “Agregar a favoritos del sistema”.
3. Debería aparecer la ventana Organizador de Favoritos del Sistema. En esta ventana, active la opción "Montar volúmenes favoritos del sistema al iniciar Windows" y haga clic en Aceptar.

El orden en que se muestran los volúmenes favoritos del sistema en la ventana Organizador de Favoritos del Sistema (Favoritos > Organizar Volúmenes Favoritos del Sistema) es el mismo en que se montan. Puede usar los botones Subir y Bajar para cambiar el orden de los volúmenes.

Se puede asignar una etiqueta especial a cada volumen favorito del sistema. Esta etiqueta no es la misma que la del sistema de archivos y se muestra en la interfaz de usuario de VeraCrypt en lugar de la ruta del volumen.
Para asignar dicha etiqueta, siga estos pasos:

1. Seleccione Favoritos > 'Organizar volúmenes favoritos del sistema'.
2. Debería aparecer la ventana "Organizador de Favoritos del Sistema". En esta ventana, seleccione el volumen cuya etiqueta desea editar.
3. Ingrese la etiqueta en el campo de entrada 'Etiqueta del volumen favorito seleccionado' y haga clic en Aceptar.

Tenga en cuenta que la ventana Organizador de Favoritos del Sistema (Favoritos > Organizar Volúmenes Favoritos del Sistema) permite configurar varias opciones para cada volumen favorito del sistema. Por ejemplo, cualquiera de ellos puede montarse como de solo lectura o como medio extraíble.

Advertencia: cuando la letra de unidad asignada a un volumen favorito del sistema (guardado en el archivo de configuración) no está libre, el volumen no se monta y no se muestra ningún mensaje de error.

Tenga en cuenta que Windows necesita usar algunos archivos (p. ej., archivos de paginación, archivos de Active Directory, etc.) antes de montar los volúmenes favoritos del sistema. Por lo tanto, estos archivos no pueden almacenarse en ellos. Sin embargo, sí pueden almacenarse en cualquier partición dentro del alcance de la clave de cifrado del sistema (p. ej., en la partición del sistema o en cualquier partición de una unidad del sistema completamente cifrada con VeraCrypt).

Para eliminar un volumen de la lista de volúmenes favoritos del sistema, seleccione Favoritos > Organizar volúmenes favoritos del sistema, seleccione el volumen, haga clic en Eliminar y haga clic en Aceptar.

Cifrado del sistema

VeraCrypt puede cifrar sobre la marcha una partición del sistema o una unidad completa del sistema, es decir, una partición o unidad donde está instalado Windows y desde la cual arranca.

El cifrado del sistema proporciona el máximo nivel de seguridad y privacidad, ya que todos los archivos, incluidos los archivos temporales que Windows y las aplicaciones crean en la partición del sistema (normalmente sin su conocimiento ni consentimiento), los archivos de hibernación, los archivos de intercambio, etc., se cifran permanentemente (incluso si se interrumpe repentinamente el suministro eléctrico). Windows también registra grandes cantidades de datos potencialmente confidenciales, como los nombres y las ubicaciones de los archivos que abre, las aplicaciones que ejecuta, etc. Todos estos archivos de registro y entradas del registro también se cifran permanentemente.

El cifrado del sistema implica autenticación previa al arranque, lo que significa que cualquier persona que desee acceder y usar el sistema cifrado, leer y escribir archivos almacenados en la unidad del sistema, etc., deberá introducir la contraseña correcta cada vez antes de que Windows arranque. La autenticación previa al arranque la gestiona el cargador de arranque VeraCrypt, ubicado en la primera pista de la unidad de arranque y en el disco de rescate VeraCrypt (véase más abajo).

Tenga en cuenta que VeraCrypt puede cifrar una partición o unidad del sistema sin cifrar mientras el sistema operativo está en ejecución (mientras se cifra el sistema, puede usar su ordenador con normalidad, sin restricciones). Asimismo, una partición o unidad del sistema cifrada con VeraCrypt puede descifrarse mientras el sistema operativo está en ejecución. Puede interrumpir el proceso de cifrado o descifrado en cualquier momento, dejar la partición o unidad parcialmente sin cifrar, reiniciar o apagar el ordenador y, a continuación, reanudar el proceso, que continuará desde el punto en que se detuvo.

El modo de operación utilizado para el cifrado del sistema es XTS (véase la sección "Modos de Operación"). Para más detalles técnicos sobre el cifrado del sistema, consulte la sección "Esquema de Cifrado" en el capítulo "Detalles Técnicos".

Para cifrar una partición del sistema o una unidad completa, seleccione Sistema > Cifrar partición/unidad del sistema y siga las instrucciones del asistente. Para descifrar una partición/unidad del sistema, seleccione Sistema > Descifrar partición/unidad del sistema permanentemente.

Debido a los requisitos del BIOS, la contraseña de prearranque se escribe utilizando el diseño del teclado de EE. UU. Durante el proceso de cifrado del sistema, VeraCrypt cambia el teclado a la distribución estadounidense de forma automática y transparente para garantizar que la contraseña introducida coincida con la introducida en el modo de prearranque. Por lo tanto, para evitar errores de contraseña, se debe escribir la contraseña con las mismas teclas que al crear el cifrado del sistema.

Nota: De forma predeterminada, Windows 7 y versiones posteriores arrancan desde una pequeña partición especial. Esta partición contiene los archivos necesarios para arrancar el sistema. Windows solo permite que las aplicaciones con privilegios de administrador escriban en ella (cuando el sistema está en ejecución). VeraCrypt cifra la partición solo si se elige cifrar toda la unidad del sistema (en lugar de cifrar solo la partición donde está instalado Windows).

Sistema operativo oculto

Podría suceder que alguien le obligue a descifrar el sistema operativo. Hay muchas situaciones en las que no puede negarse a hacerlo (por ejemplo, debido a una extorsión). VeraCrypt le permite crear un sistema operativo oculto cuya existencia debería ser imposible de probar (siempre que se sigan ciertas directrices). Por lo tanto, no tendrá que descifrar ni revelar la contraseña del sistema operativo oculto. Para más información, consulte la sección " Sistema operativo oculto" en el capítulo "Negación plausible".

Sistemas operativos compatibles con el cifrado del sistema

Nota: Tras el lanzamiento de esta versión de VeraCrypt, es posible que se haya publicado una nueva versión de un sistema operativo cuya compatibilidad con VeraCrypt se haya verificado. Por lo tanto, si esta es la última versión estable de VeraCrypt, le recomendamos consultar la versión en línea de este capítulo en: https://veracrypt.codeplex.com/wikipage?title=Supported%20Systems%20for%20System %20Encryption

VeraCrypt actualmente puede cifrar los siguientes sistemas operativos (solo modo BIOS, UEFI/GPT no compatible):

• Windows 10 • Windows 8 y 8.1 • Windows 7 • Windows Vista (SP1 o posterior) • Windows XP • Windows Server 2012 • Windows Server 2008 y Windows Server 2008 R2 (64 bits) • Windows Server 2003

Nota: Los siguientes sistemas operativos (entre otros) no son compatibles: Windows RT, Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64 y las versiones Embedded/Tablet de Windows.

Consulte también la sección Sistemas operativos compatibles.

Disco de rescate de VeraCrypt

Durante el proceso de preparación del cifrado de una partición/unidad del sistema, VeraCrypt requiere que cree un disco de rescate VeraCrypt (CD/DVD), que cumple los siguientes propósitos:

Si la pantalla del cargador de arranque VeraCrypt no aparece después de iniciar el ordenador (o si Windows no arranca), es posible que esté dañado. El disco de rescate VeraCrypt le permite restaurarlo y, por lo tanto, recuperar el acceso a su sistema y datos cifrados (sin embargo, tenga en cuenta que deberá introducir la contraseña correcta). En la pantalla del disco de rescate, seleccione Opciones de reparación > Restaurar cargador de arranque VeraCrypt. A continuación, pulse "Y" para confirmar, extraiga el disco de rescate de la unidad de CD/DVD y reinicie el ordenador.

Si el cargador de arranque VeraCrypt se daña con frecuencia (por ejemplo, debido a un software de activación mal diseñado) o si no desea que resida en el disco duro (por ejemplo, si desea usar un cargador/gestor de arranque alternativo para otros sistemas operativos), puede arrancar directamente desde el disco de rescate VeraCrypt (ya que también contiene el cargador de arranque VeraCrypt) sin tener que restaurarlo en el disco duro. Simplemente inserte el disco de rescate en la unidad de CD/DVD e introduzca su contraseña en la pantalla del disco de rescate.

Si ingresa repetidamente la contraseña correcta, pero VeraCrypt indica que es incorrecta, es posible que la clave maestra u otros datos importantes estén dañados. El Disco de Rescate de VeraCrypt le permite restaurarlos y así recuperar el acceso a su sistema y datos cifrados (sin embargo, tenga en cuenta que, en ese caso, deberá ingresar la contraseña correcta). En la pantalla Disco de Rescate, seleccione Opciones de Reparación > Restaurar datos de la clave.
Luego ingrese su contraseña, presione 'Y' para confirmar la acción, retire el Disco de Rescate de

su unidad de CD/DVD y reinicie su computadora.

Nota: Esta función no se puede usar para restaurar el encabezado de un volumen oculto que contenga un sistema operativo oculto (consulte la sección " Sistema operativo oculto"). Para restaurar dicho encabezado de volumen, haga clic en Seleccionar dispositivo, seleccione la partición detrás de la partición del sistema señuelo, haga clic en Aceptar, seleccione Herramientas > Restaurar encabezado de volumen y siga las instrucciones.

ADVERTENCIA: Al restaurar datos clave con un disco de rescate VeraCrypt, también se restaura la contraseña válida al crearlo. Por lo tanto, siempre que cambie la contraseña, debe destruir su disco de rescate VeraCrypt y crear uno nuevo (seleccione Sistema > Crear disco de rescate). De lo contrario, si un atacante conoce su contraseña anterior (por ejemplo, si la ha capturado un registrador de pulsaciones de teclas) y encuentra su antiguo disco de rescate VeraCrypt, podría usarlo para restaurar los datos clave (la clave maestra cifrada con la contraseña anterior) y así descifrar la partición/unidad del sistema.

- Si Windows está dañado y no puede iniciarse, VeraCrypt Rescue Disk le permite Descifre permanentemente la partición/unidad antes de iniciar Windows. En la pantalla Disco de rescate, seleccione Opciones de reparación > Descifrar permanentemente la partición/unidad del sistema. Introduzca la contraseña correcta y espere a que se complete el descifrado. A continuación, puede, por ejemplo, arrancar el CD/DVD de instalación de MS Windows para reparar la instalación de Windows. Tenga en cuenta que esta función no se puede usar para descifrar un volumen oculto que contenga un sistema operativo oculto (consulte la sección " Sistema operativo oculto").

  Nota: Como alternativa, si Windows está dañado (no puede iniciarse) y necesita repararlo (o acceder a los archivos que contiene), puede evitar descifrar la partición/unidad del sistema siguiendo estos pasos: Si tiene varios sistemas operativos instalados en su computadora, inicie el que no requiera autenticación previa al arranque. Si no tiene varios sistemas operativos instalados en su computadora, puede iniciar un CD/DVD WinPE o BartPE, o puede conectar la unidad del sistema como una unidad secundaria o externa a otra computadora y luego iniciar el sistema operativo instalado en la computadora. Después de iniciar un sistema, ejecute VeraCrypt, haga clic en Seleccionar dispositivo, seleccione la partición del sistema afectada, haga clic en Aceptar , seleccione Sistema > Montar sin autenticación previa al arranque, ingrese su contraseña de autenticación previa al arranque y haga clic en Aceptar. La partición se montará como un volumen VeraCrypt normal (los datos se descifrarán/cifrarán sobre la marcha en la RAM al acceder, como de costumbre).

- Su disco de rescate VeraCrypt contiene una copia de seguridad del contenido original de la primera pista de la unidad (creada antes de que se escribiera el cargador de arranque VeraCrypt) y le permite restaurarla si es necesario. La primera pista suele contener un cargador de sistema o un gestor de arranque. En la pantalla Disco de rescate, seleccione Opciones de reparación > Restaurar el cargador de sistema original.

Tenga en cuenta que incluso si pierde su disco de rescate VeraCrypt y un atacante lo encuentra, no podrá descifrar la partición o la unidad del sistema sin la contraseña correcta.

Para arrancar un disco de rescate VeraCrypt, insértelo en la unidad de CD/DVD y reinicie el ordenador. Si no aparece la pantalla del disco de rescate VeraCrypt (o si no ve la opción "Opciones de reparación" en la sección "Controles de teclado"), es posible que el BIOS esté configurado para intentar arrancar desde los discos duros antes que desde las unidades de CD/DVD. En ese caso, reinicie el ordenador, pulse F2 o Supr (en cuanto vea la pantalla de inicio del BIOS) y espere hasta que aparezca la pantalla de configuración. Si no aparece ninguna pantalla de configuración, reinicie el ordenador y vuelva a pulsar F2 o Supr repetidamente en cuanto lo haga. Cuando aparezca la pantalla de configuración del BIOS, configúrelo para que arranque primero desde la unidad de CD/DVD (por ejemplo,

Para obtener más información sobre cómo hacerlo, consulte la documentación de su BIOS/placa base o contacte con el equipo de soporte técnico del proveedor de su computadora. A continuación, reinicie el equipo. Debería aparecer la pantalla del Disco de Rescate de VeraCrypt. Nota: En la pantalla del Disco de Rescate de VeraCrypt, puede seleccionar "Opciones de reparación" pulsando F8.

Si su disco de rescate VeraCrypt está dañado, puede crear uno nuevo seleccionando Sistema > Crear disco de rescate. Para comprobar si su disco de rescate VeraCrypt está dañado, insértelo en la unidad de CD/DVD y seleccione Sistema > Verificar disco de rescate.

Negación plausible

En caso de que un adversario le obligue a revelar su contraseña, VeraCrypt proporciona y admite dos tipos de negación plausible:

1. Volúmenes ocultos (consulte la sección Volumen oculto a continuación) y sistemas operativos ocultos (ver sección Sistema Operativo Oculto).

2. Hasta que se descifre, una partición o dispositivo VeraCrypt parece no consistir en nada más que Datos aleatorios (no contienen ningún tipo de "firma"). Por lo tanto, debería ser imposible demostrar que una partición o un dispositivo es un volumen VeraCrypt o que ha sido cifrado (siempre que se cumplan los requisitos y precauciones de seguridad indicados en el capítulo " Requisitos y precauciones de seguridad"). Una posible explicación plausible para la existencia de una partición/dispositivo que contiene únicamente datos aleatorios es que se haya borrado de forma segura el contenido de la partición/dispositivo utilizando una herramienta que borra datos sobrescribiéndolos con datos aleatorios (de hecho, VeraCrypt también puede utilizarse para borrar de forma segura una partición/dispositivo, creando un volumen vacío y cifrado alojado en el dispositivo). Sin embargo, es necesario evitar fugas de datos (véase la sección " Fugas de datos") y tener en cuenta que, para el cifrado del sistema, la primera pista de la unidad contiene el gestor de arranque VeraCrypt (sin cifrar), que se puede identificar fácilmente como tal (para más información, consulte el capítulo " Cifrado del sistema"). Al utilizar el cifrado del sistema, se puede lograr una negación plausible mediante la creación de un sistema operativo oculto (consulte la sección Sistema operativo oculto).

   Aunque los volúmenes (contenedores) de VeraCrypt alojados en archivos tampoco contienen ningún tipo de "firma" (hasta que se descifran, parecen consistir únicamente en datos aleatorios), no pueden proporcionar este tipo de negación plausible, ya que prácticamente no hay una explicación plausible para la existencia de un archivo que contenga únicamente datos aleatorios. Sin embargo, sí es posible lograr una negación plausible con un volumen (contenedor) de VeraCrypt alojado en archivos creando un volumen oculto dentro de él (véase más arriba).

Notas

- Al formatear una partición de disco duro como un volumen VeraCrypt (o cifrar una partición en su lugar), la tabla de particiones (incluido el tipo de partición) nunca se modifica (no se escribe ninguna “firma” o “ID” de VeraCrypt en la tabla de particiones).

- Existen métodos para encontrar archivos o dispositivos que contienen datos aleatorios (como VeraCrypt volúmenes). Tenga en cuenta, sin embargo, que esto no debería afectar la negación plausible de ninguna manera. El adversario aún no debería poder demostrar que la partición/dispositivo es un volumen VeraCrypt ni que el archivo, la partición o el dispositivo contiene un volumen VeraCrypt oculto (siempre que se cumplan los requisitos y precauciones de seguridad que se indican en el capítulo " Requisitos y precauciones de seguridad" y en la subsección " Requisitos y precauciones de seguridad relacionados con volúmenes ocultos").

Volumen oculto

Puede suceder que alguien le obligue a revelar la contraseña de un volumen cifrado.
Existen muchas situaciones en las que no es posible negarse a revelar la contraseña (por ejemplo, debido a una extorsión).
Usar un volumen oculto permite resolver estas situaciones sin revelar la contraseña de su volumen.

El diseño de un volumen VeraCrypt estándar antes y después de que se creara un volumen oculto dentro de él.

El principio es que un volumen VeraCrypt se crea dentro de otro volumen VeraCrypt (dentro del espacio libre del volumen). Incluso cuando el volumen externo está montado, debería ser imposible comprobar si contiene un volumen oculto*, ya que el espacio libre de cualquier volumen VeraCrypt siempre se llena con datos aleatorios al crearse el volumen† y ninguna parte del volumen oculto (desmontado) se puede distinguir de los datos aleatorios. Tenga en cuenta que VeraCrypt no modifica el sistema de archivos (información sobre el espacio libre, etc.) del volumen externo de ninguna manera.

La contraseña del volumen oculto debe ser sustancialmente diferente de la del volumen externo. En el volumen externo (antes de crear el volumen oculto dentro de él), debe copiar algunos archivos de aspecto confidencial que NO desea ocultar. Estos archivos estarán ahí por

---

* Siempre que se hayan seguido todas las instrucciones del Asistente de creación de volúmenes de VeraCrypt y se hayan observado los requisitos y precauciones indicados en la subsección « Requisitos y precauciones de seguridad para volúmenes ocultos» . † Siempre que las opciones « Formato rápido» y «Dinámico» estén desactivadas y que el volumen no contenga un sistema de archivos cifrado (VeraCrypt no permite crear un volumen oculto dentro de dicho volumen). Para obtener información sobre el método para rellenar el espacio libre del volumen con datos aleatorios, consulte el capítulo « Detalles técnicos», sección « Especificación del formato del volumen de VeraCrypt».

Cualquiera que te obligue a compartir la contraseña. Solo revelarás la contraseña del volumen externo, no la del oculto. Los archivos confidenciales se almacenarán en el volumen oculto.

Un volumen oculto se puede montar de la misma manera que un volumen estándar de VeraCrypt: Haga clic en "Seleccionar archivo" o "Seleccionar dispositivo" para seleccionar el volumen externo/host (importante: asegúrese de que el volumen no esté montado). A continuación, haga clic en "Montar" e introduzca la contraseña del volumen oculto. La contraseña determina si se montará el volumen oculto o el externo (es decir, al introducir la contraseña del volumen externo, se montará este; al introducir la contraseña del volumen oculto, se montará este).

VeraCrypt primero intenta descifrar el encabezado de volumen estándar con la contraseña introducida. Si falla, carga en la RAM el área del volumen donde se puede almacenar un encabezado de volumen oculto (es decir, los bytes 65536–131071, que contienen únicamente datos aleatorios cuando no hay un volumen oculto dentro del volumen) e intenta descifrarlo con la contraseña introducida. Tenga en cuenta que los encabezados de volumen ocultos no se pueden identificar, ya que parecen estar compuestos exclusivamente de datos aleatorios. Si el encabezado se descifra correctamente (para obtener información sobre cómo VeraCrypt determina que se ha descifrado correctamente, consulte la sección " Esquema de cifrado"), la información sobre el tamaño del volumen oculto se recupera del encabezado descifrado (que aún está almacenado en la RAM) y el volumen oculto se monta (su tamaño también determina su desplazamiento).

Se puede crear un volumen oculto dentro de cualquier tipo de volumen VeraCrypt, es decir, dentro de un volumen alojado en archivos o en una partición/dispositivo (requiere privilegios de administrador). Para crear un volumen VeraCrypt oculto, haga clic en "Crear volumen" en la ventana principal del programa y seleccione "Crear un volumen VeraCrypt oculto". El asistente le proporcionará ayuda y toda la información necesaria para crear correctamente un volumen VeraCrypt oculto.

Al crear un volumen oculto, puede resultar muy difícil, o incluso imposible, para un usuario sin experiencia configurar su tamaño de forma que no sobrescriba los datos del volumen externo. Por lo tanto, el Asistente para la creación de volúmenes escanea automáticamente el mapa de bits del clúster del volumen externo (antes de crear el volumen oculto) y determina su tamaño máximo.*

Si surge algún problema al crear un volumen oculto, consulte el capítulo Solución de problemas para obtener posibles soluciones.

Tenga en cuenta que también es posible crear e iniciar un sistema operativo que resida en un volumen oculto (consulte la sección Sistema operativo oculto en el capítulo Negación plausible).

* El asistente escanea el mapa de bits del clúster para determinar el tamaño del área ininterrumpida de espacio libre (si la hay) cuyo extremo está alineado con el extremo del volumen externo. Esta área alberga el volumen oculto y, por lo tanto, su tamaño limita el tamaño máximo posible del volumen oculto. En Linux y Mac OS X, el asistente no escanea el mapa de bits del clúster, pero el controlador detecta los datos escritos en el volumen externo y utiliza su posición como se describió anteriormente.

Protección de volúmenes ocultos contra daños

Si monta un volumen VeraCrypt que contiene un volumen oculto, podrá leer los datos almacenados en el volumen externo sin ningún riesgo. Sin embargo, si usted (o el sistema operativo) necesita guardar datos en el volumen externo, existe el riesgo de que el volumen oculto se dañe (se sobrescriba). Para evitarlo, debe proteger el volumen oculto como se describe en esta sección.

Al montar un volumen externo, escriba su contraseña y antes de hacer clic en Aceptar, haga clic en Montar Opciones:

En el cuadro de diálogo Opciones de montaje , active la opción "Proteger el volumen oculto contra daños causados por escritura en el volumen externo ". En el campo "Contraseña del volumen oculto" , escriba la contraseña del volumen oculto. Haga clic en Aceptar y, en el cuadro de diálogo principal de introducción de contraseña, haga clic en Aceptar.

Ambas contraseñas deben ser correctas; de lo contrario, el volumen externo no se montará. Cuando la protección de volumen oculto está habilitada, VeraCrypt no monta el volumen oculto. Solo descifra su encabezado (en RAM) y recupera información sobre el tamaño del volumen oculto (del encabezado descifrado). A continuación, se monta el volumen externo y cualquier intento de guardar datos en el área del volumen oculto será rechazado (hasta que se desmonte el volumen externo). Tenga en cuenta que VeraCrypt nunca modifica el sistema de archivos (p. ej., información sobre clústeres asignados, cantidad de espacio libre, etc.) dentro del volumen externo de ninguna manera. En cuanto se desmonta el volumen, se pierde la protección. Al volver a montar el volumen, no es posible determinar si ha utilizado la protección de volumen oculto. El volumen oculto...

La protección de volumen sólo puede ser activada por usuarios que proporcionen la contraseña correcta (y/o archivos de clave) para el volumen oculto (cada vez que montan el volumen externo).

En cuanto se deniega o impide una operación de escritura en el área del volumen oculto (para proteger dicho volumen), todo el volumen del host (tanto el externo como el oculto) queda protegido contra escritura hasta que se desmonte (el controlador de VeraCrypt informa al sistema del error "parámetro no válido" cada vez que se intenta escribir datos en el volumen). Esto preserva la posibilidad de denegación (de lo contrario, ciertas inconsistencias en el sistema de archivos podrían indicar que este volumen ha utilizado la protección de volumen oculto). Cuando se impiden daños en el volumen oculto, se muestra una advertencia (siempre que la tarea en segundo plano de VeraCrypt esté habilitada; consulte el capítulo " Tarea en segundo plano de VeraCrypt").
Además, el tipo de volumen externo montado que se muestra en la ventana principal cambia a 'Externo(!)':

Además, el campo Volumen oculto protegido en la ventana de diálogo Propiedades de volumen dice: 'Sí (¡daño evitado!)'.

Tenga en cuenta que cuando se previene el daño a un volumen oculto, no se escribe información sobre el evento en el volumen. Al desmontar y volver a montar el volumen externo, las propiedades del volumen no mostrarán la cadena "daño prevenido".

Hay varias formas de comprobar que un volumen oculto está protegido contra daños:

1. Después de montar el volumen externo, se muestra un cuadro de mensaje de confirmación que indica que el volumen oculto está siendo protegido (si no se muestra, el volumen oculto no está protegido).
2. En el cuadro de diálogo Propiedades de volumen , el campo Volumen oculto protegido dice 'Sí': 3. El tipo de volumen externo montado es Externo:

Importante: Usted es la única persona que puede montar su volumen externo con la protección de volumen oculto habilitada (ya que nadie más conoce su contraseña). Cuando un adversario le pida que monte un volumen externo, por supuesto, no debe hacerlo con la protección de volumen oculto habilitada. Debe montarlo como un volumen normal (en ese caso, VeraCrypt no mostrará el tipo de volumen "Externo", sino "Normal"). Esto se debe a que, mientras un volumen externo esté montado con la protección de volumen oculto habilitada, el adversario puede descubrir que existe un volumen oculto dentro del volumen externo (podrá descubrirlo hasta que se desmonte el volumen y posiblemente incluso después de apagar el ordenador; consulte Datos sin cifrar en la RAM).

Advertencia: Tenga en cuenta que la opción «Proteger el volumen oculto contra daños causados por escritura en el volumen externo» del cuadro de diálogo Opciones de montaje se desactiva automáticamente tras un intento de montaje, independientemente de si se realiza correctamente o no (todos los volúmenes ocultos que ya están protegidos seguirán protegidos). Por lo tanto, debe marcar esta opción cada vez que intente montar el volumen externo (si desea proteger el volumen oculto).

Si desea montar un volumen externo y proteger un volumen oculto mediante contraseñas en caché, siga estos pasos: Mantenga presionada la tecla Control (Ctrl) al hacer clic en "Montar" (o seleccione "Montar con opciones" en el menú " Volúmenes "). Se abrirá el cuadro de diálogo "Opciones de montaje" . Active la opción "Proteger el volumen oculto contra daños causados por escritura en el volumen externo" y deje la casilla de contraseña vacía. A continuación, haga clic en "Aceptar".

Si necesita montar un volumen externo y sabe que no necesitará guardar ningún dato en él, la forma más cómoda de proteger el volumen oculto contra daños es montar el volumen externo como de solo lectura (consulte la sección Opciones de montaje).

Requisitos de seguridad y precauciones relativas a los volúmenes ocultos

Si utiliza un volumen VeraCrypt oculto, debe seguir los requisitos y precauciones de seguridad que se detallan a continuación en esta sección.
Aviso legal: No se garantiza que esta sección incluya una lista de todos los problemas de seguridad y ataques que podrían afectar o limitar la capacidad de VeraCrypt para proteger los datos almacenados en un volumen VeraCrypt oculto y su capacidad para proporcionar una denegación plausible.

Si un adversario accede a un volumen VeraCrypt (desmontado) en varios momentos, podría determinar qué sectores del volumen están cambiando. Si modifica el contenido de un volumen oculto (por ejemplo, al crear o copiar archivos nuevos en él, o al modificar, eliminar, renombrar o mover archivos almacenados en él, etc.), el contenido de los sectores (texto cifrado) en el área del volumen oculto cambiará. Tras obtener la contraseña del volumen externo, el adversario podría exigir una explicación de por qué cambiaron estos sectores. Si no proporciona una explicación plausible, podría indicar la existencia de un volumen oculto dentro del volumen externo.

Téngase en cuenta que problemas similares al descrito anteriormente también pueden surgir, por ejemplo, en los siguientes casos:

- El sistema de archivos en el que almacena un contenedor VeraCrypt alojado en archivos ha sido desfragmentado y queda una copia del contenedor VeraCrypt (o de su fragmento) en el espacio libre del volumen del host (en el sistema de archivos desfragmentado). Para evitarlo, realice una de las siguientes acciones: • Use un volumen VeraCrypt alojado en una partición o dispositivo en lugar de uno alojado en un archivo. • Borre de forma segura el espacio libre del volumen del host (en el sistema de archivos desfragmentado) después de la desfragmentación. En Windows, esto se puede hacer con la utilidad gratuita de Microsoft SDelete. En Linux, se puede usar la utilidad shred del paquete GNU coreutils para este propósito. • No desfragmente los sistemas de archivos donde almacene volúmenes de VeraCrypt.

- Un contenedor VeraCrypt alojado en archivos se almacena en un sistema de archivos de registro (como NTFS). Es posible que quede una copia del contenedor de VeraCrypt (o de su fragmento) en el volumen del host. Para evitar esto, haga una de las siguientes cosas: • Utilice un volumen VeraCrypt alojado en una partición o dispositivo en lugar de uno alojado en archivos. • Almacene el contenedor en un sistema de archivos sin registro (por ejemplo, FAT32).

- Un volumen de VeraCrypt reside en un dispositivo/sistema de archivos que utiliza un sistema de nivelación de desgaste. Mecanismo (p. ej., una unidad SSD de memoria flash o una unidad flash USB). Es posible que quede una copia (o un fragmento) del volumen VeraCrypt en el dispositivo. Por lo tanto, no almacene volúmenes ocultos en dichos dispositivos/sistemas de archivos. Para obtener más información sobre la nivelación de desgaste, consulte la sección " Nivelación de desgaste" en el capítulo " Requisitos y precauciones de seguridad".

- Un volumen de VeraCrypt reside en un dispositivo/sistema de archivos que guarda datos (o en un dispositivo/sistema de archivos que es controlado o monitoreado por un sistema/dispositivo que guarda datos)

(p. ej., el valor de un temporizador o contador) que permite determinar si un bloque se escribió antes que otro o cuántas veces se escribió o leyó un bloque. Por lo tanto, no almacene volúmenes ocultos en dichos dispositivos o sistemas de archivos. Para saber si un dispositivo o sistema guarda dichos datos, consulte la documentación que lo acompaña o póngase en contacto con el fabricante.

- Un volumen de VeraCrypt reside en un dispositivo propenso al desgaste (es posible determinar que un bloque se ha escrito/leído más veces que otro bloque). Por lo tanto, no almacene volúmenes ocultos en dichos dispositivos/sistemas de archivos. Para saber si un dispositivo es propenso a este desgaste, consulte la documentación que lo acompaña o póngase en contacto con el proveedor/fabricante.

Se realiza una copia de seguridad del contenido de un volumen oculto clonando su volumen host o se crea un nuevo volumen oculto clonándolo. Por lo tanto, no debe hacerlo. Siga las instrucciones del capítulo " Cómo realizar copias de seguridad de forma segura" y de la sección "Clones de volumen".

- Asegúrese de que el formato rápido esté deshabilitado al cifrar una partición o un dispositivo dentro del cual pretendemos crear un volumen oculto.

- En Windows, asegúrese de no haber eliminado ningún archivo dentro de un volumen en el que pretende crear un volumen oculto (el escáner de mapa de bits del clúster no detecta archivos eliminados).

- En Linux o Mac OS X, si desea crear un volumen oculto dentro de un volumen de VeraCrypt alojado en archivos, asegúrese de que el volumen no esté alojado en archivos dispersos (la versión de Windows de VeraCrypt verifica esto y no permite la creación de volúmenes ocultos dentro de archivos dispersos).

Al montar un volumen oculto, el sistema operativo y las aplicaciones de terceros pueden escribir en volúmenes no ocultos (normalmente, en el volumen del sistema sin cifrar) información sin cifrar sobre los datos almacenados en el volumen oculto (p. ej., nombres de archivo y ubicaciones de archivos accedidos recientemente, bases de datos creadas por herramientas de indexación de archivos, etc.), los propios datos sin cifrar (archivos temporales, etc.), información sin cifrar sobre el sistema de archivos que reside en el volumen oculto (que podría utilizarse, por ejemplo, para identificar el sistema de archivos y determinar si se trata del sistema de archivos que reside en el volumen externo), la contraseña/clave del volumen oculto u otros tipos de datos confidenciales. Por lo tanto, se deben seguir los siguientes requisitos y precauciones de seguridad:

- Windows: Cree un sistema operativo oculto (para obtener información sobre cómo hacerlo, consulte la sección Sistema operativo oculto) y monte volúmenes ocultos solo cuando se esté ejecutando dicho sistema. Nota: Cuando se está ejecutando un sistema operativo oculto, VeraCrypt garantiza que todos los sistemas de archivos locales sin cifrar y los volúmenes VeraCrypt no ocultos sean de solo lectura (es decir, no se pueden acceder archivos). Se permite escribir datos en dichos sistemas de archivos o volúmenes VeraCrypt).* Se permite escribir datos en sistemas de archivos dentro de volúmenes VeraCrypt ocultos. Como alternativa, si no se puede usar un sistema operativo oculto, utilice un sistema Windows PE con Live CD (almacenado completamente en un CD/DVD y arrancado desde él) que garantice que cualquier dato escrito en el volumen del sistema se escriba en un disco RAM. Monte volúmenes ocultos solo cuando se esté ejecutando dicho sistema con Live CD (si no se puede usar un sistema operativo oculto). Además, durante dicha sesión de Live CD, solo los sistemas de archivos que residen en volúmenes VeraCrypt ocultos pueden montarse en modo de lectura y escritura (los volúmenes/sistemas de archivos externos o sin cifrar deben montarse en modo de solo lectura o no deben montarse ni ser accesibles en absoluto); de lo contrario, debe asegurarse de que las aplicaciones y el sistema operativo no escriban datos confidenciales (véase más arriba) en volúmenes/sistemas de archivos no ocultos durante la sesión de Live CD.

*Esto no se aplica a sistemas de archivos en medios tipo CD/DVD ni en dispositivos/medios personalizados, atípicos o no estándar.

- o Linux: Descargue o cree una versión "live-CD" de su sistema operativo (es decir, un CD "en vivo"). Sistema Linux almacenado completamente en un CD/DVD y arrancado desde él, lo que garantiza que cualquier dato escrito en el volumen del sistema se escriba en un disco RAM. Monte volúmenes ocultos solo cuando se esté ejecutando dicho sistema de "CD en vivo". Durante la sesión, solo los sistemas de archivos que residen en volúmenes VeraCrypt ocultos pueden montarse en modo de lectura y escritura (los volúmenes/sistemas de archivos externos o sin cifrar deben montarse en modo de solo lectura o no deben montarse/ser accesibles en absoluto). Si no puede cumplir con este requisito y no puede garantizar que las aplicaciones y el sistema operativo no escriban datos confidenciales (véase más arriba) en volúmenes/sistemas de archivos no ocultos, no debe montar ni crear volúmenes VeraCrypt ocultos en Linux.

- o Mac OS X: Si no puede garantizar que las aplicaciones y el sistema operativo no escriban datos confidenciales (ver arriba) en volúmenes/sistemas de archivos no ocultos, no debe montar ni crear volúmenes VeraCrypt ocultos en Mac OS X.

Al montar un volumen externo con la protección de volúmenes ocultos activada (consulte la sección " Protección de volúmenes ocultos contra daños"), debe seguir los mismos requisitos y precauciones de seguridad que al montar un volumen oculto (consulte más arriba). Esto se debe a que el sistema operativo podría filtrar la contraseña o clave del volumen oculto a un volumen no oculto o sin cifrar.

- Si utiliza un sistema operativo que reside dentro de un volumen oculto (consulte la sección Oculto Sistema operativo), además de lo anterior, deberá seguir estos requisitos y precauciones de seguridad:

  - o Debes utilizar el sistema operativo señuelo con la misma frecuencia con la que utilizas tu computadora. Idealmente, debería usarlo para todas las actividades que no involucren datos confidenciales. De lo contrario, la posible negación del sistema operativo oculto podría verse afectada (si revela la contraseña del sistema operativo señuelo a un adversario, este podría descubrir que el sistema no se usa con frecuencia, lo que podría indicar la existencia de un sistema operativo oculto en su computadora). Tenga en cuenta que puede guardar datos en la partición del sistema señuelo en cualquier momento sin riesgo de que el volumen oculto se dañe (ya que el sistema señuelo no está instalado en el volumen externo).

  - Si el sistema operativo requiere activación, debe activarse antes de clonarse (la clonación forma parte del proceso de creación de un sistema operativo oculto; consulte la sección " Sistema operativo oculto") y el sistema operativo oculto (es decir, el clon) nunca debe reactivarse. Esto se debe a que el sistema operativo oculto se crea copiando el contenido de la partición del sistema a un volumen oculto (por lo que, si el sistema operativo no está activado, el sistema operativo oculto tampoco lo estará). Si activó o reactivó un sistema operativo oculto, la fecha y la hora de la activación (y otros datos) podrían registrarse en un servidor de Microsoft (y en el sistema operativo oculto), pero no en el sistema operativo señuelo. Por lo tanto, si un adversario tuviera acceso a los datos almacenados en el servidor o interceptara su solicitud al servidor (y si le reveló la contraseña del sistema operativo señuelo), podría descubrir que el sistema operativo señuelo se activó (o reactivó) en un momento diferente, lo que podría indicar la existencia de un sistema operativo oculto en su equipo.

    Por razones similares, cualquier software que requiera activación debe instalarse y activarse antes de comenzar a crear el sistema operativo oculto.

  - Cuando necesite apagar el sistema oculto e iniciar el sistema señuelo, no reinicie la computadora. En su lugar, apáguela o hiberne y luego déjela apagada durante al menos varios minutos (cuanto más tiempo, mejor) antes de encenderla y...

Arrancar el sistema señuelo. Esto es necesario para borrar la memoria, que puede contener datos confidenciales. Para más información, consulte la sección " Datos sin cifrar en la RAM" del capítulo " Requisitos y precauciones de seguridad".

o La computadora puede estar conectada a una red (incluido Internet) sólo cuando el El sistema operativo señuelo se está ejecutando. Cuando el sistema operativo oculto se esté ejecutando, el ordenador no debe estar conectado a ninguna red, ni siquiera a internet (una de las formas más fiables de garantizarlo es desconectar el cable de red, si lo hay). Tenga en cuenta que si se descargan o suben datos a un servidor remoto, la fecha y la hora de la conexión, así como otros datos, suelen registrarse en el servidor. También se registran diversos tipos de datos en el sistema operativo (p. ej., datos de actualización automática de Windows, registros de aplicaciones, registros de errores, etc.). Por lo tanto, si un adversario tuviera acceso a los datos almacenados en el servidor o interceptara su solicitud al servidor (y si le revelara la contraseña del sistema operativo señuelo), podría descubrir que la conexión no se realizó desde el sistema operativo señuelo, lo que podría indicar la existencia de un sistema operativo oculto en su ordenador.

Tenga en cuenta también que podrían surgir problemas similares si se compartiera algún sistema de archivos en la red bajo el sistema operativo oculto (independientemente de si el sistema de archivos es remoto o local). Por lo tanto, cuando se ejecuta el sistema operativo oculto, no debe haber ningún sistema de archivos compartido en la red (en ninguna dirección).

Cualquier acción que un adversario pueda detectar (o cualquier acción que modifique datos fuera de los volúmenes ocultos montados) debe realizarse únicamente cuando el sistema operativo señuelo esté en ejecución (a menos que tenga una explicación alternativa plausible, como usar un sistema de CD en vivo para realizar dichas acciones). Por ejemplo, la opción "Ajuste automático al horario de verano" podría estar habilitada únicamente en el sistema señuelo.

o Si el BIOS, EFI o cualquier otro componente registra eventos de apagado o cualquier otro evento que pudiera indicar que se utiliza un volumen/sistema oculto (por ejemplo, al comparar dichos eventos con los eventos en el registro de eventos de Windows), debe deshabilitar dicho registro o asegurarse de que el registro se borre de forma segura después de cada sesión (o evitar de otra manera dicho problema de manera apropiada).

Además de lo anterior, deberás seguir los requisitos y precauciones de seguridad que se enumeran en los siguientes capítulos:

• Requisitos y precauciones de seguridad • Cómo realizar copias de seguridad de forma segura

Sistema operativo oculto

Si la partición o unidad de su sistema está cifrada con VeraCrypt, deberá introducir su contraseña de autenticación previa al arranque en la pantalla del cargador de arranque de VeraCrypt después de encender o reiniciar el ordenador. Es posible que alguien le obligue a descifrar el sistema operativo o a revelar la contraseña de autenticación previa al arranque. Existen muchas situaciones en las que no puede negarse a hacerlo (por ejemplo, debido a una extorsión). VeraCrypt le permite crear un sistema operativo oculto cuya existencia debería ser imposible de probar (siempre que se sigan ciertas directrices; consulte a continuación). Por lo tanto, no tendrá que descifrar ni revelar la contraseña del sistema operativo oculto.

Antes de continuar leyendo esta sección, asegúrese de haber leído la sección Volumen oculto y de que comprende qué es un volumen oculto de VeraCrypt.

Un sistema operativo oculto es un sistema (por ejemplo, Windows 7 o Windows XP) instalado en un volumen VeraCrypt oculto. Debería ser imposible demostrar la existencia de un volumen VeraCrypt oculto (siempre que se sigan ciertas directrices; para más información, consulte la sección " Volumen oculto") y, por lo tanto, debería ser imposible demostrar la existencia de un sistema operativo oculto.

Sin embargo, para arrancar un sistema cifrado con VeraCrypt, es necesario almacenar una copia sin cifrar del gestor de arranque de VeraCrypt en la unidad del sistema o en un disco de rescate de VeraCrypt. Por lo tanto, la mera presencia del gestor de arranque de VeraCrypt puede indicar que hay un sistema cifrado con VeraCrypt en el equipo. Por lo tanto, para explicar la presencia del gestor de arranque de VeraCrypt, el asistente de VeraCrypt ayuda a crear un segundo sistema operativo cifrado, denominado sistema operativo señuelo, durante el proceso de creación de un sistema operativo oculto. Un sistema operativo señuelo no debe contener archivos confidenciales. Su existencia no es secreta (no se instala en un volumen oculto). La contraseña del sistema operativo señuelo puede revelarse de forma segura a cualquiera que le obligue a revelar su contraseña de autenticación previa al arranque.*

Debe usar el sistema operativo señuelo con la misma frecuencia con la que usa su computadora. Idealmente, debería usarlo para todas las actividades que no involucren datos confidenciales. De lo contrario, la posible negación del sistema operativo oculto podría verse afectada (si revela la contraseña del sistema operativo señuelo a un adversario, este podría descubrir que el sistema no se usa con mucha frecuencia, lo que podría indicar la existencia de un sistema operativo oculto en su computadora). Tenga en cuenta que puede guardar datos en la partición del sistema señuelo en cualquier momento sin riesgo de que el volumen oculto se dañe (ya que el sistema señuelo no está instalado en el volumen externo; consulte a continuación).

Habrá dos contraseñas de autenticación previas al arranque: una para el sistema oculto y otra para el sistema señuelo. Si desea iniciar el sistema oculto, simplemente introduzca la contraseña correspondiente en la pantalla del cargador de arranque de VeraCrypt (que aparece después de encender o reiniciar el equipo). Asimismo, si desea iniciar el sistema señuelo (por ejemplo, si se lo solicita un adversario), simplemente introduzca la contraseña correspondiente en la pantalla del cargador de arranque de VeraCrypt.

Nota: Cuando ingresa una contraseña de autenticación previa al arranque, el cargador de arranque VeraCrypt primero intenta descifrar (usando la contraseña ingresada) los últimos 512 bytes de la primera pista lógica de la unidad del sistema (donde se encuentran los datos de la clave maestra cifrada para las particiones/unidades del sistema cifradas no ocultas).

---

* No es práctico (y por lo tanto no se admite) instalar sistemas operativos en dos volúmenes de VeraCrypt que estén integrados dentro de una sola partición, porque el uso del sistema operativo externo a menudo requeriría que los datos se escribieran en el área del sistema operativo oculto (y si dichas operaciones de escritura se impidieran utilizando la función de protección del volumen oculto, causaría inherentemente fallas del sistema, es decir, errores de "pantalla azul").

se almacenan normalmente). Si falla y existe una partición detrás de la partición activa, el gestor de arranque de VeraCrypt (incluso si no hay ningún volumen oculto en la unidad) intenta descifrar automáticamente (utilizando la misma contraseña introducida) el área de la primera partición detrás de la partición activa* donde podría estar almacenado el encabezado cifrado de un posible volumen oculto. Tenga en cuenta que VeraCrypt nunca sabe de antemano si existe un volumen oculto (el encabezado del volumen oculto no se puede identificar, ya que parece estar compuesto exclusivamente de datos aleatorios). Si el encabezado se descifra correctamente (para obtener información sobre cómo VeraCrypt determina que se descifró correctamente, consulte la sección Esquema de cifrado), la información sobre el tamaño del volumen oculto se recupera del encabezado descifrado (que aún está almacenado en la RAM) y el volumen oculto se monta (su tamaño también determina su desplazamiento). Para obtener más detalles técnicos, consulte la sección Esquema de cifrado en el capítulo Detalles técnicos.

Al ejecutarse, el sistema operativo oculto parece estar instalado en la misma partición que el sistema operativo original (el sistema señuelo). Sin embargo, en realidad, está instalado en la partición que lo respalda (en un volumen oculto). Todas las operaciones de lectura/escritura se redirigen de forma transparente desde la partición del sistema al volumen oculto. Ni el sistema operativo ni las aplicaciones sabrán que los datos escritos y leídos desde la partición del sistema se escriben y leen realmente desde la partición que lo respalda (desde/hacia un volumen oculto). Estos datos se cifran y descifran sobre la marcha, como de costumbre (con una clave de cifrado distinta a la utilizada para el sistema operativo señuelo).

Tenga en cuenta que también habrá una tercera contraseña: la del volumen externo. No es una contraseña de autenticación previa al arranque, sino una contraseña normal de volumen VeraCrypt. Puede revelarse de forma segura a cualquiera que le obligue a revelar la contraseña de la partición cifrada donde reside el volumen oculto (que contiene el sistema operativo oculto). Por lo tanto, la existencia del volumen oculto (y del sistema operativo oculto) permanecerá en secreto. Si no está seguro de comprender cómo es posible esto o qué es un volumen externo, lea la sección "Volumen oculto". El volumen externo debe contener algunos archivos de aspecto confidencial que no desea ocultar.

En resumen, habrá tres contraseñas en total. Dos de ellas pueden ser reveladas a un atacante (para el sistema señuelo y para el volumen externo). La tercera contraseña, para el sistema oculto, debe permanecer secreta.

Ejemplo de diseño de una unidad del sistema que contiene un sistema operativo oculto

*Si el tamaño de la partición activa es inferior a 256 MB, los datos se leen desde la segunda partición detrás de la activa (Windows 7 y posteriores, de manera predeterminada, no arrancan desde la partición en la que están instalados).

Proceso de creación de un sistema operativo oculto

Para iniciar el proceso de creación de un sistema operativo oculto, seleccione Sistema > Crear sistema operativo oculto y luego siga las instrucciones del asistente.

Inicialmente, el asistente verifica que exista una partición adecuada para un sistema operativo oculto en la unidad del sistema. Tenga en cuenta que, antes de crear un sistema operativo oculto, debe crear una partición para él en la unidad del sistema. Debe ser la primera partición después de la partición del sistema y debe ser al menos un 5 % más grande que la partición del sistema (la partición del sistema es aquella donde está instalado el sistema operativo actual). Sin embargo, si el volumen externo (que no debe confundirse con la partición del sistema) está formateado como NTFS, la partición para el sistema operativo oculto debe ser al menos un 110 % (2,1 veces) más grande que la partición del sistema (esto se debe a que el sistema de archivos NTFS siempre almacena los datos internos exactamente en el centro del volumen y, por lo tanto, el volumen oculto, que contendrá un clon de la partición del sistema, solo puede residir en la segunda mitad de la partición).

En los siguientes pasos, el asistente creará dos volúmenes VeraCrypt (externo y oculto) dentro de la primera partición, detrás de la partición del sistema. El volumen oculto contendrá el sistema operativo oculto.
El tamaño del volumen oculto siempre coincide con el tamaño de la partición del sistema. Esto se debe a que el volumen oculto deberá contener un clon del contenido de la partición del sistema (ver más abajo). Tenga en cuenta que el clon se cifrará con una clave de cifrado diferente a la del original.
Antes de comenzar a copiar algunos archivos de aspecto confidencial al volumen externo, el asistente le indica el tamaño máximo de espacio recomendado que deben ocupar los archivos, de modo que haya suficiente espacio libre en el volumen externo para el volumen oculto.

Observación: Después de copiar algunos archivos sensibles al volumen externo, se analizará el mapa de bits del clúster para determinar el tamaño del área ininterrumpida de espacio libre cuyo extremo está alineado con el del volumen externo. Esta área albergará el volumen oculto, por lo que limita su tamaño máximo. Se determinará el tamaño máximo del volumen oculto y se verificará que sea mayor que el tamaño de la partición del sistema (lo cual es necesario, ya que todo el contenido de la partición del sistema deberá copiarse al volumen oculto; consulte a continuación). Esto garantiza que los datos almacenados en el volumen externo no se sobrescriban con los datos escritos en el área del volumen oculto (por ejemplo, al copiar el sistema en él). El tamaño del volumen oculto siempre es el mismo que el tamaño de la partición del sistema.

A continuación, VeraCrypt creará el sistema operativo oculto copiando el contenido de la partición del sistema al volumen oculto. Los datos copiados se cifrarán automáticamente con una clave de cifrado distinta a la utilizada para el sistema operativo señuelo. El proceso de copia del sistema se realiza en el entorno previo al arranque (antes de que Windows se inicie) y puede tardar bastante tiempo en completarse: varias horas o incluso días (dependiendo del tamaño de la partición del sistema y del rendimiento del ordenador). Podrá interrumpir el proceso, apagar el ordenador, iniciar el sistema operativo y reanudarlo.

Sin embargo, si lo interrumpe, todo el proceso de copia del sistema deberá comenzar desde el principio (ya que el contenido de la partición del sistema no debe cambiar durante la clonación). El sistema operativo oculto será inicialmente un clon del sistema operativo con el que inició el asistente.

Windows crea (normalmente, sin su conocimiento ni consentimiento) diversos archivos de registro, archivos temporales, etc., en la partición del sistema. También guarda el contenido de la RAM en archivos de hibernación y paginación ubicados en la partición del sistema. Por lo tanto, si un atacante analizara los archivos almacenados en la partición donde reside el sistema original (del cual el sistema oculto es un clon), podría descubrir, por ejemplo, que utilizó el asistente de VeraCrypt en el modo de creación de sistemas ocultos (lo que podría indicar la existencia de un sistema operativo oculto en su equipo). Para evitar estos problemas, VeraCrypt borrará de forma segura todo el contenido de la partición donde reside el sistema original.

Tras la creación del sistema oculto, para lograr una negación plausible, VeraCrypt le solicitará que instale un nuevo sistema en la partición y lo cifre con VeraCrypt.
De esta forma crearás el sistema señuelo y se completará todo el proceso de creación del sistema operativo oculto.

Nota: VeraCrypt borrará el contenido de la partición donde reside el sistema original, llenándola completamente con datos aleatorios. Si le revelaste la contraseña del sistema señuelo a un adversario y este te preguntara por qué el espacio libre de la partición del sistema (señuelo) contiene datos aleatorios, podrías responder, por ejemplo: "La partición contenía anteriormente un sistema cifrado por VeraCrypt, pero olvidé la contraseña de autenticación previa al arranque (o el sistema se dañó y dejó de arrancar), así que tuve que reinstalar Windows y cifrar la partición de nuevo".

Negación plausible y protección contra fugas de datos

Por razones de seguridad, cuando se ejecuta un sistema operativo oculto, VeraCrypt garantiza que todos los sistemas de archivos locales no cifrados y los volúmenes VeraCrypt no ocultos sean de solo lectura (es decir, no se pueden escribir archivos en dichos sistemas de archivos o volúmenes VeraCrypt).* Se permite escribir datos en cualquier sistema de archivos que resida dentro de un volumen VeraCrypt oculto (siempre que el volumen oculto no esté ubicado en un contenedor almacenado en un sistema de archivos no cifrado o en cualquier otro sistema de archivos de solo lectura).

Hay tres razones principales por las que se han implementado tales contramedidas:

1. Permite la creación de una plataforma segura para el montaje de volúmenes VeraCrypt ocultos.
   Tenga en cuenta que recomendamos oficialmente que los volúmenes ocultos se monten solo cuando se esté ejecutando un sistema operativo oculto. Para obtener más información, consulte la subsección "Requisitos y precauciones de seguridad para volúmenes ocultos".

2. En algunos casos, es posible determinar que, en un momento dado, un sistema de archivos no se montó (o que un archivo del sistema no se guardó ni se accedió desde dentro) en una instancia específica de un sistema operativo (por ejemplo, analizando y comparando registros del sistema de archivos, marcas de tiempo de archivos, registros de aplicaciones, registros de errores, etc.). Esto podría indicar que hay un sistema operativo oculto instalado en el equipo. Las contramedidas previenen estos problemas.

3. Previene la corrupción de datos y permite una hibernación segura. Al reanudar Windows tras la hibernación, asume que todos los sistemas de archivos montados se encuentran en el mismo estado que cuando el sistema entró en hibernación. VeraCrypt garantiza esto protegiendo contra escritura cualquier sistema de archivos accesible tanto desde los sistemas señuelo como desde los ocultos. Sin esta protección, el sistema de archivos podría corromperse al ser montado por un sistema mientras el otro está en hibernación.

Si necesita transferir archivos de forma segura desde el sistema señuelo al sistema oculto, siga estos pasos:

1. Inicie el sistema de señuelo.
2. Guarde los archivos en un volumen sin cifrar o en un volumen VeraCrypt externo/normal.
3. Inicie el sistema oculto. 4. Si
guardó los archivos en un volumen VeraCrypt, móntelo (se montará automáticamente como sólo lectura).
5. Copie los archivos a la partición del sistema oculta o a otro volumen oculto.

*Esto no se aplica a sistemas de archivos en medios tipo CD/DVD ni en dispositivos/medios personalizados, atípicos o no estándar.

Posibles explicaciones para la existencia de dos particiones VeraCrypt en una sola unidad

Un adversario podría preguntarle por qué creó dos particiones cifradas con VeraCrypt en una sola unidad (una partición del sistema y otra que no es del sistema) en lugar de cifrar todo el disco con una sola clave de cifrado. Hay muchas razones posibles para hacerlo. Sin embargo, si no conoce ninguna...

(además de crear un sistema operativo oculto), puede proporcionar, por ejemplo, una de las siguientes explicaciones:

- Si hay más de dos particiones en una unidad del sistema y desea cifrar solo dos de ellas (la partición del sistema y la posterior) y dejar las demás sin cifrar (por ejemplo, para obtener el mejor rendimiento posible al leer y escribir datos confidenciales en dichas particiones), la única forma de hacerlo es cifrar ambas particiones por separado (tenga en cuenta que, con una sola clave de cifrado, VeraCrypt podría cifrar toda la unidad del sistema y todas sus particiones, pero no puede cifrar solo dos; solo una o todas las particiones se pueden cifrar con una sola clave). Como resultado, habrá dos particiones VeraCrypt adyacentes en la unidad del sistema (la primera será una partición del sistema y la segunda, una partición no del sistema), cada una cifrada con una clave diferente (lo que también ocurre al crear un sistema operativo oculto, y por lo tanto, se puede explicar de esta manera).

  Si no conoce ninguna buena razón por la que debería haber más de una partición en una unidad del sistema:

  Generalmente se recomienda separar los archivos que no son del sistema (documentos) de los archivos del sistema. Una de las formas más fáciles y confiables de hacerlo es crear dos particiones en la unidad del sistema: una para el sistema operativo y la otra para los documentos (archivos que no son del sistema).
  Las razones por las que se recomienda esta práctica incluyen:
  Si el sistema de archivos de una de las particiones está dañado, los archivos de esa partición pueden corromperse o perderse, mientras que los de la otra no se ven afectados. Es más fácil reinstalar el sistema sin perder los documentos (la reinstalación de un sistema operativo implica formatear la partición del sistema, tras lo cual se pierden todos los archivos almacenados). Si el sistema está dañado, la reinstalación completa suele ser la única opción.

Un algoritmo de cifrado en cascada (p. ej., AES-Twofish-Serpent) puede ser mucho más lento que uno sin cascada (p. ej., AES). Sin embargo, un algoritmo de cifrado en cascada puede ser más seguro que uno sin cascada (por ejemplo, la probabilidad de que tres algoritmos de cifrado distintos se rompan, p. ej., debido a los avances en criptoanálisis, es significativamente menor que la probabilidad de que solo uno de ellos se rompa). Por lo tanto, si cifra el volumen externo con un algoritmo de cifrado en cascada y el sistema señuelo con un algoritmo sin cascada, puede responder que busca el mejor rendimiento (y la seguridad adecuada) para la partición del sistema, y la mayor seguridad posible (pero peor rendimiento) para la partición que no es del sistema (es decir, el volumen externo), donde almacena los datos más sensibles, a los que no necesita acceder con mucha frecuencia (a diferencia del sistema operativo, que usa con mucha frecuencia y, por lo tanto, necesita que tenga el mejor rendimiento posible). En la partición del sistema, se almacenan datos que son menos confidenciales (pero a los que necesita acceder muy a menudo) que los datos que almacena en la partición que no es del sistema (es decir, en el volumen externo).

• Siempre que encripte el volumen externo con un algoritmo de cifrado en cascada (por ejemplo, AES-Twofish-Serpent) y el sistema señuelo con un algoritmo de cifrado que no sea en cascada (por ejemplo, AES), también puede responder que quería evitar los problemas que VeraCrypt advierte al intentar seleccionar un algoritmo de cifrado en cascada para el cifrado del sistema (consulte la lista de problemas a continuación). Por lo tanto, para evitarlos, decidió cifrar la partición del sistema con un algoritmo distinto del de cifrado en cascada. Sin embargo, seguía queriendo usar un algoritmo de cifrado en cascada (porque es más seguro que uno distinto) para los datos más sensibles, así que decidió crear una segunda partición, a la que estos problemas no afectan (porque no es del sistema) y cifrarla con un algoritmo de cifrado en cascada. En la partición del sistema, se almacenan datos menos sensibles que los que se almacenan en la partición distinta del sistema (es decir, en el volumen externo).

Nota: Cuando el usuario intenta cifrar la partición del sistema con un algoritmo de cifrado en cascada, VeraCrypt le advierte que puede causar los siguientes problemas (e implícitamente recomienda elegir en su lugar un algoritmo de cifrado que no sea en cascada):

En los algoritmos de cifrado en cascada, el cargador de arranque VeraCrypt es más grande de lo normal y, por lo tanto, no hay suficiente espacio en la primera pista de la unidad para una copia de seguridad. Por lo tanto, si se daña (lo que suele ocurrir, por ejemplo, durante la activación de programas antipiratería mal diseñados), el usuario debe usar el disco de rescate VeraCrypt para repararlo o arrancar el sistema.

o En algunas computadoras, salir del modo hibernación demora más tiempo.

• A diferencia de una contraseña para un volumen VeraCrypt que no es del sistema, una autenticación previa al arranque La contraseña debe escribirse cada vez que se enciende o reinicia el ordenador. Por lo tanto, si la contraseña de autenticación previa al arranque es larga (necesaria por seguridad), puede resultar tedioso escribirla con tanta frecuencia. Por lo tanto, puede responder que le resultó más conveniente usar una contraseña corta (y, por lo tanto, menos segura) para la partición del sistema (es decir, el sistema señuelo) y que le conviene almacenar los datos más confidenciales (a los que no necesita acceder con tanta frecuencia) en la partición VeraCrypt (es decir, en el volumen externo), para la cual eligió una contraseña muy larga.

Dado que la contraseña de la partición del sistema no es muy segura (debido a su brevedad), no se almacenan intencionalmente datos confidenciales en ella. Sin embargo, se prefiere cifrar la partición, ya que se almacenan datos potencialmente confidenciales o poco confidenciales como resultado del uso diario del ordenador (por ejemplo, contraseñas de foros en línea que visita, que su navegador puede recordar automáticamente, historial de navegación, aplicaciones que ejecuta, etc.).

• Cuando un atacante se apodera de su computadora cuando hay un volumen VeraCrypt montado (por ejemplo, ejemplo, cuando usa una computadora portátil afuera), en la mayoría de los casos, puede leer cualquier dato almacenado en el volumen (los datos se descifran sobre la marcha a medida que los lee). Por lo tanto, puede ser conveniente limitar al mínimo el tiempo que el volumen está montado. Obviamente, esto puede ser imposible o difícil si los datos confidenciales se almacenan en una partición del sistema cifrada o en una unidad del sistema completamente cifrada (porque también tendría que limitar al mínimo el tiempo que trabaja con la computadora). Por lo tanto, puede responder que creó una partición separada (cifrada con una clave diferente a la de su partición del sistema) para sus datos más confidenciales y que la monta solo cuando es necesario y la desmonta lo antes posible (para limitar al mínimo el tiempo que el volumen está montado). En la partición del sistema, almacena datos que son menos confidenciales (pero a los que necesita acceder con frecuencia) que los datos que almacena en la partición que no es del sistema (es decir, en el volumen externo).

Precauciones y requisitos de seguridad relacionados con los sistemas operativos ocultos

Dado que un sistema operativo oculto reside en un volumen VeraCrypt oculto, el usuario de dicho sistema debe cumplir con todos los requisitos y precauciones de seguridad aplicables a los volúmenes VeraCrypt ocultos normales. Estos requisitos y precauciones, así como los requisitos y precauciones adicionales específicos de los sistemas operativos ocultos, se detallan en la subsección « Requisitos y precauciones de seguridad para volúmenes ocultos».

ADVERTENCIA: Si no protege el volumen oculto (para obtener información sobre cómo hacerlo, consulte la sección " Protección de volúmenes ocultos contra daños"), no escriba en el volumen externo (tenga en cuenta que el sistema operativo señuelo no está instalado en el volumen externo). De lo contrario, podría sobrescribir y dañar el volumen oculto (y el sistema operativo oculto que contiene).

Si se han seguido todas las instrucciones del asistente y se han seguido los requisitos de seguridad y las precauciones enumeradas en la subsección Requisitos de seguridad y precauciones relacionados con volúmenes ocultos , debería ser imposible demostrar que el volumen oculto y el sistema operativo oculto existen, incluso cuando el volumen externo esté montado o cuando el sistema operativo señuelo se haya descifrado o iniciado.

Ventana principal del programa

Seleccionar archivo

Permite seleccionar un volumen de VeraCrypt alojado en archivos. Tras seleccionarlo, puede realizar diversas operaciones (por ejemplo, montarlo haciendo clic en "Montar"). También puede seleccionar un volumen arrastrando su icono al icono de "VeraCrypt.exe" (VeraCrypt se iniciará automáticamente) o a la ventana principal del programa.

Seleccionar dispositivo

Le permite seleccionar una partición VeraCrypt o un dispositivo de almacenamiento (como una memoria USB). Una vez seleccionado, puedes realizar varias operaciones con él (por ejemplo, montarlo haciendo clic en "Montar").

Nota: Hay una forma más cómoda de montar particiones/dispositivos de VeraCrypt: consulte la sección Dispositivos de montaje automático para obtener más información.

Montar

Tras hacer clic en "Montar", VeraCrypt intentará montar el volumen seleccionado usando las contraseñas almacenadas en caché (si las hay) y, si ninguna funciona, le solicitará una contraseña. Si introduce la contraseña correcta (o proporciona los archivos de claves correctos), el volumen se montará.
Importante: Tenga en cuenta que cuando sale de la aplicación VeraCrypt, el controlador de VeraCrypt continúa funcionando y no se desmonta ningún volumen de VeraCrypt.

Dispositivos de montaje automático

Esta función permite montar particiones/dispositivos VeraCrypt sin tener que seleccionarlos manualmente (haciendo clic en "Seleccionar dispositivo"). VeraCrypt escanea los encabezados de todas las particiones/dispositivos disponibles en el sistema (excepto unidades de DVD y dispositivos similares) uno por uno e intenta montar cada uno como un volumen VeraCrypt. Tenga en cuenta que no se puede identificar una partición/dispositivo VeraCrypt ni el cifrado con el que se ha cifrado. Por lo tanto, el programa no puede "encontrar" particiones VeraCrypt directamente. En su lugar, debe intentar montar cada partición/dispositivo (incluso sin cifrar) utilizando todos los algoritmos de cifrado y todas las contraseñas almacenadas en caché (si las hay). Por lo tanto, tenga en cuenta que este proceso puede tardar bastante en ordenadores lentos.

Si la contraseña introducida es incorrecta, se intentará el montaje usando las contraseñas en caché (si las hay). Si introduce una contraseña vacía y la opción " Usar archivos de claves" no está marcada, solo se usarán las contraseñas en caché al intentar montar automáticamente particiones/dispositivos. Si no necesita configurar las opciones de montaje, puede omitir la solicitud de contraseña manteniendo pulsada la tecla Mayús al hacer clic en "Montar dispositivos automáticamente" (solo se usarán las contraseñas en caché, si las hay).

Las letras de unidad se asignarán comenzando por la que esté seleccionada en la lista de unidades en la ventana principal.

Desmontar

Esta función permite desmontar el volumen VeraCrypt seleccionado en la lista de unidades de la ventana principal. Desmontar un volumen VeraCrypt significa cerrarlo e impedir la lectura y escritura en él.

Desmontar todo

Nota: La información de esta sección se aplica a todos los elementos de menú y botones con el mismo título o uno similar (por ejemplo, también se aplica al elemento de menú de la bandeja del sistema Desmontar todo).

Esta función permite desmontar varios volúmenes VeraCrypt. Desmontar un volumen VeraCrypt significa cerrarlo e impedir la lectura/escritura desde/hacia él. Esta función desmonta todos los volúmenes VeraCrypt montados, excepto los siguientes:

- Particiones/unidades dentro del alcance clave del cifrado del sistema activo (por ejemplo, una partición del sistema cifrada por VeraCrypt o una partición que no es del sistema ubicada en una unidad del sistema cifrada por VeraCrypt, montada cuando se ejecuta el sistema operativo cifrado).

- Volúmenes de VeraCrypt que no son completamente accesibles para la cuenta de usuario (por ejemplo, un volumen montado desde dentro de otra cuenta de usuario).

Volúmenes de VeraCrypt que no se muestran en la ventana de la aplicación. Por ejemplo, una instancia de VeraCrypt sin privilegios de administrador intentó desmontar volúmenes favoritos del sistema cuando la opción "Permitir que solo los administradores vean y desmonten volúmenes favoritos del sistema en VeraCrypt" estaba habilitada.

Borrar caché

Borra todas las contraseñas (que también pueden contener el contenido de los archivos de claves procesados) almacenadas en la memoria del controlador. Si no hay contraseñas en la caché, este botón está deshabilitado. Para obtener información sobre la caché de contraseñas, consulte la sección " Caché de contraseñas en la memoria del controlador".

Nunca guardes el historial

Si esta opción está deshabilitada, los nombres de archivo y/o las rutas de los últimos veinte archivos/dispositivos que se intentaron montar como volúmenes de VeraCrypt se guardarán en el archivo Historial (cuyo contenido se puede mostrar haciendo clic en el cuadro combinado Volumen en la ventana principal).

Cuando esta opción está habilitada, VeraCrypt borra las entradas de registro creadas por el selector de archivos de Windows para VeraCrypt y establece el "directorio actual" en el directorio de inicio del usuario (en modo portátil, en el directorio desde el que se inició VeraCrypt) cada vez que se selecciona un contenedor o un archivo de claves mediante el selector de archivos de Windows. Por lo tanto, el selector de archivos de Windows no recordará la ruta del último contenedor montado (ni del último archivo de claves seleccionado). Sin embargo, tenga en cuenta que no se garantiza que las operaciones descritas en este párrafo se realicen de forma fiable y segura (véase, por ejemplo, Requisitos y precauciones de seguridad), por lo que le recomendamos encarecidamente que encripte la partición/unidad del sistema en lugar de confiar en ellos (consulte Cifrado del sistema).

Además, si esta opción está habilitada, el campo de entrada de la ruta de volumen en la ventana principal de VeraCrypt se borra cada vez que oculta VeraCrypt.

Nota: Puede borrar el historial de volumen seleccionando Herramientas > Borrar historial de volumen.

Salida

Finaliza la aplicación VeraCrypt. El controlador continúa funcionando y no se desmontan volúmenes VeraCrypt. Al ejecutarse en modo portátil, el controlador VeraCrypt se descarga cuando ya no es necesario (por ejemplo, cuando se cierran todas las instancias de la aplicación principal o del Asistente de creación de volúmenes y no se monta ningún volumen VeraCrypt). Sin embargo, si fuerza el desmontaje en
a

Al ejecutar VeraCrypt en modo portátil o montar un volumen con formato NTFS grabable en Windows Vista o posterior, es posible que el controlador de VeraCrypt no se descargue al salir de VeraCrypt (solo se descargará al apagar o reiniciar el sistema). Esto evita diversos problemas causados por errores de Windows (por ejemplo, sería imposible reiniciar VeraCrypt mientras haya aplicaciones usando el volumen desmontado).

Herramientas de volumen

Cambiar la contraseña del volumen

Consulte la sección Volúmenes > Cambiar contraseña de volumen.

Algoritmo de derivación de claves de encabezado de conjunto

Consulte la sección Volúmenes > Algoritmo de derivación de clave de encabezado establecido.

Encabezado del volumen de respaldo

Consulte la sección Herramientas > Encabezado de volumen de respaldo.

Restaurar encabezado de volumen

Consulte la sección Herramientas > Restaurar encabezado de volumen.

Menú del programa

Nota: Para ahorrar espacio, en esta documentación solo se describen los elementos del menú que no se explican por sí solos.

Volúmenes > Montar automáticamente todos los volúmenes alojados en el dispositivo

Consulte la sección Dispositivos de montaje automático.

Volúmenes > Desmontar todos los volúmenes montados

Consulte la sección Desmontar todo.

Volúmenes > Cambiar contraseña de volumen

Permite cambiar la contraseña del volumen VeraCrypt seleccionado (independientemente de si el volumen es oculto o estándar). Solo se cambian la clave de encabezado y la clave de encabezado secundaria (modo XTS); la clave maestra permanece sin cambios. Esta función vuelve a cifrar el encabezado del volumen utilizando una clave de cifrado derivada de una nueva contraseña. Tenga en cuenta que el encabezado del volumen contiene la clave de cifrado maestra con la que se cifra el volumen. Por lo tanto, los datos almacenados en el volumen no se perderán después de usar esta función (el cambio de contraseña solo tardará unos segundos).

Para cambiar una contraseña de volumen de VeraCrypt, haga clic en Seleccionar archivo o Seleccionar dispositivo, luego seleccione el volumen y en el menú Volúmenes seleccione Cambiar contraseña de volumen.

Nota: Para obtener información sobre cómo cambiar una contraseña utilizada para la autenticación previa al arranque, consulte la sección Sistema > Cambiar contraseña.

Véase también el capítulo Requisitos y precauciones de seguridad.

PRF PKCS-5

En este campo puede seleccionar el algoritmo que se utilizará para derivar nuevas claves de encabezado de volumen (para obtener más información, consulte la sección Derivación de clave de encabezado, sal y recuento de iteraciones) y para generar la nueva sal (para obtener más información, consulte la sección Generador de números aleatorios).

Nota: Cuando VeraCrypt vuelve a cifrar un encabezado de volumen, el encabezado del volumen original se sobrescribe primero muchas veces (3, 7, 35 o 256 según la elección del usuario) con datos aleatorios para evitar que los adversarios utilicen técnicas como la microscopía de fuerza magnética o la microscopía de túnel de barrido de fuerza magnética [17] para recuperar el encabezado sobrescrito (sin embargo, consulte también el capítulo Requisitos y precauciones de seguridad).

Volúmenes > Algoritmo de derivación de claves de encabezado de conjunto

Esta función permite volver a cifrar un encabezado de volumen con una clave de encabezado derivada de una función PRF diferente (por ejemplo, en lugar de HMAC-RIPEMD-160, podría usar HMAC-Whirlpool). Tenga en cuenta que el encabezado del volumen contiene la clave de cifrado maestra con la que se cifra el volumen.
Por lo tanto, los datos almacenados en el volumen no se perderán después de usar esta función. Para más información

Para obtener más información, consulte la sección Derivación de clave de encabezado, sal y recuento de iteraciones.

Nota: Cuando VeraCrypt vuelve a cifrar un encabezado de volumen, el encabezado del volumen original se sobrescribe primero muchas veces (3, 7, 35 o 256 según la elección del usuario) con datos aleatorios para evitar que los adversarios utilicen técnicas como la microscopía de fuerza magnética o la microscopía de túnel de barrido de fuerza magnética [17] para recuperar el encabezado sobrescrito (sin embargo, consulte también el capítulo Requisitos y precauciones de seguridad).

Volúmenes > Agregar o quitar archivos de claves a o desde volúmenes > Eliminar todos los archivos clave del volumen

Consulte el capítulo Archivos de claves.

Favoritos > Agregar volumen montado a favoritos

Favoritos > Organizar volúmenes favoritos

Favoritos > Volúmenes de favoritos de montaje

Ver el capítulo Volúmenes favoritos.

Favoritos > Agregar volumen montado a los favoritos del sistema

Favoritos > Organizar volúmenes favoritos del sistema

Consulte el capítulo Volúmenes favoritos del sistema.

Sistema > Cambiar contraseña

Cambia la contraseña utilizada para la autenticación previa al arranque (consulte el capítulo Cifrado del sistema).

ADVERTENCIA: Su Disco de Rescate VeraCrypt le permite restaurar datos de claves si se dañan. Al hacerlo, también restaura la contraseña válida cuando se creó el Disco de Rescate VeraCrypt.
Por lo tanto, cada vez que cambie la contraseña, debe destruir su Disco de Rescate VeraCrypt y crear uno nuevo (seleccione Sistema > Crear Disco de Rescate). De lo contrario, un atacante podría descifrar la partición/unidad de su sistema usando la contraseña anterior (si encuentra el Disco de Rescate VeraCrypt antiguo y lo usa para restaurar los datos clave). Consulte también el capítulo " Requisitos y precauciones de seguridad".

Para obtener más información sobre cómo cambiar una contraseña, consulte la sección Volúmenes > Cambiar contraseña de volumen más arriba.

Sistema > Montar sin autenticación previa al arranque

Marque esta opción si necesita montar una partición dentro del alcance de la clave de cifrado del sistema sin autenticación previa al arranque. Por ejemplo, si necesita montar una partición ubicada en la unidad de sistema cifrada de otro sistema operativo que no se esté ejecutando. Esto puede ser útil, por ejemplo, al realizar una copia de seguridad o reparar un sistema operativo cifrado con VeraCrypt (desde otro sistema operativo).

Nota 1: Si necesita montar varias particiones a la vez, haga clic en “Montar dispositivos automáticamente”, luego haga clic en “Opciones de montaje” y habilite la opción “Montar partición usando cifrado del sistema sin autenticación previa al arranque”.

Tenga en cuenta que no puede utilizar esta función para montar particiones extendidas (lógicas) que estén ubicadas en una unidad de sistema completamente cifrada.

Herramientas > Borrar historial de volumen

Borra la lista que contiene los nombres de archivos (si están alojados en archivos) y las rutas de los últimos veinte volúmenes montados correctamente.

Herramientas > Configuración del disco Traveler

Consulte el capítulo Modo portátil.

Herramientas > Generador de archivos de claves

Consulte la sección Herramientas > Generador de archivos de claves en el capítulo Archivos de claves.

Herramientas > Encabezado del volumen de respaldo
Herramientas > Restaurar encabezado de volumen

Si el encabezado de un volumen de VeraCrypt está dañado, en la mayoría de los casos, es imposible montarlo. Por lo tanto, cada volumen creado por VeraCrypt (excepto las particiones del sistema) contiene un encabezado de copia de seguridad integrado, ubicado al final del volumen. Para mayor seguridad, también puede crear archivos de copia de seguridad externos del encabezado del volumen. Para ello, haga clic en Seleccionar dispositivo o Seleccionar archivo, seleccione el volumen, seleccione Herramientas > Copia de seguridad del encabezado del volumen y siga las instrucciones.

Nota: Para el cifrado del sistema, no hay un encabezado de copia de seguridad al final del volumen. Para volúmenes que no son del sistema, primero se realiza una operación de reducción para asegurar que todos los datos se coloquen al principio del volumen, dejando todo el espacio libre al final para tener un lugar donde colocar el encabezado de copia de seguridad. Para particiones del sistema, no es posible realizar esta operación de reducción mientras Windows esté en ejecución, por lo que no se puede crear el encabezado de copia de seguridad al final de la partición. La alternativa para el cifrado del sistema es usar el Disco de Rescate.

Nota: Un encabezado de copia de seguridad (integrado o externo) no es una copia del encabezado del volumen original, ya que está cifrado con una clave de encabezado diferente, derivada de una sal distinta (consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones"). Al cambiar la contraseña o los archivos de claves del volumen, o al restaurar el encabezado desde la copia de seguridad del encabezado integrado (o externo), tanto el encabezado del volumen como el encabezado de la copia de seguridad (integrado en el volumen) se vuelven a cifrar con claves de encabezado derivadas de sales recién generadas (la sal del encabezado del volumen es diferente de la del encabezado de la copia de seguridad). Cada sal es generada por el generador de números aleatorios de VeraCrypt (consulte la sección " Generador de números aleatorios").

Se pueden usar ambos tipos de copias de seguridad de encabezado (integradas y externas) para reparar un encabezado de volumen dañado. Para ello, haga clic en Seleccionar dispositivo o Seleccionar archivo, seleccione el volumen, seleccione Herramientas > Restaurar encabezado de volumen y siga las instrucciones.

ADVERTENCIA: Al restaurar el encabezado de un volumen, también se restaura la contraseña del volumen válida al crear la copia de seguridad. Además, si se necesitan archivos de clave para montar un volumen al crear la copia de seguridad, también se necesitarán para montarlo.

De nuevo después de restaurar el encabezado del volumen. Para más información, consulte la sección "Esquema de cifrado" en el capítulo "Detalles técnicos".

Después de crear una copia de seguridad del encabezado del volumen, es posible que necesite crear una nueva solo cuando Cambia la contraseña del volumen o los archivos de claves. De lo contrario, el encabezado del volumen permanece. sin modificar para que la copia de seguridad del encabezado del volumen permanezca actualizada.

Nota: Aparte de la sal (que es una secuencia de números aleatorios), los archivos de respaldo de encabezado externo no contienen información no cifrada y no se pueden descifrar sin conocer la información correcta. Contraseña y/o proporcionar los archivos de clave correctos. Para más información, consulte el capítulo " Detalles técnicos".

Cuando se crea una copia de seguridad del encabezado externo, tanto el encabezado del volumen estándar como el Se realiza una copia de seguridad del área donde se puede almacenar un encabezado de volumen oculto, incluso si no hay ningún encabezado oculto. Volumen dentro del volumen (para preservar la negación plausible de volúmenes ocultos). Si hay ningún volumen oculto dentro del volumen, el área reservada para el encabezado del volumen oculto en El archivo de respaldo se llenará con datos aleatorios (para preservar la negación plausible).

Al restaurar un encabezado de volumen, debe elegir el tipo de volumen cuyo encabezado desea restaurar (un volumen estándar u oculto). Solo se puede usar un encabezado de volumen. Restaurados a la vez. Para restaurar ambos encabezados, debe usar la función dos veces (Herramientas > Restaurar encabezado de volumen). Deberá ingresar la contraseña correcta (y/o proporcionar los archivos de clave correctos) que eran válidos cuando se creó la copia de seguridad del encabezado del volumen. La contraseña (y/o los archivos de claves) también determinarán automáticamente el tipo de volumen. encabezado a restaurar, es decir, estándar u oculto (tenga en cuenta que VeraCrypt determina el tipo (a través del proceso de prueba y error).

Nota: Si el usuario no proporciona la contraseña correcta (y/o los archivos de claves) dos veces seguidas cuando Al intentar montar un volumen, VeraCrypt intentará montar el volumen automáticamente usando el encabezado de respaldo incorporado (además de intentar montarlo usando el encabezado principal) cada uno la siguiente vez que el usuario intenta montar el volumen (hasta que hace clic) Cancelar). Si VeraCrypt no puede descifrar el encabezado principal pero descifra correctamente el encabezado de copia de seguridad integrado al mismo tiempo, se monta el volumen y el usuario Se advirtió que el encabezado del volumen está dañado (y se informó cómo repararlo).

Configuración > Opciones de rendimiento y controlador

Abre el cuadro de diálogo Rendimiento, donde puede habilitar o deshabilitar la aceleración de hardware AES y la paralelización basada en subprocesos. También puede cambiar la siguiente opción del controlador:

Habilitar la compatibilidad con códigos de control de disco extendidos

Si está habilitado, el controlador VeraCrypt permitirá devolver información técnica ampliada sobre los volúmenes montados mediante el código de control IOCTL_STORAGE_QUERY_PROPERTY. Este código de control siempre es compatible con las unidades físicas y algunas aplicaciones pueden requerirlo para obtener información técnica sobre una unidad (por ejemplo, el programa fsutil de Windows utiliza este código de control para obtener el tamaño del sector físico de una unidad).

Al habilitar esta opción, el comportamiento de los volúmenes VeraCrypt se acerca mucho más al de los discos físicos y, si está deshabilitada, las aplicaciones pueden distinguir fácilmente entre discos físicos y volúmenes VeraCrypt, ya que enviar este código de control a un volumen VeraCrypt generará un error.

Deshabilite esta opción si experimenta problemas de estabilidad (como problemas de acceso al volumen o BSOD del sistema) que pueden ser causados por software y controladores mal escritos.

Configuración > Preferencias

Invoca la ventana de diálogo Preferencias, donde puede cambiar, entre otras cosas, las siguientes opciones:

Borrar las contraseñas almacenadas en caché al salir

Si está habilitado, las contraseñas (que también pueden contener contenidos de archivos de clave procesados) se almacenan en caché en el controlador La memoria se borrará cuando VeraCrypt salga.

Almacenar contraseñas en caché en la memoria del controlador

Cuando se marca, se guardan las contraseñas y/o el contenido del archivo de claves procesado hasta los últimos cuatro Los volúmenes de VeraCrypt montados correctamente se almacenan en caché. Esto permite el montaje de volúmenes. sin tener que escribir sus contraseñas (y seleccionar archivos de claves) repetidamente. VeraCrypt nunca guarda cualquier contraseña en un disco (sin embargo, consulte el capítulo Requisitos de seguridad y Precauciones).
El almacenamiento en caché de contraseñas se puede habilitar o deshabilitar en las Preferencias (Configuración > Preferencias) y en la ventana de solicitud de contraseña. Si la partición/unidad del sistema está cifrada, el almacenamiento en caché de La contraseña de autenticación previa al arranque se puede habilitar o deshabilitar en el cifrado del sistema Configuración (Configuración > 'Cifrado del sistema').

Contraseña de caché temporal durante las operaciones de "Montar volúmenes favoritos"

Cuando esta opción no está marcada (es la opción predeterminada), VeraCrypt mostrará la ventana de solicitud de contraseña para cada volumen favorito durante la ejecución de la operación "Montar volúmenes favoritos" y cada contraseña se borra una vez que se monta el volumen (a menos que el almacenamiento en caché de contraseñas esté habilitado).

Si esta opción está marcada y hay dos o más volúmenes favoritos, durante la operación "Montar volúmenes favoritos", VeraCrypt probará primero la contraseña del favorito anterior y, si no funciona, mostrará una ventana de solicitud de contraseña. Esta lógica se aplica a partir del segundo volumen favorito. Una vez procesados todos los volúmenes favoritos, la contraseña se borra de la memoria.

Esta opción es útil cuando los volúmenes favoritos comparten la misma contraseña, ya que la ventana de solicitud de contraseña solo se mostrará una vez para el primer favorito y VeraCrypt montará automáticamente todos los favoritos posteriores.

Tenga en cuenta que, dado que no podemos asumir que todos los favoritos usan el mismo PRF (hash) ni el mismo modo TrueCrypt, VeraCrypt usa la detección automática para el PRF de los volúmenes favoritos posteriores e intenta ambos valores TrueCryptMode (falso, verdadero), lo que significa que el tiempo de montaje total será más lento en comparación con el montaje individual de cada volumen con la selección manual del PRF correcto y el TrueCryptMode correcto.

Abra la ventana del Explorador para el volumen montado correctamente

Si esta opción está marcada, luego de que se haya montado exitosamente un volumen VeraCrypt, un La ventana del explorador que muestra el directorio raíz del volumen (por ejemplo, T:\) se abrirá automáticamente. abierto.

Utilice un icono de barra de tareas diferente cuando haya volúmenes montados

Si está habilitado, la apariencia del icono de la barra de tareas de VeraCrypt (que se muestra dentro de la bandeja del sistema) El área de notificación) es diferente mientras se monta un volumen VeraCrypt, excepto lo siguiente:

- Particiones/unidades dentro del alcance clave del cifrado del sistema activo (por ejemplo, una partición del sistema cifrada por VeraCrypt o una partición que no es del sistema ubicada en una unidad del sistema cifrada por VeraCrypt, montada cuando se ejecuta el sistema operativo cifrado).

- Volúmenes de VeraCrypt que no son completamente accesibles para la cuenta de usuario (por ejemplo, un volumen montado desde dentro de otra cuenta de usuario).

Volúmenes de VeraCrypt que no se muestran en la ventana de la aplicación. Por ejemplo, una instancia de VeraCrypt sin privilegios de administrador intentó desmontar volúmenes favoritos del sistema cuando la opción "Permitir que solo los administradores vean y desmonten volúmenes favoritos del sistema en VeraCrypt" estaba habilitada.

Tarea en segundo plano de VeraCrypt: habilitada

Consulte el capítulo Tarea en segundo plano de VeraCrypt.

Tarea en segundo plano de VeraCrypt: salir cuando no haya volúmenes montados

Si esta opción está marcada, la tarea en segundo plano de VeraCrypt se cierra automáticamente y sin intervención del usuario en cuanto no haya volúmenes de VeraCrypt montados. Para más información, consulte el capítulo " Tarea en segundo plano de VeraCrypt". Tenga en cuenta que esta opción no se puede desactivar cuando VeraCrypt se ejecuta en modo portátil.

Desmontar automáticamente el volumen después de que no se hayan leído ni escrito datos en él

Después de que no se hayan escrito ni leído datos en un volumen VeraCrypt durante n minutos, el volumen se desmonta automáticamente.

Forzar el desmontaje automático incluso si el volumen contiene archivos o directorios abiertos

Esta opción solo se aplica al desmontaje automático (no al desmontaje normal). Fuerza el desmontaje (sin preguntar) del volumen que se va a desmontar automáticamente si contiene archivos o directorios abiertos (es decir, archivos o directorios que el sistema o las aplicaciones están usando).

Volúmenes de montaje

Si aún no lo ha hecho, lea las secciones ' Montar' y el capítulo Ventana principal del programa. 'Dispositivos de montaje automático' en el

Contraseña de caché en la memoria del controlador

Esta opción se puede configurar en el cuadro de diálogo de introducción de contraseña para que se aplique solo a ese intento de montaje en particular. También se puede configurar como predeterminada en las Preferencias. Para obtener más información, consulte la sección Configuración > Preferencias, subsección Almacenar contraseñas en la memoria del controlador.

Opciones de montaje

Las opciones de montaje afectan los parámetros del volumen que se va a montar. El cuadro de diálogo Opciones de montaje se abre haciendo clic en el botón Opciones de montaje en el cuadro de diálogo de introducción de contraseña. Si se guarda una contraseña correcta en caché, los volúmenes se montan automáticamente al hacer clic en "Montar". Si necesita cambiar las opciones de montaje de un volumen que se va a montar con una contraseña guardada en caché, mantenga pulsada la tecla Control (Ctrl) mientras hace clic en "Montar" o en un volumen favorito del menú Favoritos , o seleccione "Montar con opciones" en el menú Volúmenes .

Las opciones de montaje predeterminadas se pueden configurar en las preferencias principales del programa (Configuración > Preferencias).

Montar el volumen como de sólo lectura

Cuando está marcada, no será posible escribir ningún dato en el volumen montado.

Montar el volumen como medio extraíble

Consulte la sección Volumen montado como medio extraíble.

Utilice el encabezado de respaldo integrado en el volumen si está disponible

Todos los volúmenes creados por VeraCrypt contienen un encabezado de copia de seguridad integrado (ubicado al final del volumen). Si marca esta opción, VeraCrypt intentará montar el volumen utilizando dicho encabezado. Tenga en cuenta que si el encabezado del volumen está dañado, no es necesario usar esta opción.
En su lugar, puede reparar el encabezado seleccionando Herramientas > Restaurar encabezado de volumen.

Montar la partición usando el cifrado del sistema sin autenticación previa al arranque

Marque esta opción si necesita montar una partición dentro del alcance de la clave de cifrado del sistema sin autenticación previa al arranque. Por ejemplo, si necesita montar una partición ubicada en la unidad de sistema cifrada de otro sistema operativo que no se esté ejecutando. Esto puede ser útil, por ejemplo, al realizar una copia de seguridad o reparar un sistema operativo cifrado con VeraCrypt (desde otro sistema operativo). Tenga en cuenta que esta opción también se puede activar al usar las funciones "Montar dispositivos automáticamente" o "Montar todos los volúmenes alojados en el dispositivo automáticamente" .

Protección de volumen oculto

Consulte la sección Protección de volúmenes ocultos contra daños.

Paralelización

Si su ordenador tiene un procesador multinúcleo (o varios procesadores), VeraCrypt utiliza todos los núcleos (o procesadores) en paralelo para el cifrado y descifrado. Por ejemplo, cuando VeraCrypt descifra un fragmento de datos, primero lo divide en varias partes más pequeñas. El número de partes es igual al número de núcleos (o procesadores). A continuación, todas las partes se descifran en paralelo (la parte 1 la descifra el subproceso 1, la parte 2 la descifra el subproceso 2, etc.). El mismo método se utiliza para el cifrado.

Entonces, si su computadora tiene, por ejemplo, un procesador de cuatro núcleos, el cifrado y el descifrado son cuatro veces más rápidos que en un procesador de un solo núcleo con especificaciones equivalentes (así mismo, son dos veces más rápidos en procesadores de doble núcleo, etc.).

El aumento en la velocidad de cifrado/descifrado es directamente proporcional al número de núcleos y/o procesadores.

Nota: Los procesadores con tecnología Hyper-Threading proporcionan múltiples núcleos lógicos por cada núcleo físico (o múltiples procesadores lógicos por cada procesador físico). Cuando Hyper-Threading está habilitado en la configuración del firmware del equipo (p. ej., BIOS), VeraCrypt crea un subproceso por cada núcleo lógico/procesador. Por ejemplo, en un procesador de 6 núcleos que proporciona dos núcleos lógicos por cada núcleo físico, VeraCrypt utiliza 12 subprocesos.

Si su computadora tiene un procesador/CPU multinúcleo (o varios procesadores/CPU), la derivación de claves de encabezado también se paraleliza. Como resultado, el montaje de un volumen es mucho más rápido en un procesador multinúcleo (o computadora multiprocesador) que en un procesador de un solo núcleo (o computadora de un solo procesador) con especificaciones equivalentes.

Tubería

Al cifrar o descifrar datos, VeraCrypt utiliza el denominado procesamiento asíncrono (pipelining). Mientras una aplicación carga una parte de un archivo desde un volumen o unidad cifrados con VeraCrypt, VeraCrypt lo descifra automáticamente (en RAM). Gracias al pipelining, la aplicación no tiene que esperar a que se descifre ninguna parte del archivo y puede empezar a cargar otras partes inmediatamente. Lo mismo ocurre con el cifrado al escribir datos en un volumen o unidad cifrados.

La canalización permite leer y escribir datos en una unidad cifrada tan rápido como si la unidad no estuviera cifrada (lo mismo se aplica a los volúmenes de VeraCrypt alojados en archivos y particiones).*

Nota: La canalización se implementa solo en las versiones de Windows de VeraCrypt.

---

* Algunas unidades de estado sólido comprimen los datos internamente, lo que parece aumentar la velocidad real de lectura/escritura cuando los datos son comprimibles (por ejemplo, archivos de texto). Sin embargo, los datos cifrados no se pueden comprimir (ya que parecen consistir únicamente en "ruido" aleatorio sin patrones comprimibles). Esto puede tener diversas implicaciones. Por ejemplo, el software de evaluación comparativa que lee o escribe datos comprimibles (como secuencias de ceros) reportará velocidades más bajas en volúmenes cifrados que en volúmenes sin cifrar (para evitar esto, utilice software de evaluación comparativa que lea/escriba datos aleatorios u otros tipos de datos no comprimibles).

Aceleración de hardware

Algunos procesadores (CPU) admiten el cifrado AES acelerado por hardware,* que suele ser entre 4 y 8 veces más rápido que el cifrado realizado mediante la implementación puramente de software en los mismos procesadores.

De forma predeterminada, VeraCrypt utiliza AES acelerado por hardware en ordenadores con procesadores que admiten las instrucciones AES-NI de Intel. Específicamente, VeraCrypt utiliza las instrucciones AES-NI que realizan las llamadas rondas AES (es decir, las partes principales del algoritmo AES).† VeraCrypt no utiliza ninguna de las instrucciones AES-NI que generan claves.

Nota: De manera predeterminada, VeraCrypt también utiliza AES acelerado por hardware cuando un sistema Windows cifrado se inicia o se reanuda desde la hibernación (siempre que el procesador admita las instrucciones Intel AES-NI).

Para saber si VeraCrypt puede usar AES acelerado por hardware en su computadora, seleccione Configuración > Rendimiento/Configuración del controlador y marque el campo denominado 'El procesador (CPU) en esta computadora admite la aceleración de hardware para AES'.

Para saber si el procesador que desea adquirir es compatible con las instrucciones Intel AES-NI (también llamadas "Nuevas Instrucciones AES"), que VeraCrypt utiliza para AES acelerado por hardware, consulte la documentación del procesador o póngase en contacto con el proveedor/fabricante. También puede hacer clic aquí. Para ver una lista oficial de procesadores Intel compatibles con las instrucciones AES-NI, tenga en cuenta que algunos procesadores Intel, que el sitio web de Intel indica como compatibles con AES-NI, solo las admiten con una actualización de la configuración del procesador (por ejemplo, i7-2630/2635QM, i7-2670/2675QM, i5-2430/2435M, i5-2410/2415M). En estos casos, debe contactar al fabricante de la placa base o el ordenador para obtener una actualización de la BIOS que incluya la última actualización de la configuración del procesador.

Si desea desactivar la aceleración por hardware de AES (por ejemplo, porque desea que VeraCrypt utilice únicamente una implementación de AES de código abierto), puede hacerlo seleccionando Configuración > Opciones de rendimiento y controlador y desactivando la opción "Acelerar el cifrado/descifrado AES mediante las instrucciones AES del procesador". Tenga en cuenta que, al cambiar esta configuración, es necesario reiniciar el sistema operativo para garantizar que todos los componentes de VeraCrypt ejecuten internamente el cambio de modo solicitado. También tenga en cuenta que, al crear un disco de rescate de VeraCrypt, el estado de esta opción se escribe en el disco de rescate y se utiliza cada vez que se arranca desde él (lo que afecta a la fase de prearranque y al arranque inicial).

Para crear un nuevo disco de rescate de VeraCrypt, seleccione Sistema > Crear disco de rescate.

---

*En este capítulo, la palabra «cifrado» también se refiere al descifrado.

† Estas instrucciones son AESENC, AESENCLAST, AESDEC y AESDECLAST y realizan las siguientes transformaciones AES: ShiftRows, SubBytes, MixColumns, InvShiftRows, InvSubBytes, InvMixColumns y AddRoundKey (para más detalles sobre estas transformaciones, consulte [3]).

Teclas de acceso rápido

Para configurar las teclas de acceso rápido de VeraCrypt en todo el sistema, haga clic en Configuración > Teclas de acceso rápido. Tenga en cuenta que las teclas de acceso rápido solo funcionan cuando VeraCrypt o la tarea en segundo plano de VeraCrypt se está ejecutando.

Archivos de claves

Un archivo de claves es un archivo cuyo contenido se combina con una contraseña (para obtener información sobre el método utilizado para combinar un archivo de claves con una contraseña, consulte la sección Archivos de claves en el capítulo Detalles técnicos). Hasta que se proporcione el archivo de claves correcto, no se podrá montar ningún volumen que lo utilice.

No es necesario usar archivos de claves. Sin embargo, su uso tiene algunas ventajas:

- Puede mejorar la protección contra ataques de fuerza bruta (especialmente significativo si el volumen La contraseña no es muy fuerte).
- Permite el uso de tokens de seguridad y tarjetas inteligentes (ver más abajo).
- Permite que varios usuarios monten un solo volumen utilizando diferentes contraseñas de usuario o PIN. Simplemente proporcione a cada usuario un token de seguridad o una tarjeta inteligente que contenga el mismo archivo de clave VeraCrypt y permítales elegir su contraseña personal o PIN que protegerá su token de seguridad o tarjeta inteligente.
- Permite gestionar el acceso compartido de múltiples usuarios (todos los titulares de archivos de claves deben presentar sus archivos de claves) antes de que se pueda montar un volumen).

Cualquier tipo de archivo (por ejemplo, .txt, .exe, mp3* , .avi) puede usarse como archivo de clave de VeraCrypt (sin embargo, recomendamos usar archivos comprimidos, como .mp3, .jpg, .zip, etc.). Tenga en cuenta que VeraCrypt nunca modifica el contenido del archivo de clave.

Puede seleccionar más de un archivo de claves; el orden es indiferente. También puede dejar que VeraCrypt genere un archivo con contenido aleatorio y usarlo como archivo de claves. Para ello, seleccione Herramientas > Generador de archivos de claves.

Nota: Los archivos de clave actualmente no son compatibles con el cifrado del sistema.

ADVERTENCIA: Si pierde un archivo clave o si cambia cualquier bit de sus primeros 1024 kilobytes, será imposible montar volúmenes que utilicen el archivo clave.

ADVERTENCIA: Si el almacenamiento en caché de contraseñas está habilitado, este también contiene el contenido procesado de los archivos de claves utilizados para montar correctamente un volumen. De esta forma, es posible remontar el volumen incluso si el archivo de claves no está disponible o accesible. Para evitarlo, haga clic en "Borrar caché" o desactive el almacenamiento en caché de contraseñas (para más información, consulte la subsección "Configuración > Preferencias", elemento "Almacenar contraseñas en la memoria del controlador" en la sección "Menú del programa").

Consulte también la sección Elección de contraseñas y archivos de claves en el capítulo Requisitos y precauciones de seguridad.

Ventana de diálogo Archivos de claves

Si desea utilizar archivos clave (es decir, “aplicarlos”) al crear o montar volúmenes, o cambiar contraseñas, busque la opción “Usar archivos clave” y el botón Archivos clave debajo de un campo de ingreso de contraseña.

---

* Sin embargo, si usa un archivo MP3 como archivo de claves, debe asegurarse de que ningún programa modifique las etiquetas ID3 (p. ej., título de la canción, nombre del artista, etc.) dentro del archivo MP3. De lo contrario, será imposible montar volúmenes que usen el archivo de claves.

Estos elementos de control aparecen en varias ventanas de diálogo y siempre tienen las mismas funciones.
Marque la opción "Usar archivos de claves" y haga clic en "Archivos de claves". Debería aparecer el cuadro de diálogo "Archivos de claves", donde podrá especificar los archivos de claves (para ello, haga clic en " Agregar archivos " o " Agregar archivos de token") o las rutas de búsqueda de archivos de claves (haga clic en "Agregar ruta").

Tokens de seguridad y tarjetas inteligentes

VeraCrypt puede usar directamente archivos de claves almacenados en un token de seguridad o una tarjeta inteligente que cumpla con el estándar PKCS #11 (2.0 o posterior) [23] y que permita al usuario almacenar un archivo (objeto de datos) en el token/tarjeta. Para usar archivos de claves como archivos de claves de VeraCrypt, haga clic en " Agregar archivos de token" (en el cuadro de diálogo del archivo de claves).

El acceso a un archivo de claves almacenado en un token de seguridad o una tarjeta inteligente suele estar protegido mediante códigos PIN, que pueden introducirse mediante un teclado PIN físico o a través de la interfaz gráfica de usuario de VeraCrypt. También puede protegerse mediante otros medios, como lectores de huellas dactilares.

Para que VeraCrypt pueda acceder a un token de seguridad o una tarjeta inteligente, primero debe instalar una biblioteca de software PKCS #11 (2.0 o posterior) para el token o la tarjeta inteligente. Dicha biblioteca puede venir con el dispositivo o puede descargarse del sitio web del proveedor o de terceros.

Si su token de seguridad o tarjeta inteligente no contiene ningún archivo (objeto de datos) que pueda usar como archivo de clave de VeraCrypt, puede usar VeraCrypt para importar cualquier archivo al token o tarjeta inteligente (si el dispositivo lo admite). Para ello, siga estos pasos:

1. En la ventana de diálogo del archivo de clave, haga clic en Agregar archivos de token.
2. Si el token o la tarjeta inteligente está protegida por un PIN, una contraseña u otro medio (como un lector de huellas dactilares), autentíquese (por ejemplo, ingresando el PIN usando un teclado PIN de hardware).
3. Debería aparecer la ventana de diálogo "Archivo de clave del token de seguridad". En ella, haga clic en "Importar archivo de clave al token" y seleccione el archivo que desea importar al token o a la tarjeta inteligente.

Tenga en cuenta que puede importar, por ejemplo, archivos de claves de 512 bits con contenido aleatorio generado por VeraCrypt (consulte Herramientas > Generador de archivos de claves a continuación).

Para cerrar todas las sesiones de token de seguridad abiertas, seleccione Herramientas > Cerrar todas las sesiones de token de seguridad o defina y utilice una combinación de teclas de acceso rápido (Configuración > Teclas de acceso rápido > Cerrar todas las sesiones de token de seguridad).

Ruta de búsqueda del archivo de claves

Al agregar una carpeta en la ventana de diálogo del archivo clave (haga clic en Agregar ruta), especifica una ruta de búsqueda del archivo clave.
Todos los archivos que se encuentren en la ruta de búsqueda de archivos clave* se utilizarán como archivos clave, excepto los archivos que tengan la opción Oculto.
conjunto de atributos de archivo.

Importante: tenga en cuenta que las carpetas (y los archivos que contienen) y los archivos ocultos que se encuentran en una ruta de búsqueda de archivo clave se ignoran.

Las rutas de búsqueda de archivos de claves son especialmente útiles si, por ejemplo, almacena archivos de claves en una memoria USB que lleva consigo. Puede configurar la letra de la unidad de la memoria USB como ruta de búsqueda predeterminada. Para ello, seleccione Configuración > Archivos de claves predeterminados. A continuación, haga clic en Agregar ruta, busque la letra de unidad asignada a la memoria USB y haga clic en Aceptar. Ahora, cada vez que monte un volumen (y si la opción " Usar archivos de claves " está marcada en el cuadro de diálogo de contraseña), VeraCrypt escaneará la ruta y usará todos los archivos que encuentre en la memoria USB como archivos de claves.

ADVERTENCIA: Al agregar una carpeta (en lugar de un archivo) a la lista de archivos clave, solo se recuerda la ruta, no los nombres de archivo. Esto significa, por ejemplo, que si crea un nuevo archivo en la carpeta o copia un archivo adicional, no se podrán montar los volúmenes que usaron archivos clave de la carpeta (hasta que elimine el archivo recién agregado).

Contraseña vacía y archivo de claves

Al usar un archivo de claves, la contraseña puede estar vacía, por lo que este podría ser el único elemento necesario para montar el volumen (lo cual no recomendamos). Si se configuran y habilitan los archivos de claves predeterminados al montar un volumen, antes de solicitar la contraseña, VeraCrypt intenta montar automáticamente el volumen usando una contraseña vacía y los archivos de claves predeterminados (sin embargo, esto no aplica a la función "Montar dispositivos automáticamente"). Si necesita configurar las opciones de montaje (por ejemplo, montar como solo lectura, proteger volumen oculto, etc.) para un volumen que se monta de esta manera, mantenga presionada la tecla Control (Ctrl) mientras hace clic en "Montar" (o seleccione " Montar con opciones" en el menú " Volúmenes "). Esto abrirá el cuadro de diálogo "Opciones de montaje" .

Selección rápida

Los archivos clave y las rutas de búsqueda de archivos clave se pueden seleccionar rápidamente de las siguientes maneras:

- Haga clic con el botón derecho en el botón Archivos de claves en la ventana de diálogo de ingreso de contraseña y seleccione una de las opciones elementos del menú.
- Arrastre los iconos de archivo/carpeta correspondientes a la ventana de diálogo del archivo de claves o a la contraseña diálogo de entrada.

* Se encuentra en el momento en que está montando el volumen, cambiando su contraseña o realizando cualquier otra operación que involucre el re-cifrado del encabezado del volumen.

Volúmenes > Agregar o quitar archivos de claves a/desde el volumen

Esta función permite volver a cifrar el encabezado de un volumen con una clave de cifrado derivada de cualquier número de archivos de clave (con o sin contraseña), o de ningún archivo de clave. Por lo tanto, un volumen que solo se puede montar con contraseña puede convertirse en un volumen que requiere archivos de clave (además de la contraseña) para su montaje. Tenga en cuenta que el encabezado del volumen contiene la clave de cifrado maestra con la que se cifra el volumen. Por lo tanto, los datos almacenados en el volumen no se perderán después de usar esta función.

Esta función también se puede utilizar para cambiar o configurar archivos de claves de volumen (es decir, para eliminar algunos o todos los archivos de claves y aplicar otros nuevos).

Observación: Esta función es internamente igual a la función de cambio de contraseña.

Cuando VeraCrypt vuelve a cifrar un encabezado de volumen, el encabezado del volumen original se sobrescribe primero 256 veces con datos aleatorios para evitar que los adversarios utilicen técnicas como la microscopía de fuerza magnética o la microscopía de túnel de barrido de fuerza magnética [17] para recuperar el encabezado sobrescrito (sin embargo, consulte también el capítulo Requisitos y precauciones de seguridad).

Volúmenes > Eliminar todos los archivos de claves del volumen

Esta función permite volver a cifrar el encabezado de un volumen con una clave de cifrado derivada de una contraseña y sin archivos de claves (para que pueda montarse usando solo una contraseña, sin archivos de claves). Tenga en cuenta que el encabezado del volumen contiene la clave de cifrado maestra con la que se cifra el volumen. Por lo tanto, los datos almacenados en el volumen no se perderán después de usar esta función.

Observación: Esta función es internamente igual a la función de cambio de contraseña.

Cuando VeraCrypt vuelve a cifrar un encabezado de volumen, el encabezado del volumen original se sobrescribe primero 256 veces con datos aleatorios para evitar que los adversarios utilicen técnicas como la microscopía de fuerza magnética o la microscopía de túnel de barrido de fuerza magnética [17] para recuperar el encabezado sobrescrito (sin embargo, consulte también el capítulo Requisitos y precauciones de seguridad).

Herramientas > Generador de archivos de claves

Puede usar esta función para generar uno o más archivos con contenido aleatorio, que puede usar como archivo(s) de claves (recomendado). Esta función utiliza el generador de números aleatorios de VeraCrypt. Tenga en cuenta que, por defecto, solo se genera un archivo de clave y el tamaño del archivo resultante es de 64 bytes (es decir, 512 bits), que también es la longitud máxima posible de la contraseña de VeraCrypt. También es posible generar varios archivos y especificar su tamaño (ya sea un valor fijo para todos o dejar que VeraCrypt elija los tamaños de archivo aleatoriamente). En todos los casos, el tamaño del archivo debe estar comprendido entre 64 bytes y 1048576 bytes (que equivale a 1 MB, el número máximo de bytes de un archivo de clave procesado por VeraCrypt).

Configuración > Archivos de claves predeterminados

Utilice esta función para configurar los archivos de claves predeterminados o sus rutas de búsqueda. Esta función es especialmente útil si, por ejemplo, almacena archivos de claves en una memoria USB. Puede añadir la letra de unidad a la configuración predeterminada del archivo de claves. Para ello, haga clic en " Añadir ruta", busque la letra de unidad asignada a la memoria USB y haga clic en "Aceptar". Ahora, cada vez que monte un volumen (y si la opción "Usar archivos de claves" está marcada en el cuadro de diálogo de contraseña), VeraCrypt escaneará la ruta y usará todos los archivos que encuentre como archivos de claves.

ADVERTENCIA: Al agregar una carpeta (en lugar de un archivo) a su lista predeterminada de archivos de claves, solo se recuerda la ruta, no los nombres de archivo. Esto significa, por ejemplo, que si crea un nuevo archivo en la carpeta o copia un archivo adicional, no se podrán montar los volúmenes que usaron archivos de claves de la carpeta (hasta que elimine el archivo recién agregado).

IMPORTANTE: Tenga en cuenta que al configurar archivos de claves predeterminados o rutas de búsqueda predeterminadas, los nombres de archivo y las rutas se guardan sin cifrar en el archivo Default Keyfiles.xml. Para obtener más información, consulte el capítulo " Archivos de sistema y datos de aplicación de VeraCrypt".

Tokens de seguridad y tarjetas inteligentes

VeraCrypt admite tokens de seguridad (o criptográficos) y tarjetas inteligentes a los que se puede acceder mediante el protocolo PKCS #11 (2.0 o posterior) [23]. Para más información, consulte la sección " Tokens de seguridad y tarjetas inteligentes" en el capítulo "Archivos de claves".

Modo portátil

VeraCrypt puede ejecutarse en modo portátil, lo que significa que no necesita instalarse en el sistema operativo. Sin embargo, hay dos aspectos a tener en cuenta:

1) Necesita privilegios de administrador para poder ejecutar VeraCrypt en modo portátil (para conocer los motivos, consulte el capítulo Usar VeraCrypt sin privilegios de administrador).

> Nota: No importa qué tipo de software utilice, en lo que respecta a la privacidad personal en la mayoría de los casos, no es seguro trabajar con datos confidenciales en sistemas en los que no tiene privilegios de administrador, ya que el administrador puede capturar y copiar fácilmente sus datos confidenciales, incluidas contraseñas y claves.

2) Después de examinar el archivo de registro, es posible que se pueda determinar que VeraCrypt se ejecutó (y que se montó un volumen de VeraCrypt) en un sistema Windows incluso si se ejecutó en modo portátil.

Nota: Si esto es un problema, consulte esta pregunta. en las preguntas frecuentes para una posible solución.

Hay dos formas de ejecutar VeraCrypt en modo portátil:

1) Después de extraer los archivos del paquete autoextraíble de VeraCrypt, puede ejecutarlo directamente VeraCrypt.exe.

   Nota: Para extraer archivos del paquete autoextraíble de VeraCrypt, ejecútelo y luego seleccione Extraer (en lugar de Instalar) en la segunda página del asistente de configuración de VeraCrypt.

2) Puede utilizar la función de configuración del disco de viajero para preparar un disco de viajero especial y lanzarlo. VeraCrypt desde allí.

La segunda opción tiene varias ventajas, que se describen en las siguientes secciones de este capítulo.

Nota: Al ejecutarse en modo portátil, el controlador de VeraCrypt se descarga cuando ya no es necesario (por ejemplo, cuando se cierran todas las instancias de la aplicación principal o del Asistente para la creación de volúmenes y no hay volúmenes de VeraCrypt montados). Sin embargo, si fuerza el desmontaje de un volumen de VeraCrypt cuando este se ejecuta en modo portátil, o monta un volumen con formato NTFS grabable en Windows Vista o posterior, es posible que el controlador de VeraCrypt no se descargue al salir de VeraCrypt (solo se descargará al apagar o reiniciar el sistema). Esto evita diversos problemas causados por errores en Windows (por ejemplo, sería imposible reiniciar VeraCrypt mientras haya aplicaciones usando el volumen desmontado).

Herramientas > Configuración del disco Traveler

Puede usar esta función para preparar un disco de viaje especial e iniciar VeraCrypt desde allí. Tenga en cuenta que el disco de viaje de VeraCrypt no es un volumen de VeraCrypt, sino un volumen sin cifrar . Un disco de viaje contiene archivos ejecutables de VeraCrypt y, opcionalmente, el script "autorun.inf" (consulte la sección " Configuración de ejecución automática" más adelante). Tras seleccionar Herramientas > Configuración del disco de viaje, debería aparecer el cuadro de diálogo "Configuración del disco de viaje" . Algunos de los parámetros que se pueden configurar en el cuadro de diálogo requieren una explicación más detallada:

Incluir el Asistente de creación de volúmenes de VeraCrypt

Marque esta opción si necesita crear nuevos volúmenes de VeraCrypt con la ejecución de VeraCrypt desde el disco de viajero que creará. Desmarcar esta opción ahorra espacio en el disco de viajero.

Configuración de ejecución automática (autorun.inf)

En esta sección, puede configurar el disco de viaje para que inicie VeraCrypt automáticamente o monte un volumen específico de VeraCrypt al insertarlo. Esto se logra creando un archivo de script especial llamado "autorun.inf" en el disco de viaje. El sistema operativo ejecuta automáticamente este archivo cada vez que se inserta el disco de viaje.

Sin embargo, tenga en cuenta que esta función solo funciona con dispositivos de almacenamiento extraíbles como CD/DVD (se requiere Windows XP SP2, Windows Vista o una versión posterior de Windows para que funcione en memorias USB) y solo cuando está habilitada en el sistema operativo. Dependiendo de la configuración del sistema operativo, estas funciones de ejecución y montaje automáticos podrían funcionar solo cuando los archivos del disco de viaje se crean en un soporte no grabable similar a un CD/DVD (lo cual no es un error de VeraCrypt, sino una limitación de Windows).

Tenga en cuenta también que el archivo 'autorun.inf' debe estar en el directorio raíz (es decir, por ejemplo G:\, X:\ o Y:\, etc.) de un disco no cifrado para que esta característica funcione.

Soporte de TrueCrypt

A partir de la versión 1.0f, VeraCrypt permite cargar volúmenes y particiones TrueCrypt, tanto normales como ocultas. Para activar esta función, marque la opción "Modo TrueCrypt" en el cuadro de diálogo de solicitud de contraseña, como se muestra a continuación.

Nota: Solo se admiten volúmenes y particiones creados con las versiones 6.x y 7.x de TrueCrypt.

Conversión de volúmenes y particiones TrueCrypt

A partir de la versión 1.0f, los volúmenes TrueCrypt y las particiones que no son del sistema se pueden convertir al formato VeraCrypt mediante cualquiera de las siguientes acciones: • Cambiar la contraseña del volumen • Establecer el algoritmo de derivación de clave de encabezado • Agregar o quitar archivos de clave • Eliminar todos los archivos de clave

Se debe marcar el “Modo TrueCrypt” en el cuadro de diálogo como se muestra a continuación:

Nota: No se admite la conversión de particiones del sistema cifradas con TrueCrypt.

Parámetros de montaje predeterminados

A partir de la versión 1.0f-2, es posible especificar el algoritmo PRF y el modo TrueCrypt que se seleccionarán de forma predeterminada en el cuadro de diálogo de contraseña.

Como se muestra a continuación, seleccione la entrada "Parámetros de montaje predeterminados" en el menú "Configuración":

Se mostrará el siguiente cuadro de diálogo:

Realice sus modificaciones y luego haga clic en Aceptar.
Luego, los valores elegidos se escriben en el archivo de configuración principal de VeraCrypt (Configuration.xml), lo que los hace persistentes.

Todos los diálogos de solicitud de contraseña posteriores usarán los valores predeterminados previamente seleccionados. Por ejemplo, si en el diálogo "Parámetros de montaje predeterminados" marca "Modo TrueCrypt" y selecciona SHA-512 como PRF, los diálogos de solicitud de contraseña posteriores se verán así:

Nota: Los parámetros de montaje predeterminados se pueden anular mediante la línea de comandos Los conmutadores /tc y /hash siempre tienen prioridad.

Paquetes de idiomas

Los paquetes de idioma contienen traducciones de terceros de los textos de la interfaz de usuario de VeraCrypt. Nota que los paquetes de idiomas actualmente sólo son compatibles con la versión Windows de VeraCrypt.

Instalación

Desde la versión 1.0e, todos los paquetes de idioma están incluidos en el instalador de VeraCrypt para Windows y se encuentran en el directorio de instalación de VeraCrypt. Para seleccionar un nuevo idioma, ejecute VeraCrypt, seleccione Configuración > Idioma, seleccione su idioma y haga clic en Aceptar.

Para volver al inglés, seleccione Configuración > Idioma. Luego, seleccione Inglés y haga clic en Aceptar.

Todavía puedes descargar un archivo que contiene todos los paquetes de idiomas para la última versión (1.17) desde el siguiente enlace.

Algoritmos de cifrado

Los volúmenes de VeraCrypt se pueden cifrar utilizando los siguientes algoritmos:

Algoritmo	Diseñador(es)	Tamaño de la clave (bits)	Bloquear Tamaño (Brotes)	Modo de Operación
AES	J. Daemen, V. Rijmen	256	128	XTS
Camelia	Mitsubishi Electric y NTT de Japón	256	128	XTS
GOST89 (SBOX dinámico)	Norma Nacional de Rusia Federación GOST 28147-89 / GOST R 34.12-2015	256	64 (extendido a 128)	XTS
Kuznyechik	Norma Nacional de Rusia Federación GOST R 34.12-2015	256	128	XTS
Serpiente	Anderson R, Biham E, Knudsen L.	256	128	XTS
Dos peces	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpiente		256; 256; 256	128	XTS
Serpiente-AES		256; 256	128	XTS
Serpiente-Twofish-AES		256; 256; 256	128	XTS
Dos peces-serpiente		256; 256	128	XTS

Para obtener información sobre el modo XTS, consulte la sección Modos de operación.

AES

El estándar de cifrado avanzado (AES) especifica un algoritmo criptográfico aprobado por FIPS (Rijndael, diseñado por Joan Daemen y Vincent Rijmen, publicado en 1998) que puede ser utilizado por Los departamentos y agencias federales de EE. UU. protegerán criptográficamente la información confidencial [3]. VeraCrypt utiliza AES con 14 rondas y una clave de 256 bits (es decir, AES-256, publicada en 2001) operando en modo XTS (ver sección Modos de Operación).

En junio de 2003, después de que la NSA (Agencia de Seguridad Nacional de Estados Unidos) realizó una revisión y análisis de AES, el CNSS (Comité de Sistemas de Seguridad Nacional) de EE. UU. anunció en [1] que el diseño y la potencia de AES-256 (y AES-192) son suficientes para proteger la información clasificada hasta el Nivel de alto secreto. Esto se aplica a todos los departamentos o agencias del gobierno de EE. UU. que sean... considerando la adquisición o el uso de productos que incorporan el Estándar de Cifrado Avanzado (AES) para satisfacer los requisitos de garantía de la información asociados con la protección de la información nacional. sistemas de seguridad y/o información de seguridad nacional [1].

Serpiente

Diseñado por Ross Anderson, Eli Biham y Lars Knudsen; publicado en 1998. Utiliza una clave de 256 bits, un bloque de 128 bits y opera en modo XTS (véase la sección " Modos de Operación"). Serpent fue uno de los finalistas del AES. No fue seleccionado como el algoritmo AES propuesto, a pesar de que parecía tener un margen de seguridad mayor que el ganador, Rijndael [4]. Más concretamente, Serpent parecía tener un margen de seguridad alto , mientras que Rijndael parecía tener un margen de seguridad solo adecuado [4]. Rijndael también ha recibido críticas que sugieren que su estructura matemática podría dar lugar a ataques en el futuro [4].

En [5], el equipo de Twofish presenta una tabla de factores de seguridad para los finalistas de AES. El factor de seguridad se define como el número de rondas del cifrado completo dividido entre el mayor número de rondas descifradas. Por lo tanto, un cifrado descifrado tiene el factor de seguridad más bajo: 1. Serpent tuvo el factor de seguridad más alto de los finalistas de AES: 3,56 (para todos los tamaños de clave admitidos). Rijndael-256 tuvo un factor de seguridad de 1,56.

A pesar de estos hechos, Rijndael se consideró una opción adecuada para la AES por su combinación de seguridad, rendimiento, eficiencia, implementabilidad y flexibilidad [4]. En la última Conferencia de Candidatos de la AES, Rijndael obtuvo 86 votos, Serpent 59, Twofish 31, RC6 23 y MARS 13 [18, 19].*

Dos peces

Diseñado por Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall y Niels Ferguson; publicado en 1998. Utiliza una clave de 256 bits y un bloque de 128 bits, y opera en modo XTS (véase la sección " Modos de Operación"). Twofish fue uno de los finalistas de AES. Este cifrado utiliza cajas S dependientes de la clave. Twofish puede considerarse como un conjunto de dos cajas S de 128 bits derivadas de una 2^{128} diferentes criptosistemas, donde clave de 256 bits que controlan la selección del criptosistema [4]. En [13], el equipo de Twofish afirma que las cajas S dependientes de la clave constituyen una forma de margen de seguridad contra ataques desconocidos [4].

Camelia

Desarrollado conjuntamente por Mitsubishi Electric y NTT de Japón. Publicado por primera vez en el año 2000. Utiliza una clave de 256 bits y un bloque de 128 bits, y opera en modo XTS. Ha sido aprobado para su uso por la ISO/IEC, el proyecto NESSIE de la Unión Europea y el proyecto japonés CRYPTREC.

Kuznyechik

Kuznyechik es un cifrador de bloques publicado por primera vez en 2015 y definido en la Norma Nacional de la Federación Rusa GOST R 34.12-2015 y también en RFC 7801. Utiliza una clave de 256 bits y un bloque de 128 bits y funciona en modo XTS.

---

* Estos son votos positivos. Si se restan los votos negativos de los positivos, se obtienen los siguientes resultados: Rijndael: 76 votos, Serpent: 52 votos, Twofish: 10 votos, RC6: -14 votos, MARS: -70 votos [19].

GOST-89 (también conocido como Magma)

El cifrado por bloques GOST, definido en la norma GOST 28147-89, es un cifrado por bloques de clave simétrica, estándar de los gobiernos soviético y ruso. Desarrollado en la década de 1970, el estándar fue clasificado como "Alto Secreto" y posteriormente degradado a "Secreto" en 1990. Era una alternativa soviética al algoritmo estándar estadounidense, DES. Aún está presente en la última revisión de la norma GOST, GOST R 34.12-2015, bajo el nombre Magma. Utiliza una clave de 256 bits y un tamaño de bloque de 64 bits.
VeraCrypt utiliza una versión modificada, basada en ideas del proyecto GostCrypt, que utiliza SBOX dinámico en lugar del estático definido en el estándar GOST y que opera en bloques de 128 bits gracias a un esquema similar a CBC.

Cascadas de cifras

AES-Twofish

Dos cifrados en cascada [15, 16] que operan en modo XTS (ver la sección Modos de operación). Cada bloque de 128 bits se cifra primero con Twofish (clave de 256 bits) en modo XTS y, posteriormente, con AES (clave de 256 bits) en modo XTS. Cada cifrado en cascada utiliza su propia clave. Todas las claves de cifrado son independientes entre sí (tenga en cuenta que las claves de encabezado también lo son, aunque se deriven de una única contraseña; consulte Derivación de claves de encabezado, sal y número de iteraciones). Consulte más arriba para obtener información sobre cada cifrado en cascada.

AES-Twofish-Serpiente

Tres cifrados en cascada [15, 16] que operan en modo XTS (ver la sección Modos de operación). Cada bloque de 128 bits se cifra primero con Serpent (clave de 256 bits) en modo XTS, luego con Twofish (clave de 256 bits) en modo XTS y, finalmente, con AES (clave de 256 bits) en modo XTS. Cada cifrado en cascada utiliza su propia clave. Todas las claves de cifrado son independientes entre sí (tenga en cuenta que las claves de encabezado también lo son, aunque se deriven de una única contraseña; consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones"). Consulte más arriba para obtener información sobre cada cifrado en cascada.

Serpiente-AES

Dos cifrados en cascada [15, 16] que operan en modo XTS (ver la sección Modos de operación). Cada bloque de 128 bits se cifra primero con AES (clave de 256 bits) en modo XTS y, posteriormente, con Serpent (clave de 256 bits) en modo XTS. Cada cifrado en cascada utiliza su propia clave. Todas las claves de cifrado son independientes entre sí (tenga en cuenta que las claves de encabezado también lo son, aunque se deriven de una única contraseña; consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones"). Consulte más arriba para obtener información sobre cada cifrado en cascada.

Serpiente-Twofish-AES

Tres cifrados en cascada [15, 16] que operan en modo XTS (ver la sección Modos de operación). Cada bloque de 128 bits se cifra primero con AES (clave de 256 bits) en modo XTS, luego con Twofish (clave de 256 bits) en modo XTS y, finalmente, con Serpent (clave de 256 bits) en modo XTS. Cada cifrado en cascada utiliza su propia clave. Todas las claves de cifrado son independientes entre sí (tenga en cuenta que las claves de encabezado también lo son, aunque se deriven de una única contraseña; consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones"). Consulte más arriba para obtener información sobre cada cifrado en cascada.

Dos peces-serpiente

Dos cifrados en cascada [15, 16] que operan en modo XTS (ver la sección Modos de operación). Cada bloque de 128 bits se cifra primero con Serpent (clave de 256 bits) en modo XTS y luego con Twofish

(Clave de 256 bits) en modo XTS. Cada cifrado en cascada utiliza su propia clave. Todas las claves de cifrado son independientes entre sí (tenga en cuenta que las claves de encabezado también lo son, aunque se deriven de una única contraseña; consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones").
Consulte más arriba para obtener información sobre cada cifrado en cascada.

Algoritmos hash

En el Asistente de Creación de Volumen, en la ventana de diálogo de cambio de contraseña y en la ventana de diálogo del Generador de Archivos de Claves, puede seleccionar un algoritmo hash. El Generador de Números Aleatorios de VeraCrypt utiliza un algoritmo hash seleccionado por el usuario como función de "mezcla" pseudoaleatoria, y la función de derivación de clave de encabezado (HMAC basada en una función hash, como se especifica en PKCS #5 v2.0) también utiliza un algoritmo hash seleccionado por el usuario. Al crear un nuevo volumen, el Generador de Números Aleatorios genera la clave maestra, la clave secundaria (modo XTS) y la sal. Para obtener más información, consulte la sección " Generador de Números Aleatorios" y la sección " Derivación de clave de encabezado, sal y número de iteraciones".

RIPEMD-160

RIPEMD-160, publicado en 1996, es un algoritmo hash diseñado por Hans Dobbertin, Antoon Bosselaers y Bart Preneel en una comunidad académica abierta. El tamaño de salida de RIPEMD-160 es de 160 bits. RIPEMD-160 es una versión reforzada del algoritmo hash RIPEMD, desarrollado en el marco del proyecto RIPE (Evaluación de Primitivas de Integridad RACE) de la Unión Europea, 1988-1992. RIPEMD-160 fue adoptado por la Organización Internacional de Normalización (ISO) y la IEC en la norma internacional ISO/IEC 10118-3:2004 [21].

SHA-256

SHA-256 es un algoritmo hash diseñado por la NSA y publicado por el NIST en FIPS PUB 180-2 [14] en 2002 (el primer borrador se publicó en 2001). El tamaño de salida de este algoritmo es de 256 bits.

SHA-512

SHA-512 es un algoritmo hash diseñado por la NSA y publicado por el NIST en FIPS PUB 180-2 [14] en 2002 (el primer borrador se publicó en 2001). El tamaño de salida de este algoritmo es de 512 bits.

Torbellino

El algoritmo hash Whirlpool fue diseñado por Vincent Rijmen (codiseñador del algoritmo de cifrado AES) y Paulo SLM Barreto. El tamaño de salida de este algoritmo es de 512 bits. La primera versión de Whirlpool, ahora denominada Whirlpool-0, se publicó en noviembre de 2000. La segunda versión, ahora denominada Whirlpool-T, fue seleccionada para el portafolio de primitivas criptográficas NESSIE (Nuevos Esquemas Europeos de Firmas, Integridad y Cifrado) , un proyecto organizado por la Unión Europea similar a la competencia AES. VeraCrypt utiliza la tercera versión (final) de Whirlpool, adoptada por la Organización Internacional de Normalización (ISO) y la IEC en la norma internacional ISO/IEC 10118-3:2004 [21].

Streebog

Streebog es una familia de dos algoritmos hash, Streebog-256 y Streebog-512, definidos en el estándar nacional ruso GOST R 34.11-2012 Tecnologías de la Información - Seguridad de la Información Criptográfica - Función Hash. También se describe en la RFC 6986. Es competidor del estándar NIST SHA-3. VeraCrypt utiliza únicamente Streebog-512, que tiene un tamaño de salida de 512 bits.

Sistemas operativos compatibles

Nota: Tras el lanzamiento de esta versión de VeraCrypt, es posible que se haya publicado una nueva versión de un sistema operativo, cuya compatibilidad con VeraCrypt se haya verificado y añadido a la lista de sistemas compatibles. Por lo tanto, si esta es la última versión estable de VeraCrypt, le recomendamos consultar la versión en línea de este capítulo en https://veracrypt.codeplex.com/wikipage?title=Supported %20Operating%20Systems.

VeraCrypt actualmente es compatible con los siguientes sistemas operativos:

- Windows 10 •
  Windows 8 y 8.1 • Windows
  7 • Windows Vista
  • Windows XP •
  Windows Server
  2012 • Windows Server 2008 R2
  (64 bits) • Windows Server 2008 • Windows
  Server 2003

- Mac OS X 10.11 El Capitan • Mac OS
  X 10.10 Yosemite • Mac OS X 10.9
  Mavericks • Mac OS X 10.8 Mountain
  Lion • Mac OS X 10.7 Lion • Mac OS X
  10.6 Snow Leopard

- Linux x 8 6 (versiones de 32 bits y 64 bits, kernel 2.6 o compatible)

Nota: Los siguientes sistemas operativos (entre otros) no son compatibles: Windows RT, Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64 y las versiones Embedded/Tablet de Windows.

Consulte también la sección Sistemas operativos compatibles con el cifrado del sistema.

Uso de la línea de comandos

Tenga en cuenta que esta sección se aplica a la versión de Windows de VeraCrypt. Para obtener información sobre el comando
Para el uso de la línea que se aplica a las versiones de Linux y Mac OS X, ejecute: veracrypt –h

/ayuda o /?	Mostrar ayuda de la línea de comandos.
/truecrypt o /tc	Active el modo de compatibilidad TrueCrypt que permite montar volúmenes creados con las series TrueCrypt 6.x y 7.x.
/picadillo	Debe ir seguido de un parámetro que indique el algoritmo hash PRF a utilizar. Al montar el volumen, los valores posibles para el parámetro /hash son: sha256, sha-256, sha512, sha-512, whirlpool, ripemd160 y ripemd-160. Cuando se omite /hash, VeraCrypt probará todos los algoritmos PRF posibles, alargando así el tiempo de la operación de montaje.
/volumen o /v	Debe ir seguido de un parámetro que indique el nombre del archivo y la ruta de un volumen de VeraCrypt a montar (no utilizar al desmontar) o el ID del volumen del disco/partición a montar. La sintaxis del ID del volumen es ID:XXXXXX...XX donde la parte XX es una cadena de 64 caracteres hexadecimales que representa el ID de 32 bytes del volumen deseado para montar. Para montar una partición/volumen alojado en un dispositivo, utilice, por ejemplo, /v \Device\Harddisk1\Partition3 (para determinar la ruta a un partición/dispositivo, ejecute VeraCrypt y haga clic en Seleccionar dispositivo). También puede Montar una partición o un volumen dinámico usando su nombre de volumen (por ejemplo, ejemplo, /v \\?\Volumen{5cceb196-48bf-46ab-ad00-70965512253a}\). A Para determinar el nombre del volumen, use, por ejemplo, mountvol.exe. Tenga en cuenta también que Las rutas de los dispositivos distinguen entre mayúsculas y minúsculas. También puede especificar el ID del volumen. partición/volumen alojado en el dispositivo para montar, por ejemplo: /v Identificación:53B9A8D59CC84264004DA8728FC8F3E2EE6C130145ABD3835695C 29FD601EDCA. El valor de ID de volumen se puede recuperar mediante el volumen diálogo de propiedades.
/letra o /l	Debe ir seguido de un parámetro que indique la letra del controlador a montar. el volumen como. Cuando se omite /l y se usa /a, el primer volumen libre Se utiliza la letra de unidad.
/explorar o /e	Abra una ventana del Explorador después de haber montado un volumen.
/bip o /b	Emitirá un pitido después de que se haya montado o desmontado correctamente un volumen.
/auto o /a	Si no se especifica ningún parámetro, se monta automáticamente el volumen. Si los dispositivos... se especifica como parámetro (por ejemplo, /a dispositivos), montar automáticamente todos Volúmenes de VeraCrypt alojados en dispositivos o particiones actualmente accesibles. Si Se especifica favoritos como parámetro para montar automáticamente volúmenes favoritos. Tenga en cuenta que /auto está implícito si se especifican /quit y /volumen. Si Si necesita evitar que aparezca la ventana de la aplicación, utilice /quit.
/desmontar o /d	Desmontar el volumen especificado por la letra de unidad (p. ej., /dx). Cuando no hay unidad Si se especifica la letra, se desmontan todos los volúmenes de VeraCrypt montados actualmente.

/fuerza o /f	Fuerza el desmontaje (si el volumen que se va a desmontar contiene archivos que se están utilizado por el sistema o una aplicación) y fuerza el montaje en compartido modo (es decir, sin acceso exclusivo).
/archivo de claves o /k	Debe ir seguido de un parámetro que especifique un archivo de claves o un archivo de claves. Ruta de búsqueda. Para varios archivos de claves, especifique, por ejemplo: /k c:\keyfile1.dat /kd:\KeyfileFolder /kc:\kf2 A Para especificar un archivo de claves almacenado en un token de seguridad o una tarjeta inteligente, utilice el siguiente sintaxis: token://ranura/NÚMERO_DE_RANURA/archivo/NOMBRE_DE_ARCHIVO
/tryemptypass	SÓLO cuando se configura el archivo de clave predeterminado o cuando se especifica un archivo de clave en la línea de comando. Si va seguido de y o sí o si no se especifica ningún parámetro: intente montarlo usando una contraseña vacía y el archivo de claves antes de mostrar la solicitud de contraseña. Si va seguido de n o no: no intente montar utilizando una contraseña vacía y el archivo de claves, y muestre la solicitud de contraseña de inmediato.
/nowaitdlg	Si va seguido de y o sí o si no se especifica ningún parámetro: no mostrar el cuadro de diálogo de espera mientras se realizan operaciones como montar volúmenes. Si va seguido de n o no: fuerza la visualización del cuadro de diálogo de espera mientras se realizan operaciones.
/librita de tokens	Debe ir seguido de un parámetro que indique la biblioteca PKCS #11 que se utilizará para tokens de seguridad y tarjetas inteligentes (por ejemplo: /tokenlib c:\pkcs11lib.dll).
/ tokenpin	Debe ir seguido de un parámetro que indique el PIN a utilizar para autenticarse en el token de seguridad o tarjeta inteligente (por ejemplo: /tokenpin 0000).
/cache o /c	Si va seguido de y o sí o si no se especifica ningún parámetro: habilitar caché de contraseñas. Si va seguido de n o no: deshabilitar el caché de contraseñas (por ejemplo, /cn). Si va seguido de f o favoritos: contraseña de caché temporal al montar varios favoritos (por ejemplo, /cf). Tenga en cuenta que desactivar el caché de contraseñas no lo borrará (use /w para borrarlo). el caché de contraseñas).
/historia o /h	Si va seguido de y o ningún parámetro: habilita guardar el historial de los montados volúmenes; si va seguido de n: deshabilita el guardado del historial de volúmenes montados (por ejemplo, /hn).
/wipecache o /w	Borra cualquier contraseña almacenada en caché en la memoria del controlador.
/contraseña o /p	Debe ir seguido de un parámetro que indique la contraseña del volumen. Si el La contraseña contiene espacios, debe estar entre comillas. (p. ej., /p "Mi contraseña"). Use /p "" para especificar un espacio vacío contraseña. Advertencia: Este método para ingresar una contraseña de volumen puede ser inseguro, por ejemplo, cuando un símbolo del sistema no está cifrado El registro del historial se guarda en un disco sin cifrar.
/pim	Debe ir seguido de un número entero positivo que indique el PIM (Multiplicador de Iteraciones Personales) a utilizar para el volumen.
/salir o /q	Realizar automáticamente las acciones solicitadas y salir (VeraCrypt principal) La ventana no se mostrará). Si se especifican las preferencias como parámetro (por ejemplo,

/q preferencias), luego se cargan/guardan las configuraciones del programa y
Anular la configuración especificada en la línea de comando.
/q background inicia la tarea en segundo plano de VeraCrypt (icono de la bandeja)
a menos que esté deshabilitado en las Preferencias.

/silencio o /s

Si se especifica /q, se suprime la interacción con el usuario (avisos, errores)
mensajes, advertencias, etc.). Si no se especifica /q, esta opción no tiene
efecto.

/opción de montaje o /m

Debe ir seguido de un parámetro que puede tener uno de los valores que se indican a
continuación.

ro o readonly: monta el volumen como de solo lectura.

rm o extraíble: Montar el volumen como medio extraíble (ver sección
Volumen montado como medio extraíble).

ts o marca de tiempo: no conserva la marca de tiempo de modificación del contenedor.

sm o sistema: Sin autenticación previa al arranque, monte una partición que sea
dentro del alcance clave del cifrado del sistema (por ejemplo, una partición ubicada
en la unidad del sistema encriptada de otro sistema operativo que no es
en ejecución). Útil, por ejemplo, para operaciones de copia de seguridad o reparación.
Nota: Si proporciona una contraseña como parámetro de /p, asegúrese de que
La contraseña se ha escrito utilizando el diseño de teclado estándar de EE. UU. (en
Por el contrario, la GUI lo garantiza automáticamente). Esto es necesario debido a la
hecho de que la contraseña debe escribirse en el entorno de prearranque
(antes de que se inicie Windows) donde se utilizan distribuciones de teclado de Windows que no son de EE. UU.
No disponible.

bk o headerbak: monta el volumen utilizando el encabezado de respaldo incorporado.
Nota: Todos los volúmenes creados por VeraCrypt contienen una copia de seguridad incorporada
encabezado (ubicado al final del volumen).

recuperación: no verifique ninguna suma de comprobación almacenada en el encabezado del volumen.
Esta opción debe usarse solo cuando el encabezado del volumen esté dañado
y el volumen no se puede montar ni siquiera con la opción de montaje
encabezado atrás.

label=LabelValue: Usa el valor de cadena LabelValue como etiqueta del volumen montado en el
Explorador de Windows. La longitud máxima de LabelValue es de 32 caracteres para volúmenes
NTFS y de 11 caracteres para volúmenes FAT. Por ejemplo, /m label=MyDrive establecerá la
etiqueta de la unidad en el Explorador como MyDrive.

Ejemplo: /m ro

Tenga en cuenta que este modificador puede estar presente varias veces en la línea de comando para
especificar múltiples opciones de montaje (por ejemplo: /m rm /m ts)

VeraCrypt Format.exe (Asistente de creación de volúmenes de VeraCrypt):

/crear

Cree un volumen basado en contenedor en modo de línea de comandos. Debe ir seguido del
nombre del archivo del contenedor que se va a crear.

/tamaño

(Solo con /create)
Debe ir seguido de un parámetro que indique el tamaño del archivo contenedor que se creará.
Este parámetro es un número que indica el tamaño en bytes.
Puede tener un sufijo 'K', 'M', 'G' o 'T' para indicar que el valor está en Kilobytes,
Megabytes, Gigabytes o Terabytes respectivamente. Por ejemplo:

- /size 5000000: el tamaño del contenedor será de 5000000 bytes
- /size 25K: el tamaño del contenedor será de 25 KiloBytes.
- /size 100M: el tamaño del contenedor será de 100 MegaBytes.
- /size 2G: el tamaño del contenedor será de 2 GigaBytes.
- /size 1T: el tamaño del contenedor será de 1 TeraBytes.

/contraseña

(Solo con /create)
Debe ir seguido de un parámetro que indique la contraseña del contenedor que se creará.

/picadillo

(Solo con /create)
Debe ir seguido de un parámetro que indique el algoritmo hash PRF a utilizar.
Al crear el volumen. Tiene la misma sintaxis que VeraCrypt.exe.

/cifrado

(Solo con /create)
Debe ir seguido de un parámetro que indique el algoritmo de cifrado a utilizar. El valor predeterminado es AES si no se especifica esta opción. El parámetro puede tener los siguientes valores (sin distinguir entre mayúsculas y minúsculas): AES Serpent Twofish AES(Twofish)
AES(Twofish(Serpiente))
Serpiente (AES)
Serpiente(Twofish(AES))
Dos peces (serpiente)

/sistema de archivos

(Solo con /create)
Debe ir seguido de un parámetro que indique el sistema de archivos que se usará para el volumen.
El parámetro puede tener los siguientes valores: Ninguno: no usar ningún
sistema de archivos. FAT: formatear con
FAT/FAT32. NTFS: formatear con
NTFS. Tenga en cuenta que, en este caso, se mostrará un mensaje de control de cuentas de usuario (UAC).
se muestra a menos que el proceso se ejecute con privilegios administrativos completos.

/dinámica

(Solo con /create)
No tiene parámetros e indica que el volumen se creará como un volumen dinámico.

/fuerza

(Solo con /create)
No tiene parámetros e indica que se forzará la sobrescritura sin requerir confirmación del usuario.

/silencioso

(Solo con /create)
No tiene parámetros e indica que no se mostrará ningún cuadro de mensaje ni diálogo al usuario. Si se produce algún error, la operación fallará silenciosamente.

/noisocheck o /n

No verifique que los discos de rescate de VeraCrypt se hayan grabado correctamente. ADVERTENCIA: Nunca intente usar esta opción para reutilizar un disco de rescate VeraCrypt creado previamente. Tenga en cuenta que cada vez que cifre una partición o unidad del sistema, deberá crear un nuevo disco de rescate VeraCrypt, incluso si usa la misma contraseña. Un disco de rescate VeraCrypt creado previamente no se puede reutilizar, ya que se creó para una clave maestra diferente.

Sintaxis

VeraCrypt.exe [/tc] [/hash {sha256|sha-256|sha512|sha-512|whirlpool |ripemd160|
ripemd-160}][/a [dispositivos|favoritos]] [/b] [/c [y|n|f]] [/d [letra de unidad]] [/e] [/f] [/h [y|n]] [/k archivo de claves o ruta de
búsqueda] [tryemptypass [y|n]] [/l unidad
letra] [/m {bk|rm|recuperación|ro|sm|ts}] [/p contraseña] [/pim valor_pim] [/q [fondo|preferencias]] [/s] [/ruta_tokenlib]
[/v volumen] [/w]

"VeraCrypt Format.exe" [/n] [/crear] [/tamaño número[{K|M|G|T}]] [/p contraseña]
[/cifrado {AES|Serpent|Twofish|AES(Twofish)|AES(Twofish(Serpent))|Serpent(AES)|
Serpiente(Twofish(AES))|Twofish(Serpiente)}] [/hash {sha256|sha-256|sha512|sha-512|
whirlpool|ripemd160|ripemd-160}] [/sistema de archivos {Ninguno|FAT|NTFS}] [/dinámico] [/forzado] [/silencioso]

Tenga en cuenta que el orden en que se especifican las opciones no importa.

Ejemplos

Monte el volumen d:\myvolume como la primera letra de unidad libre, utilizando la solicitud de contraseña (la principal
La ventana del programa no se mostrará):

veracrypt /q /vd:\mivolumen

Desmontar un volumen montado con la letra de unidad X (no se mostrará la ventana principal del programa):

veracrypt /q /dx

Monte un volumen llamado myvolume.tc usando la contraseña MyPassword, como la letra de unidad X.
VeraCrypt abrirá una ventana del explorador y emitirá un pitido; el montaje será automático:

veracrypt /v mivolumen.tc /lx /a /p MiContraseña /e /b

Cree un contenedor de archivos de 10 MB utilizando la prueba de contraseña y formateado con FAT:

"C:\Archivos de programa\VeraCrypt\VeraCrypt Format.exe" /create c:\Data\test.hc /password test /hash sha512 /
encryption serpent /filesystem FAT /size 10M /force

Modelo de seguridad

> Nota para investigadores de seguridad: Si desea reportar un problema de seguridad o publicar un ataque a VeraCrypt, asegúrese de que no ignore el modelo de seguridad de VeraCrypt descrito a continuación. De ser así, el ataque (o el informe del problema de seguridad) se considerará inválido o falso.

VeraCrypt es un programa informático cuyos principales propósitos son:

- Proteja los datos cifrándolos antes de escribirlos en un disco.
- Descifre los datos cifrados después de leerlos desde el disco.

VeraCrypt no:

- Cifrar o proteger cualquier parte de la RAM (la memoria principal de una computadora).
- Proteger cualquier dato en una computadora* si un atacante tiene privilegios de administrador† bajo un sistema operativo instalado en la computadora.
- Asegure cualquier dato en una computadora si la computadora contiene malware (por ejemplo, un virus, un troyano, un spyware) o cualquier otro software (incluido VeraCrypt o un componente del sistema operativo) que haya sido alterado, creado o pueda ser controlado por un atacante.
- Asegure cualquier dato en una computadora si un atacante tiene acceso físico a la computadora antes o mientras VeraCrypt se esté ejecutando en él.
- Asegure cualquier dato en una computadora si un atacante tiene acceso físico a la computadora. Entre el momento en que se apaga VeraCrypt y el momento en que se borra o pierde de forma permanente e irreversible todo el contenido de todos los módulos de memoria volátil conectados al ordenador (incluidos los módulos de memoria de los dispositivos periféricos).
- Proteger los datos del ordenador si un atacante puede interceptar remotamente las emanaciones del hardware (p. ej., el monitor o los cables) mientras VeraCrypt se ejecuta (o supervisar remotamente el hardware y su uso, directa o indirectamente, mientras VeraCrypt se ejecuta).

- Proteger cualquier dato almacenado en un volumen VeraCrypt‡ si un atacante sin privilegios de administrador puede acceder al contenido del volumen montado (p. ej., si los permisos de archivo/carpeta/volumen no impiden que dicho atacante acceda a él).
- Preservar/verificar la integridad o autenticidad de los datos cifrados o descifrados.
- Evitar el análisis de tráfico cuando se transmiten datos cifrados a través de una red.
- Evitar que un atacante determine en qué sectores del volumen cambió el contenido (y cuándo y cuántas veces) si puede observar el volumen (desmontado o montado) antes y después de que se escriban datos en él, o si el medio/dispositivo de almacenamiento le permite al atacante determinar dicha información (por ejemplo, el volumen reside en un dispositivo que guarda metadatos que pueden usarse para determinar cuándo se escribieron datos en un sector en particular).

- Cifre cualquier dato no cifrado existente en el lugar (o vuelva a cifrar o borre los datos) en dispositivos o sistemas de archivos que utilizan nivelación de desgaste o que, de otro modo, reubican los datos internamente.
- Asegúrese de que los usuarios elijan contraseñas o archivos de claves criptográficamente seguros.

---

* En esta sección (Modelo de seguridad), la frase “datos en una computadora” significa datos en dispositivos/medios de almacenamiento internos y externos (incluidos dispositivos extraíbles y unidades de red) conectados a la computadora.

† En esta sección (Modelo de Seguridad), el término "privilegios de administrador" no se refiere necesariamente a una cuenta de administrador válida. También puede referirse a un atacante que no tiene una cuenta de administrador válida, pero que puede (por ejemplo, debido a una configuración incorrecta del sistema o al explotar una vulnerabilidad en el sistema operativo o una aplicación de terceros) realizar cualquier acción que solo un usuario con una cuenta de administrador válida normalmente puede realizar (por ejemplo, leer o modificar una parte arbitraria de una unidad o la RAM, etc.).

‡ “Volumen VeraCrypt” también significa una partición/unidad del sistema cifrada con VeraCrypt (consulte el capítulo Cifrado del sistema).

• Asegure cualquier componente de hardware de computadora o una computadora completa. •
Asegure cualquier dato en una computadora donde no se cumplan los requisitos o precauciones de seguridad enumerados en
No se siguen los requisitos y precauciones de seguridad del capítulo . • Realice alguna de las
acciones que se indican en la sección Limitaciones (capítulo Problemas y limitaciones conocidos).

En Windows, un usuario sin privilegios de administrador puede (suponiendo las configuraciones predeterminadas de VeraCrypt y del sistema operativo):

• Montar cualquier volumen de VeraCrypt alojado en archivos, siempre que se cumplan los permisos de archivo del contenedor.
Permítelo.
• Montar cualquier partición o volumen VeraCrypt alojado en un dispositivo. •
Completar el proceso de autenticación previa al arranque y, por lo tanto, obtener acceso a los datos en una partición o unidad
del sistema cifrada (e iniciar el sistema operativo cifrado). • Omitir el proceso de autenticación previa al arranque
(esto se puede evitar desactivando la opción " Configuración > Cifrado del sistema" > "Permitir que se omita la autenticación previa al arranque pulsando la tecla Esc"; tenga en cuenta que esta opción solo puede ser activada o desactivada por un administrador).

Desmontar, usando VeraCrypt, (y, en la ventana de la aplicación VeraCrypt, ver la ruta y las propiedades de) cualquier volumen VeraCrypt que haya montado. Sin embargo, esto no aplica a los "volúmenes favoritos del sistema", que puede desmontar, etc., independientemente de quién los haya montado (esto se puede evitar activando la opción Configuración > "Volúmenes favoritos del sistema" > "Permitir que solo los administradores vean y desmonten volúmenes favoritos del sistema en VeraCrypt"; tenga en cuenta que esta opción solo puede ser activada o desactivada por un administrador).

• Cree un volumen VeraCrypt alojado en archivos que contenga un sistema de archivos FAT o ningún sistema de archivos (siempre que el • Cambiar la contraseña, los archivos de claves y el
algoritmo de derivación de clave de encabezado para un volumen VeraCrypt alojado en archivos, y restaurar o hacer una copia de seguridad del encabezado de dicho volumen (siempre que los permisos de archivo lo permitan).

• Acceder al sistema de archivos que reside dentro de un volumen VeraCrypt montado por otro usuario en el sistema (sin embargo, se pueden configurar los permisos de archivo/carpeta/volumen para evitarlo). • Usar contraseñas (y archivos de claves
procesados) almacenados en la caché de contraseñas (tenga en cuenta que el almacenamiento en caché se puede deshabilitar; para obtener más información, consulte la sección Configuración > Preferencias, subsección Almacenar contraseñas en caché en la memoria del controlador).
• Ver las propiedades básicas (por ejemplo, el tamaño del área cifrada, el cifrado y el hash)
algoritmos utilizados, etc.) de la partición/unidad del sistema cifrado cuando se ejecuta el sistema cifrado.

• Ejecute y utilice la aplicación VeraCrypt (incluido el Asistente de creación de volumen VeraCrypt) siempre que el controlador del dispositivo VeraCrypt se esté ejecutando y los permisos de archivo lo permitan.

En Linux, un usuario sin privilegios de administrador puede (asumiendo las configuraciones predeterminadas de VeraCrypt y del sistema operativo):

• Cree un volumen VeraCrypt alojado en un archivo o en una partición/dispositivo que contenga un sistema de archivos FAT o ningún sistema de archivos, siempre que los permisos de la carpeta/dispositivo correspondiente lo permitan.
• Cambiar la contraseña, los archivos de claves y el algoritmo de derivación de claves de encabezado, y restaurar o
Realizar una copia de seguridad del encabezado de un volumen VeraCrypt alojado en un archivo o en una partición/dispositivo, siempre que los permisos del archivo/dispositivo lo
permitan. • Acceder al sistema de archivos que reside dentro de un volumen VeraCrypt montado por otro usuario en el sistema (sin embargo, se pueden configurar los permisos de archivo/carpeta/volumen para evitarlo). • Ejecutar y usar la
aplicación VeraCrypt (incluida la herramienta de creación de volúmenes VeraCrypt).
Asistente) siempre que los permisos del archivo lo permitan.
• En la ventana de la aplicación VeraCrypt, vea la ruta y las propiedades de cualquier aplicación VeraCrypt.
volumen montado por él o ella.

En Mac OS X, un usuario sin privilegios de administrador puede (asumiendo las configuraciones predeterminadas de VeraCrypt y del sistema operativo):

- Montar cualquier volumen de VeraCrypt alojado en archivos o particiones/dispositivos, siempre que Los permisos del archivo/dispositivo lo permiten.
- Desmontar, usando VeraCrypt, (y, en la ventana de la aplicación VeraCrypt, ver la ruta hacia y propiedades de) cualquier volumen VeraCrypt montado por él o ella. • Crear un volumen VeraCrypt alojado en un archivo o en una partición/dispositivo, siempre que el Los permisos de carpeta/dispositivo lo permiten.
- Cambiar la contraseña, los archivos de claves y el algoritmo de derivación de claves de encabezado, y restaurar o Realizar una copia de seguridad del encabezado de un volumen VeraCrypt alojado en un archivo o en una partición/dispositivo (siempre que los permisos del archivo/dispositivo lo permitan). Acceder al sistema de archivos que reside en un volumen VeraCrypt montado por otro usuario en el sistema (sin embargo, se pueden configurar los permisos de archivo/carpeta/volumen para evitarlo). Ejecutar y usar la aplicación VeraCrypt (incluido el Asistente para la creación de volúmenes VeraCrypt) siempre que los permisos del archivo lo permitan.

VeraCrypt no admite el modo de ejecución raíz set-euid.

Información adicional y detalles sobre el modelo de seguridad están contenidos en el capítulo Requisitos y precauciones de seguridad.

Requisitos y precauciones de seguridad

IMPORTANTE: Si desea utilizar VeraCrypt, debe seguir los requisitos de seguridad y las precauciones de seguridad que se enumeran en este capítulo.

Las secciones de este capítulo especifican los requisitos de seguridad para el uso de VeraCrypt y ofrecen información sobre los aspectos que afectan o limitan la capacidad de VeraCrypt para proteger los datos y proporcionar una denegación plausible. Aviso legal: No se garantiza que este capítulo contenga una lista de todos los problemas de seguridad y ataques que podrían afectar o limitar la capacidad de VeraCrypt para proteger los datos y proporcionar una denegación plausible.

Fugas de datos

Al montar un volumen VeraCrypt, el sistema operativo y las aplicaciones de terceros pueden escribir en volúmenes no cifrados (normalmente, en el volumen del sistema no cifrado) información no cifrada sobre los datos almacenados en el volumen VeraCrypt (p. ej., nombres de archivo y ubicaciones de archivos accedidos recientemente, bases de datos creadas por herramientas de indexación de archivos, etc.), o los propios datos sin cifrar (archivos temporales, etc.), o información no cifrada sobre el sistema de archivos que reside en el volumen VeraCrypt. Tenga en cuenta que Windows registra automáticamente grandes cantidades de datos potencialmente confidenciales, como los nombres y las ubicaciones de los archivos que abre, las aplicaciones que ejecuta, etc.

Además, a partir de Windows 8, cada vez que se monta un volumen VeraCrypt formateado con NTFS, se escribe un Evento 98 en el Registro de Eventos del sistema, que contendrá el nombre del dispositivo (\ \device\VeraCryptVolumeXX) del volumen. Esta función del registro de eventos se introdujo en Windows 8 como parte de las nuevas comprobaciones de estado de NTFS, como se explica aquí. Para evitar esta fuga, el volumen VeraCrypt debe montarse como un medio extraíble. Muchas gracias a Liran Elharar por descubrir esta fuga y su solución.

Para evitar fugas de datos, debes seguir estos pasos (pueden existir pasos alternativos):

- Si no necesita una negación plausible:
  - Cifre la partición/unidad del sistema (para obtener información sobre cómo hacerlo, consulte el capítulo Cifrado del sistema) y asegúrese de que solo se monten sistemas de archivos cifrados o de solo lectura durante cada sesión en la que trabaje con datos confidenciales.

    o,

  - Si no puede realizar lo anterior, descargue o cree una versión de "CD en vivo" de su sistema operativo (es decir, un sistema en vivo almacenado y arrancado completamente desde un CD/DVD) que garantice que cualquier dato escrito en el volumen del sistema se escriba en un disco RAM. Cuando necesite trabajar con datos confidenciales, arranque dicho CD/DVD en vivo y asegúrese de que solo se monten sistemas de archivos cifrados o de solo lectura durante la sesión.

- Si necesita una negación plausible:
  - Cree un sistema operativo oculto. VeraCrypt proporcionará protección automática contra fugas de datos. Para más información, consulte la sección "Sistema operativo oculto".

    o,

  - Si no puede hacer lo anterior, descargue o cree una versión de "CD en vivo" de su sistema operativo (es decir, un sistema "en vivo" completamente almacenado y arrancado desde un CD/DVD) que

Garantiza que todos los datos escritos en el volumen del sistema se escriban en un disco RAM. Si necesita trabajar con datos confidenciales, inicie un Live CD/DVD. Si utiliza volúmenes ocultos, siga los requisitos y precauciones de seguridad que se indican en la subsección " Requisitos y precauciones de seguridad para volúmenes ocultos". Si no utiliza volúmenes ocultos, asegúrese de que solo se monten durante la sesión volúmenes VeraCrypt alojados en particiones no del sistema o sistemas de archivos de solo lectura.

Archivo de paginación

Nota: El problema que se describe a continuación no le afecta si la partición del sistema o la unidad del sistema está cifrada (para obtener más información, consulte el capítulo Cifrado del sistema) y si todos los archivos de paginación están ubicados en una o más de las particiones dentro del alcance de la clave de cifrado del sistema, por ejemplo, en la partición donde está instalado Windows (para obtener más información, consulte el cuarto párrafo de esta subsección).

Windows utiliza los archivos de paginación, también llamados archivos de intercambio, para almacenar partes de programas y archivos de datos que no caben en la memoria. Esto significa que datos confidenciales, que cree que solo se almacenan en la RAM, pueden ser escritos sin cifrar en un disco duro por Windows sin que usted lo sepa.

Tenga en cuenta que VeraCrypt no puede evitar que el contenido de archivos confidenciales que se abren en RAM se guarden sin cifrar en un archivo de paginación (tenga en cuenta que cuando abre un archivo almacenado en un volumen de VeraCrypt, por ejemplo, en un editor de texto, el contenido del archivo se almacena sin cifrar en RAM).

Para evitar los problemas descritos anteriormente, cifre la partición o unidad del sistema (para obtener información sobre cómo hacerlo, consulte el capítulo Cifrado del sistema) y asegúrese de que todos los archivos de paginación se encuentren en una o más particiones dentro del alcance de la clave de cifrado del sistema (por ejemplo, en la partición donde está instalado Windows). Tenga en cuenta que esta última condición se cumple normalmente en Windows XP de forma predeterminada. Sin embargo, Windows Vista y versiones posteriores de Windows están configurados de forma predeterminada para crear archivos de paginación en cualquier volumen adecuado. Por lo tanto, antes de empezar a usar VeraCrypt, debe seguir estos pasos: Haga clic con el botón derecho en el icono de "Equipo" (o "Mi PC") en el escritorio o en el menú Inicio y, a continuación, seleccione Propiedades > (en Windows Vista o posterior: > Configuración avanzada del sistema >) pestaña Avanzadas > sección Rendimiento > Configuración > pestaña Avanzadas > sección Memoria virtual > Cambiar. En Windows Vista o posterior, desactive "Administrar automáticamente el tamaño del archivo de paginación para todas las unidades".

Asegúrese de que la lista de volúmenes disponibles para la creación de archivos de paginación contenga únicamente los volúmenes dentro del alcance de clave previsto para el cifrado del sistema (por ejemplo, el volumen donde está instalado Windows). Para deshabilitar la creación de archivos de paginación en un volumen específico, selecciónelo, seleccione "Sin archivo de paginación" y haga clic en " Establecer". Al finalizar, haga clic en Aceptar y reinicie el equipo.

Nota: También puedes considerar la creación de un sistema operativo oculto (para obtener más información, consulta la sección Sistema operativo oculto).

Archivos de volcado de memoria

Nota: El problema que se describe a continuación no le afecta si la partición del sistema o la unidad del sistema están cifradas (para obtener más información, consulte el capítulo Cifrado del sistema) y si el sistema está configurado para escribir archivos de volcado de memoria en la unidad del sistema (lo que suele ocurrir de manera predeterminada).

La mayoría de los sistemas operativos, incluido Windows, pueden configurarse para escribir la información de depuración y el contenido de la memoria del sistema en los llamados archivos de volcado de memoria (también llamados archivos de volcado de memoria) cuando se produce un error (bloqueo del sistema, pantallazo azul, comprobación de errores). Por lo tanto, estos archivos pueden contener datos confidenciales. VeraCrypt no puede evitar que las contraseñas en caché, las claves de cifrado ni el contenido de archivos confidenciales abiertos en la RAM se guarden sin cifrar en archivos de volcado de memoria.

Tenga en cuenta que al abrir un archivo almacenado en un volumen VeraCrypt, por ejemplo, en un editor de texto, el contenido del archivo se almacena sin cifrar en la RAM (y puede permanecer así hasta que se apague el ordenador). También tenga en cuenta que al montar un volumen VeraCrypt, su clave maestra es...

Se almacenan sin cifrar en la RAM. Por lo tanto, debe desactivar la generación de archivos de volcado de memoria en su equipo al menos en cada sesión en la que trabaje con datos confidenciales y monte un volumen VeraCrypt. Para ello, en Windows XP o posterior, haga clic con el botón derecho en el icono "Equipo" (o "Mi PC") en el escritorio o en el menú Inicio y, a continuación, seleccione Propiedades > (en Windows Vista o posterior: > Configuración avanzada del sistema >) pestaña Avanzadas > sección Inicio y recuperación > Configuración > sección Escribir información de depuración > seleccione (ninguno) > Aceptar.

Nota para los usuarios de Windows XP/2003: como Windows XP y Windows 2003 no proporcionan ninguna API para el cifrado de archivos de volcado de memoria, si la partición/unidad del sistema está cifrada por VeraCrypt y su sistema Windows XP está configurado para escribir archivos de volcado de memoria en la unidad del sistema, el controlador de VeraCrypt evita automáticamente que Windows escriba datos en los archivos de volcado de memoria.

Archivo de hibernación

Nota: El problema descrito a continuación no le afecta si la partición o unidad del sistema está cifrada* (para más información, consulte el capítulo Cifrado del sistema) y si el archivo de hibernación se encuentra en una de las particiones dentro del alcance de la clave de cifrado del sistema (que suele ser el predeterminado), por ejemplo, en la partición donde está instalado Windows. Cuando el equipo hiberna, los datos se cifran automáticamente antes de escribirse en el archivo de hibernación.

Cuando un ordenador entra en hibernación (o modo de ahorro de energía), el contenido de la memoria del sistema se guarda en un archivo de hibernación en el disco duro. Puede configurar VeraCrypt (Configuración > Preferencias > Desmontar todo al entrar en modo de ahorro de energía) para que desmonte automáticamente todos los volúmenes VeraCrypt montados, borre sus claves maestras almacenadas en la RAM y las contraseñas en caché (si las hay) antes de que el ordenador entre en hibernación (o modo de ahorro de energía).
Sin embargo, tenga en cuenta que si no utiliza el cifrado del sistema (consulte el capítulo Cifrado del sistema), VeraCrypt no podrá evitar de forma fiable que el contenido de archivos confidenciales abiertos en la RAM se guarde sin cifrar en un archivo de hibernación. Tenga en cuenta que al abrir un archivo almacenado en un volumen de VeraCrypt, por ejemplo, en un editor de texto, el contenido del archivo se almacena sin cifrar en la RAM (y puede permanecer así hasta que se apague el ordenador).

Tenga en cuenta que cuando Windows entra en modo de suspensión, puede estar configurado para entrar en el llamado modo de suspensión híbrida, que implica hibernación. También tenga en cuenta que el sistema operativo puede estar configurado para hibernar o entrar en el modo de suspensión híbrida al hacer clic o seleccionar "Apagar" (para más información, consulte la documentación de su sistema operativo).

Para evitar los problemas descritos anteriormente, cifre la partición/unidad del sistema (para obtener información sobre cómo hacerlo, consulte el capítulo Cifrado del sistema) y asegúrese de que el archivo de hibernación se encuentre en una de las particiones dentro del alcance de la clave de cifrado del sistema (que suele ser el predeterminado), por ejemplo, en la partición donde está instalado Windows. Cuando el equipo hiberna, los datos se cifran automáticamente antes de escribirse en el archivo de hibernación.

Nota: También puedes considerar la creación de un sistema operativo oculto (para obtener más información, consulta la sección Sistema operativo oculto).

Como alternativa, si no puede utilizar el cifrado del sistema, deshabilite o evite la hibernación en su computadora al menos para cada sesión durante la cual trabaje con datos confidenciales y durante la cual monte un volumen VeraCrypt.

---

* Descargo de responsabilidad: como Windows XP y Windows 2003 no proporcionan ninguna API para el cifrado de archivos de hibernación, VeraCrypt tiene que modificar componentes no documentados de Windows XP/2003 para permitir a los usuarios cifrar archivos de hibernación. Por lo tanto, VeraCrypt no puede garantizar que los archivos de hibernación de Windows XP/2003 siempre estén cifrados. En respuesta a nuestra queja pública sobre la falta de API, Microsoft comenzó a proporcionar una API pública para el cifrado de archivos de hibernación en Windows Vista y versiones posteriores. VeraCrypt ha utilizado esta API y, por lo tanto, puede cifrar archivos de hibernación de forma segura en Windows Vista y versiones posteriores. Por lo tanto, si utiliza Windows XP/2003 y desea que el archivo de hibernación esté cifrado de forma segura, le recomendamos encarecidamente que actualice a Windows Vista o posterior.

Datos sin cifrar en la RAM

Es importante tener en cuenta que VeraCrypt es un software de cifrado de discos , que cifra únicamente discos, no RAM (memoria).

Tenga en cuenta que la mayoría de los programas no borran el área de memoria (búferes) donde almacenan los archivos (partes de ellos) sin cifrar que cargan desde un volumen VeraCrypt. Esto significa que, al salir de un programa, los datos sin cifrar con los que trabajaba pueden permanecer en la memoria (RAM) hasta que se apague el ordenador (y, según algunos investigadores, incluso durante un tiempo después de apagarlo*). Tenga en cuenta también que si abre un archivo almacenado en un volumen VeraCrypt, por ejemplo, en un editor de texto y luego fuerza el desmontaje del volumen VeraCrypt, el archivo permanecerá sin cifrar en el área de memoria (RAM) utilizada por (asignada a) el editor de texto. Esto también aplica al desmontaje automático forzado.

Inherentemente, las claves maestras sin cifrar también deben almacenarse en la RAM. Al desmonta un volumen VeraCrypt que no pertenece al sistema, VeraCrypt borra sus claves maestras (almacenadas en la RAM). Al reiniciar o apagar el equipo correctamente, todos los volúmenes VeraCrypt que no pertenecen al sistema se desmontan automáticamente y, por lo tanto, el controlador de VeraCrypt borra todas las claves maestras almacenadas en la RAM (excepto las claves maestras para particiones/unidades del sistema; véase más adelante). Sin embargo, si se interrumpe bruscamente la alimentación, se reinicia el equipo (no se reinicia correctamente) o el sistema falla, VeraCrypt deja de funcionar de forma natural y, por lo tanto, no puede borrar ninguna clave ni ningún otro dato confidencial. Además, dado que Microsoft no proporciona ninguna API adecuada para gestionar la hibernación y el apagado, las claves maestras utilizadas para el cifrado del sistema no se pueden borrar de la RAM de forma fiable cuando el equipo hiberna, se apaga o se reinicia.†

> En resumen, VeraCrypt no puede garantizar que la RAM no contenga datos confidenciales (p. ej., contraseñas, claves maestras o datos descifrados). Por lo tanto, después de cada sesión en la que trabaje con un volumen de VeraCrypt o en la que se ejecute un sistema operativo cifrado, debe apagar (o, si el archivo de hibernación está cifrado, hibernar) el ordenador y dejarlo apagado durante al menos varios minutos (cuanto más tiempo, mejor) antes de volver a encenderlo. Esto es necesario para borrar la RAM (consulte también la sección Archivo de hibernación).

Seguridad física

Si un atacante puede acceder físicamente al hardware de la computadora y usted lo usa después de que el atacante haya accedido físicamente a él, entonces VeraCrypt puede volverse incapaz de proteger los datos en la computadora.‡ Esto se debe a que el atacante puede modificar el hardware o adjuntarle un componente de hardware malicioso (como un registrador de pulsaciones de teclas de hardware) que capturará la contraseña o la clave de cifrado (por ejemplo, cuando monta un volumen de VeraCrypt) o comprometerá de otra manera la seguridad de la computadora.
Por lo tanto, no debes usar VeraCrypt en una computadora a la que un atacante haya accedido físicamente.

---

* Supuestamente, entre 1,5 y 35 segundos a temperaturas normales de funcionamiento (26-44 °C) y hasta varias horas cuando los módulos de memoria se enfrían (con el ordenador en funcionamiento) a temperaturas muy bajas (p. ej., -50 °C). Los nuevos tipos de módulos de memoria supuestamente presentan un tiempo de decaimiento mucho menor (p. ej., entre 1,5 y 2,5 segundos) que los modelos más antiguos (a partir de 2008). †

Antes de borrar una clave de la RAM, es necesario desmontar el volumen VeraCrypt correspondiente. Para volúmenes que no pertenecen al sistema, esto no causa ningún problema. Sin embargo, dado que Microsoft actualmente no proporciona ninguna API adecuada para gestionar la fase final del proceso de apagado del sistema, los archivos de paginación ubicados en volúmenes del sistema cifrados que se desmontan durante el proceso de apagado aún pueden contener páginas de memoria intercambiadas válidas (incluyendo partes de archivos del sistema de Windows). Esto podría causar errores de pantalla azul. Por lo tanto, para evitarlos, VeraCrypt no desmonta los volúmenes del sistema cifrados y, en consecuencia, no puede borrar las claves maestras de los volúmenes del sistema al apagar o reiniciar el sistema.

‡ En esta sección (Seguridad física), la frase “datos en la computadora” significa datos en dispositivos/medios de almacenamiento internos y externos (incluidos dispositivos extraíbles y unidades de red) conectados a la computadora.

Además, debe asegurarse de que VeraCrypt (incluido su controlador de dispositivo) no se esté ejecutando cuando el atacante acceda físicamente al equipo. Para más información sobre ataques de hardware con acceso físico directo, consulte la sección " Datos sin cifrar en la RAM".

Además, incluso si el atacante no puede acceder físicamente al hardware del ordenador directamente, podría vulnerar su seguridad física interceptando y analizando remotamente las emanaciones del hardware (incluidos el monitor y los cables). Por ejemplo, las emanaciones interceptadas del cable que conecta el teclado al ordenador pueden revelar las contraseñas que se escriben. Este documento no aborda todos los tipos de ataques de este tipo (a veces llamados ataques TEMPEST) ni las formas conocidas de prevenirlos (como el blindaje o la interferencia de radio). Es su responsabilidad prevenir estos ataques. Si no lo hace, VeraCrypt podría no poder proteger los datos del ordenador.

Malware

El término "malware" se refiere colectivamente a todo tipo de software malicioso, como virus informáticos, troyanos, spyware o, en general, cualquier pieza de software (incluido VeraCrypt o un componente del sistema operativo) que haya sido alterado, preparado o pueda ser controlado por un atacante. Algunos tipos de malware están diseñados, por ejemplo, para registrar las pulsaciones de teclas, incluidas las contraseñas introducidas (estas contraseñas capturadas se envían al atacante por internet o se guardan en una unidad local sin cifrar, desde la cual el atacante podría leerlas posteriormente, al acceder físicamente al ordenador). Si utiliza VeraCrypt en un ordenador infectado con cualquier tipo de malware, es posible que VeraCrypt no pueda proteger los datos del ordenador.* Por lo tanto, no debe utilizar VeraCrypt en dicho ordenador.

Es importante tener en cuenta que VeraCrypt es un software de cifrado, no un software antimalware. Es su responsabilidad evitar que el malware se ejecute en su computadora. Si no lo hace, VeraCrypt podría no poder proteger los datos en su computadora.

Hay muchas reglas que debe seguir para evitar que el malware se ejecute en su computadora. Entre las más importantes se encuentran las siguientes: Mantenga actualizado su sistema operativo, navegador de Internet y demás software crítico. En Windows XP o posterior, active DEP para todos los programas.† No abra archivos adjuntos sospechosos en correos electrónicos, especialmente archivos ejecutables, incluso si parecen haber sido enviados por familiares o amigos (sus computadoras podrían estar infectadas con malware que envía correos electrónicos maliciosos desde sus computadoras/cuentas sin su conocimiento). No siga enlaces sospechosos contenidos en correos electrónicos o sitios web (incluso si el correo electrónico/sitio web parece inofensivo o confiable). No visite sitios web sospechosos. No descargue ni instale software sospechoso. Considere usar un software antimalware confiable y de buena calidad.

Entorno multiusuario

Tenga en cuenta que el contenido de un volumen VeraCrypt montado es visible (accesible) para todos los usuarios conectados. Se pueden configurar los permisos de archivos/carpetas NTFS para evitar esto, a menos que el volumen esté montado como medio extraíble (consulte la sección " Volumen montado como medio extraíble") en una edición de escritorio de Windows Vista o posterior (los sectores de un volumen montado como medio extraíble pueden ser accesibles).

*En esta sección (Malware), la frase “datos en la computadora” significa datos en dispositivos/medios de almacenamiento internos y externos (incluidos dispositivos extraíbles y unidades de red) conectados a la computadora.

† DEP significa Prevención de Ejecución de Datos. Para más información sobre DEP, visite http://support.microsoft.com/kb/875352, http://technet.microsoft.com/en-us/library/cc700810.aspx, y http://windows.microsoft.com/es-US/windows-vista/What-is-Data-Execution-Prevention.

a nivel de volumen para usuarios sin privilegios de administrador, independientemente de si es accesible para ellos a nivel del sistema de archivos).

Además, en Windows, la caché de contraseñas es compartida por todos los usuarios conectados (para obtener más información, consulte la sección Configuración > Preferencias, subsección Almacenar contraseñas en caché en el controlador). memoria).

Tenga en cuenta también que cambiar de usuario en Windows XP o posterior (funcionalidad de cambio rápido de usuario) no desmonta un volumen de VeraCrypt montado correctamente (a diferencia del reinicio del sistema, que desmonta todos los volúmenes de VeraCrypt montados).

En Windows 2000, los permisos del archivo contenedor se ignoran al montar un volumen VeraCrypt alojado en archivos. En todas las versiones compatibles de Windows, los usuarios sin privilegios de administrador pueden montar cualquier volumen VeraCrypt alojado en una partición o dispositivo (siempre que proporcionen la contraseña o los archivos de claves correctos). Un usuario sin privilegios de administrador solo puede desmontar los volúmenes que haya montado. Sin embargo, esto no aplica a los volúmenes favoritos del sistema a menos que active la opción (desactivada por defecto) en Configuración > Volúmenes favoritos del sistema > Permitir que solo los administradores vean y desmonten los volúmenes favoritos del sistema en VeraCrypt.

Autenticidad e integridad

VeraCrypt utiliza cifrado para preservar la confidencialidad de los datos que cifra. VeraCrypt no preserva ni verifica la integridad ni la autenticidad de los datos que cifra o descifra. Por lo tanto, si permite que un adversario modifique los datos cifrados por VeraCrypt, este podrá establecer el valor de cualquier bloque de 16 bytes en un valor aleatorio o en un valor anterior que haya obtenido anteriormente. Tenga en cuenta que el adversario no puede elegir el valor que obtendrá cuando VeraCrypt descifre el bloque modificado (el valor será aleatorio) a menos que el atacante restaure una versión anterior del bloque cifrado que haya obtenido anteriormente. Es su responsabilidad verificar la integridad y la autenticidad de los datos cifrados o descifrados por VeraCrypt (por ejemplo, mediante el uso de software de terceros adecuado).

Ver también: Seguridad física, Modelo de seguridad

Elección de contraseñas y archivos de claves

Es muy importante que elijas una buena contraseña. Debes evitar elegir una que contenga solo una palabra que se pueda encontrar en un diccionario (o una combinación de ellas). No debe contener nombres, fechas de nacimiento, números de cuenta ni ningún otro elemento fácil de adivinar. Una buena contraseña es una combinación aleatoria de mayúsculas y minúsculas, números y caracteres especiales como @, ^ y +. Recomendamos encarecidamente elegir una contraseña de más caracteres (cuanto más larga, mejor). Las contraseñas cortas son fáciles de descifrar mediante ataques de fuerza bruta.

Para que los ataques de fuerza bruta a un archivo de claves sean inviables, este debe tener al menos 30 bytes de tamaño. Si un volumen utiliza varios archivos de claves, al menos uno de ellos debe tener 30 bytes o más. Tenga en cuenta que el límite de 30 bytes supone una gran cantidad de entropía en el archivo de claves. Si los primeros 1024 kilobytes de un archivo contienen poca entropía, no debe utilizarse como archivo de claves (independientemente de su tamaño). Si no está seguro de qué significa entropía, le recomendamos que permita que VeraCrypt genere un archivo con contenido aleatorio y lo utilice como archivo de claves (seleccione Herramientas > Generador de archivos de claves).

Al crear un volumen, cifrar una partición o unidad del sistema, o cambiar contraseñas o archivos de claves, no debe permitir que terceros elijan o modifiquen las contraseñas o los archivos de claves antes o durante la creación o el cambio del volumen. Por ejemplo, no debe usar generadores de contraseñas (ya sean aplicaciones web o programas locales) si no está seguro de su alta calidad y de que no estén controlados por un atacante. Los archivos de claves no deben ser archivos descargados de internet ni accesibles para otros usuarios del equipo (sean o no administradores).

Cambiar contraseñas y archivos de claves

Tenga en cuenta que el encabezado del volumen (cifrado con una clave derivada de una contraseña o archivo de claves) contiene la clave maestra (no confundir con la contraseña) con la que se cifra el volumen. Si un atacante puede hacer una copia de su volumen antes de que usted cambie la contraseña o los archivos de claves, podría usar su copia o fragmento (el encabezado antiguo) del volumen VeraCrypt para montarlo usando una contraseña o archivos de claves comprometidos, necesarios para montar el volumen antes de que usted cambiara la contraseña o los archivos de claves.

Si no está seguro de si un adversario conoce su contraseña (o tiene sus archivos de claves) y si tiene una copia de su volumen cuando necesita cambiar su contraseña y/o archivos de claves, se recomienda encarecidamente que cree un nuevo volumen de VeraCrypt y mueva los archivos del volumen antiguo al nuevo volumen (el nuevo volumen tendrá una clave maestra diferente).

Tenga en cuenta también que si un adversario conoce su contraseña (o tiene sus archivos de claves) y tiene acceso a su volumen, podría recuperar y conservar su clave maestra. De ser así, podría descifrar su volumen incluso después de cambiar la contraseña o los archivos de claves (ya que la clave maestra no cambia al cambiar la contraseña o los archivos de claves del volumen). En tal caso, cree un nuevo volumen VeraCrypt y transfiera todos los archivos del volumen anterior al nuevo.

Las siguientes secciones de este capítulo contienen información adicional relacionada con posibles problemas de seguridad relacionados con el cambio de contraseñas y/o archivos de claves:

- Requisitos y precauciones de seguridad
- Registro de sistemas de archivos
- Desfragmentación
- Sectores reasignados

Operación de recorte

Algunos dispositivos de almacenamiento (p. ej., algunas unidades de estado sólido, incluidas las unidades flash USB) utilizan la llamada operación de recorte para marcar los sectores de la unidad como libres, por ejemplo, al eliminar un archivo. En consecuencia, dichos sectores pueden contener ceros sin cifrar u otros datos indefinidos (sin cifrar), incluso si se encuentran dentro de una parte de la unidad cifrada por VeraCrypt. VeraCrypt no bloquea la operación de recorte en particiones que se encuentran dentro del alcance de la clave de cifrado del sistema (véase el capítulo Cifrado del sistema) (a menos que se esté ejecutando un sistema operativo oculto; véase la sección Sistema operativo oculto) ni en Linux en todos los volúmenes que utilizan los servicios criptográficos nativos del kernel de Linux. En esos casos, el adversario podrá identificar qué sectores contienen espacio libre (y podría utilizar esta información para análisis y ataques posteriores) y la negación plausible (véase el capítulo Negación plausible) podría verse afectada negativamente. Para evitar estos problemas, no utilice el cifrado del sistema en unidades que utilicen la operación de recorte y, en Linux, configure VeraCrypt para que no...

Utilice los servicios criptográficos del kernel nativo de Linux o asegúrese de que los volúmenes VeraCrypt no estén ubicados en unidades que utilicen la operación de recorte.

Para saber si un dispositivo utiliza la operación de recorte, consulte la documentación suministrada con el dispositivo o comuníquese con el proveedor/fabricante.

Nivelación del desgaste

Algunos dispositivos de almacenamiento (p. ej., algunas unidades de estado sólido, incluidas las memorias USB) y algunos sistemas de archivos utilizan mecanismos de nivelación de desgaste para prolongar la vida útil del dispositivo o medio de almacenamiento. Estos mecanismos garantizan que, incluso si una aplicación escribe datos repetidamente en el mismo sector lógico, estos se distribuyan uniformemente en el medio (los sectores lógicos se reasignan a diferentes sectores físicos). Por lo tanto, un atacante podría tener acceso a múltiples versiones de un mismo sector. Esto puede tener diversas implicaciones de seguridad. Por ejemplo, al cambiar la contraseña o los archivos de claves de un volumen, el encabezado del volumen se sobrescribe, en condiciones normales, con una versión reencriptada. Sin embargo, cuando el volumen reside en un dispositivo que utiliza un mecanismo de nivelación de desgaste, VeraCrypt no puede garantizar que el encabezado anterior se sobrescriba realmente. Si un adversario encontrara el encabezado del volumen antiguo (que debía sobrescribirse) en el dispositivo, podría usarlo para montarlo usando una contraseña antigua comprometida (o usando archivos de clave comprometidos necesarios para montar el volumen antes de volver a cifrar el encabezado). Por razones de seguridad, recomendamos no crear ni almacenar volúmenes VeraCrypt en dispositivos (o sistemas de archivos) que utilicen un mecanismo de nivelación de desgaste (y no usar VeraCrypt para cifrar ninguna parte de dichos dispositivos o sistemas de archivos).

Si decide no seguir esta recomendación y pretende usar cifrado local en una unidad que utiliza mecanismos de nivelación de desgaste, asegúrese de que la partición/unidad no contenga datos confidenciales antes de cifrarla por completo (VeraCrypt no puede realizar un cifrado local seguro de forma fiable para los datos existentes en dicha unidad; sin embargo, una vez cifrada por completo la partición/unidad, cualquier dato nuevo que se guarde se cifrará de forma fiable sobre la marcha). Esto incluye las siguientes precauciones: Antes de ejecutar VeraCrypt para configurar la autenticación previa al arranque, desactive los archivos de paginación y reinicie el sistema operativo (puede activarlos después de que la partición/unidad del sistema se haya cifrado por completo). Debe evitar la hibernación durante el periodo entre el momento en que inicia VeraCrypt para configurar la autenticación previa al arranque y el momento en que la partición/unidad del sistema se ha cifrado por completo. Sin embargo, tenga en cuenta que, incluso si sigue estos pasos, no se garantiza que evitará fugas de datos ni que los datos confidenciales del dispositivo se cifrarán de forma segura. Para obtener más información, consulte las secciones Fugas de datos, Archivo de paginación, Archivo de hibernación y Archivo de hibernación.

Si necesita una negación plausible, no debe usar VeraCrypt para cifrar ninguna parte de (o crear contenedores cifrados en) un dispositivo (o sistema de archivos) que utilice un mecanismo de nivelación de desgaste.

Para saber si un dispositivo utiliza un mecanismo de nivelación de desgaste, consulte la documentación suministrada con el dispositivo o comuníquese con el proveedor/fabricante.

Sectores reasignados

Algunos dispositivos de almacenamiento, como los discos duros, reasignan o reasignan internamente los sectores defectuosos. Cuando el dispositivo detecta un sector donde no se pueden escribir datos, lo marca como defectuoso y lo reasigna a un sector en un área reservada oculta de la unidad. Cualquier operación de lectura o escritura posterior desde o hacia el sector defectuoso se redirige al sector del área reservada. Esto significa que los datos existentes en el sector defectuoso permanecen en la unidad y no se pueden borrar (sobrescribir con otros datos). Esto puede

Esto tiene diversas implicaciones de seguridad. Por ejemplo, los datos que se cifrarán en el lugar podrían permanecer sin cifrar en el sector defectuoso. Asimismo, los datos que se borrarán (por ejemplo, durante la creación de un sistema operativo oculto) podrían permanecer en el sector defectuoso. La negación plausible (véase la sección "Negación plausible") podría verse afectada negativamente al reasignar un sector.

En la sección "Requisitos y precauciones de seguridad" se incluyen ejemplos adicionales de posibles implicaciones de seguridad . Tenga en cuenta que esta lista no es exhaustiva (son solo ejemplos). Tenga en cuenta también que VeraCrypt no puede evitar ningún problema de seguridad relacionado o causado por los sectores reasignados. Para averiguar el número de sectores reasignados en un disco duro, puede utilizar, por ejemplo, una herramienta de software de terceros para leer los llamados datos SMART.

Desfragmentando

Al desfragmentar el sistema de archivos donde se almacena un contenedor VeraCrypt alojado en archivos, es posible que quede una copia del contenedor VeraCrypt (o de su fragmento) en el espacio libre del volumen host (en el sistema de archivos desfragmentado). Esto puede tener diversas implicaciones de seguridad. Por ejemplo, si cambia la contraseña o los archivos de clave del volumen posteriormente, y un atacante encuentra la copia o el fragmento antiguo (el encabezado antiguo) del volumen VeraCrypt, podría usarlo para montar el volumen con una contraseña antigua comprometida (o con los archivos de clave comprometidos necesarios para montar el volumen antes de que se volviera a cifrar el encabezado del volumen). Para evitar este y otros posibles problemas de seguridad (como los mencionados en la sección " Clones de volumen"), realice una de las siguientes acciones:

- Utilice un volumen VeraCrypt alojado en una partición o dispositivo en lugar de uno alojado en archivos.
- Borre de forma segura el espacio libre en el volumen del host (en el sistema de archivos desfragmentado) después desfragmentando.
- No desfragmente los sistemas de archivos en los que almacena volúmenes de VeraCrypt.

Registro de sistemas de archivos

Cuando un contenedor VeraCrypt alojado en archivos se almacena en un sistema de archivos con registro en diario (como NTFS), una copia del contenedor VeraCrypt (o de su fragmento) puede permanecer en el espacio libre del volumen del host.

Esto puede tener diversas implicaciones de seguridad. Por ejemplo, si cambia la contraseña o los archivos de claves del volumen y un adversario encuentra la copia o el fragmento antiguo (el encabezado antiguo) del volumen VeraCrypt, podría usarlo para montar el volumen con una contraseña antigua comprometida (o con archivos de claves comprometidos que eran necesarios para montar el volumen antes de que se volviera a cifrar el encabezado del volumen). Algunos sistemas de archivos con registro en diario también registran internamente los tiempos de acceso a los archivos y otra información potencialmente confidencial. Si necesita una denegación plausible (consulte la sección Denegación plausible), no debe almacenar contenedores VeraCrypt alojados en sistemas de archivos con registro en diario. Para evitar posibles problemas de seguridad relacionados con los sistemas de archivos con registro en diario, realice una de las siguientes acciones:

- Utilice un volumen VeraCrypt alojado en una partición o dispositivo en lugar de uno alojado en archivos.
- Almacene el contenedor en un sistema de archivos sin registro (por ejemplo, FAT32).

Clones de volumen

Nunca cree un nuevo volumen VeraCrypt clonando un volumen VeraCrypt existente. Utilice siempre el Asistente para la creación de volúmenes de VeraCrypt para crear un nuevo volumen de VeraCrypt. Si clona un volumen y... Luego comience a usar tanto este volumen como su clon de manera que ambos contengan datos diferentes. Entonces podrías ayudar al criptoanálisis (ambos volúmenes compartirán un único conjunto de claves). Esto es especialmente... crítico cuando el volumen contiene un volumen oculto. Tenga en cuenta también que la negación plausible (véase La sección "Negación plausible" es imposible en estos casos. Consulte también el capítulo " Cómo realizar copias de seguridad de forma segura".

Requisitos y precauciones de seguridad adicionales

Además de los requisitos y precauciones descritos en este capítulo (Requisitos de seguridad) y Precauciones), debe seguir y tener en cuenta los requisitos de seguridad, precauciones y limitaciones enumeradas en los siguientes capítulos y secciones:

- Cómo realizar copias de seguridad de forma segura
- Limitaciones
- Modelo de seguridad •
Requisitos de seguridad y precauciones relacionadas con los volúmenes ocultos
- Negación plausible

Ver también: Firmas digitales

Cómo realizar copias de seguridad de forma segura

Debido a errores o fallos de hardware o software, los archivos almacenados en un volumen VeraCrypt pueden corromperse. Por lo tanto, le recomendamos encarecidamente que realice copias de seguridad de todos sus archivos importantes con regularidad (esto aplica a cualquier dato importante, no solo a los datos cifrados almacenados en volúmenes VeraCrypt).

Volúmenes que no son del sistema

Para realizar una copia de seguridad segura de un volumen VeraCrypt que no sea del sistema, se recomienda seguir estos pasos:

1. Cree un nuevo volumen VeraCrypt utilizando el Asistente de creación de volumen VeraCrypt (no Habilite la opción Formato rápido o Dinámico). Será su volumen de respaldo , por lo que su tamaño debe ser igual o mayor que el de su volumen principal .

   Si el volumen principal es un volumen VeraCrypt oculto (consulte la sección "Volumen oculto"), el volumen de copia de seguridad también debe serlo. Antes de crear el volumen de copia de seguridad oculto , debe crear un nuevo volumen host (externo) para él sin habilitar la opción de formato rápido . Además, especialmente si el volumen de copia de seguridad está alojado en archivos, el volumen de copia de seguridad oculto debe ocupar solo una pequeña parte del contenedor y el volumen externo debe estar casi completamente lleno de archivos (de lo contrario, la posibilidad de denegación del volumen oculto podría verse afectada).

2. Monte el volumen de respaldo recién creado .

3. Monte el volumen principal .

4. Copie todos los archivos del volumen principal montado directamente al volumen de respaldo montado .

IMPORTANTE: Si almacena el volumen de respaldo en cualquier ubicación a la que un adversario puede acceder repetidamente (por ejemplo, en un dispositivo guardado en la caja de seguridad de un banco), debe repetir todos los pasos anteriores (incluido el paso 1) cada vez que desee realizar una copia de seguridad del volumen (ver a continuación).

Si sigue los pasos anteriores, ayudará a evitar que los adversarios se enteren:

- Qué sectores de los volúmenes están cambiando (ya que siempre se sigue el paso 1). Esto es especialmente importante, por ejemplo, si se almacena el volumen de respaldo en un dispositivo guardado en la caja de seguridad de un banco (o en cualquier otra ubicación a la que un adversario pueda acceder repetidamente) y el volumen contiene un volumen oculto (para más información, consulte la subsección " Requisitos de seguridad y precauciones para volúmenes ocultos" en el capítulo "Negación plausible").

- Que uno de los volúmenes sea una copia de seguridad del otro.

Particiones del sistema

Nota: Además de hacer una copia de seguridad de los archivos, le recomendamos que también haga una copia de seguridad de su disco de rescate VeraCrypt (seleccione Sistema > Crear disco de rescate). Para obtener más información, consulte la sección Disco de rescate VeraCrypt.

Para realizar una copia de seguridad de una partición del sistema cifrada de forma segura, se recomienda seguir estos pasos:

1. Si tiene varios sistemas operativos instalados en su computadora, inicie el que no los tenga.
   No requiere autenticación previa al arranque.

   Si no tiene varios sistemas operativos instalados en su computadora, puede iniciar un CD/DVD WinPE o BartPE (Windows "en vivo" almacenado completamente y arrancado desde un CD/DVD; para obtener más información, busque la sección de Preguntas frecuentes la palabra clave "BartPE").

   Si ninguna de las opciones anteriores es posible, conecte la unidad del sistema como unidad secundaria a otra computadora y luego inicie el sistema operativo instalado en la computadora.

   Nota: Por razones de seguridad, si el sistema operativo del que desea realizar una copia de seguridad reside en un volumen oculto de VeraCrypt (consulte la sección " Sistema operativo oculto"), el sistema operativo que inicie en este paso debe ser otro sistema operativo oculto o un sistema operativo "live-CD" (consulte más arriba). Para obtener más información, consulte la subsección " Requisitos y precauciones de seguridad para volúmenes ocultos" del capítulo "Negación plausible".

2. Cree un nuevo volumen VeraCrypt que no sea del sistema utilizando la herramienta de creación de volúmenes VeraCrypt.
   Asistente (no active la opción de Formato rápido ni la opción Dinámico). Será su volumen de respaldo , por lo que su tamaño debe ser igual o mayor que el de la partición del sistema que desea respaldar.

   Si el sistema operativo del que desea realizar una copia de seguridad está instalado en un volumen VeraCrypt oculto (consulte la sección " Sistema operativo oculto"), el volumen de copia de seguridad también debe ser un volumen VeraCrypt oculto.
   Antes de crear el volumen de copia de seguridad oculto , debe crear un...
   nuevo Volumen host (externo) sin habilitar la opción de formato rápido . Además, especialmente si el volumen de respaldo está alojado en archivos, el volumen de respaldo oculto debe ocupar una porción muy pequeña del contenedor y el volumen externo podría debe estar casi completamente lleno de archivos (de lo contrario, la posibilidad de denegar el volumen oculto verse afectada).

3. Monte el volumen de respaldo recién creado .

4. Monte la partición del sistema de la que desea realizar una copia de seguridad siguiendo estos pasos:

   a. Haga clic en Seleccionar dispositivo y luego seleccione la partición del sistema que desea respaldar (en el caso de un sistema operativo oculto, seleccione la partición que contiene el volumen oculto en el que está instalado el sistema operativo).

   b. Haga clic en Aceptar.

   c. Seleccione Sistema > Montar sin autenticación previa al arranque.

   d. Ingrese su contraseña de autenticación previa al arranque y haga clic en Aceptar.

5. Monte el volumen de respaldo y luego use un programa de terceros o una herramienta de Windows para crear una imagen del sistema de archivos que reside en la partición del sistema (que se montó como un

volumen VeraCrypt normal en el paso anterior) y almacene la imagen directamente en el volumen de respaldo montado .

IMPORTANTE: Si almacena el volumen de respaldo en cualquier ubicación a la que un adversario puede acceder repetidamente (por ejemplo, en un dispositivo guardado en la caja de seguridad de un banco), debe repetir todos los pasos anteriores (incluido el paso 2) cada vez que desee realizar una copia de seguridad del volumen (ver a continuación).

Si sigue los pasos anteriores, ayudará a evitar que los adversarios se enteren:

Qué sectores de los volúmenes están cambiando (ya que siempre se sigue el paso 2). Esto es especialmente importante, por ejemplo, si se almacena el volumen de respaldo en un dispositivo guardado en la caja de seguridad de un banco (o en cualquier otra ubicación a la que un adversario pueda acceder repetidamente) y el volumen contiene un volumen oculto (para más información, consulte la subsección " Requisitos de seguridad y precauciones para volúmenes ocultos" en el capítulo "Negación plausible").

• Que uno de los volúmenes sea una copia de seguridad del otro.

Notas generales

Si almacena el volumen de respaldo en una ubicación donde un atacante pueda realizar una copia, considere cifrarlo con una cascada de cifrados (por ejemplo, con AES-Twofish-Serpent). De lo contrario, si el volumen se cifra con un solo algoritmo y este se descifra posteriormente (por ejemplo, debido a avances en criptoanálisis), el atacante podría descifrar sus copias. La probabilidad de que se descifren tres algoritmos de cifrado distintos.

se romperá es significativamente menor que la probabilidad de que sólo uno de ellos se rompa.

Misceláneas

Uso de VeraCrypt sin privilegios de administrador

En Windows, un usuario sin privilegios de administrador puede usar VeraCrypt, pero solo después de que un administrador del sistema lo instale. Esto se debe a que VeraCrypt necesita un controlador de dispositivo para proporcionar cifrado y descifrado transparente sobre la marcha, y los usuarios sin privilegios de administrador no pueden instalar ni iniciar controladores de dispositivo en Windows.

Después de que un administrador del sistema instale VeraCrypt, los usuarios sin privilegios de administrador podrán ejecutarlo, montar y desmontar cualquier tipo de volumen VeraCrypt, cargar y guardar datos desde y hacia él, y crear volúmenes VeraCrypt alojados en archivos. Sin embargo, no podrán cifrar ni formatear particiones, crear volúmenes NTFS, instalar ni desinstalar VeraCrypt, cambiar contraseñas ni archivos de claves de particiones o dispositivos VeraCrypt, realizar copias de seguridad ni restaurar encabezados de particiones o dispositivos VeraCrypt, ni ejecutar VeraCrypt en modo portátil.

> Advertencia: No importa qué tipo de software utilice, en lo que respecta a la privacidad personal en la mayoría de los casos, no es seguro trabajar con datos confidenciales en sistemas en los que no tiene privilegios de administrador, ya que el administrador puede capturar y copiar fácilmente sus datos confidenciales, incluidas contraseñas y claves.

Compartir a través de la red

Si es necesario acceder a un solo volumen de VeraCrypt simultáneamente desde varios sistemas operativos, hay dos opciones:

1. Un volumen VeraCrypt se monta solo en un ordenador (por ejemplo, en un servidor) y solo su contenido (es decir, el sistema de archivos dentro del volumen VeraCrypt) se comparte en red. Los usuarios de otros ordenadores o sistemas no montarán el volumen (ya está montado en el servidor).

   Ventajas: Todos los usuarios pueden escribir datos en el volumen VeraCrypt. El volumen compartido puede alojar tanto archivos como particiones o dispositivos.

   Desventaja: Los datos enviados a través de la red no se cifrarán. Sin embargo, aún es posible cifrarlos mediante, por ejemplo, SSL, TLS, VPN u otras tecnologías.

   Observaciones: Tenga en cuenta que, al reiniciar el sistema, el recurso compartido de red se restaurará automáticamente solo si el volumen es un volumen favorito del sistema o una partición/unidad del sistema cifrada (para obtener información sobre cómo configurar un volumen como un volumen favorito del sistema, consulte el capítulo Volúmenes favoritos del sistema).

2. Un contenedor de archivos VeraCrypt desmontado se almacena en una sola computadora (por ejemplo, en una Este archivo cifrado se comparte en red. Los usuarios de otros ordenadores o sistemas lo montarán localmente. Por lo tanto, el volumen se montará simultáneamente en varios sistemas operativos.

   Ventaja: Los datos enviados a través de la red estarán cifrados (sin embargo, todavía se recomienda cifrarlos utilizando, por ejemplo, SSL, TLS, VPN u otras tecnologías adecuadas para dificultar el análisis del tráfico y preservar la integridad de los datos).

   Desventajas: El volumen compartido solo puede estar alojado en archivos (no en particiones o dispositivos). El volumen debe montarse en modo de solo lectura en cada uno de los sistemas (consulte la sección " Opciones de montaje" para obtener información sobre cómo montar un volumen en modo de solo lectura). Tenga en cuenta que este requisito también se aplica a los volúmenes sin cifrar. Una de las razones es, por ejemplo, que los datos leídos desde un sistema de archivos convencional en un sistema operativo mientras otro lo modifica pueden ser inconsistentes (lo que podría provocar daños en los datos).

Cuando se cierra la ventana principal de VeraCrypt, la tarea en segundo plano de VeraCrypt se encarga de las siguientes tareas/funciones:

1. Teclas de acceso rápido 2. Desmontaje automático (por ejemplo, al cerrar sesión, al retirar accidentalmente un dispositivo host, al vencer el tiempo de espera, etc.)
3. Montaje automático de volúmenes favoritos
4. Notificaciones (por ejemplo, cuando se evitan daños al volumen oculto)
5. Icono de la bandeja

ADVERTENCIA: Si ni la tarea en segundo plano de VeraCrypt ni VeraCrypt están en ejecución, las tareas/funciones mencionadas anteriormente estarán deshabilitadas.

La tarea en segundo plano de VeraCrypt es en realidad la aplicación VeraCrypt.exe , que continúa ejecutándose en segundo plano después de cerrar la ventana principal de VeraCrypt. Puede determinar si se está ejecutando en la bandeja del sistema. Si ve el icono de VeraCrypt, significa que la tarea en segundo plano de VeraCrypt se está ejecutando. Puede hacer clic en el icono para abrir la ventana principal de VeraCrypt.
Al hacer clic derecho en el icono se abre un menú emergente con varias funciones relacionadas con VeraCrypt.

Puede cerrar la Tarea en Segundo Plano en cualquier momento haciendo clic derecho en el icono de VeraCrypt en la bandeja del sistema y seleccionando Salir. Si necesita desactivar la Tarea en Segundo Plano de VeraCrypt por completo y de forma permanente, seleccione Configuración > Preferencias y desmarque la opción Habilitada en el área "Tarea en Segundo Plano de VeraCrypt" del cuadro de diálogo "Preferencias" .

Volumen montado como medio extraíble

Esta sección se aplica a los volúmenes de VeraCrypt montados cuando una de las siguientes opciones está habilitada (según corresponda):

- Herramientas > Preferencias > Montar volúmenes como medios extraíbles
- Opciones de montaje > Montar volumen como medio extraíble
- Favoritos > Organizar volúmenes favoritos > Montar el volumen seleccionado como medio extraíble
- Favoritos > Organizar volúmenes favoritos del sistema > Montar el volumen seleccionado como extraíble medio

Los volúmenes VeraCrypt que se montan como medios extraíbles tienen las siguientes ventajas y desventajas:

- A Windows se le impide crear automáticamente el archivo 'Reciclado' y/o el archivo 'Sistema'. Carpetas de 'Información de volumen' en los volúmenes de VeraCrypt (en Windows, estas carpetas son utilizadas por las funciones Papelera de reciclaje y Restaurar sistema).
- A Windows 8 y versiones posteriores se les impide escribir un Evento 98 en el Registro de eventos que Contiene el nombre del dispositivo (\\device\VeraCryptVolumeXX) de los volúmenes VeraCrypt formateados con NTFS. Esta función de registro de eventos se introdujo en Windows 8 como parte de las nuevas comprobaciones de estado de NTFS, como se explica aquí. Muchas gracias a Liran Elharar por descubrir esto.

Windows puede usar métodos de almacenamiento en caché y retrasos de escritura que se suelen usar para medios extraíbles (por ejemplo, unidades flash USB). Esto podría reducir ligeramente el rendimiento, pero al mismo tiempo aumenta la probabilidad de desmontar el volumen rápidamente sin tener que forzar el desmontaje.

El sistema operativo podría minimizar el número de controladores que abre para dicho volumen. Por lo tanto, los volúmenes montados como medios extraíbles podrían requerir menos desmontajes forzados que otros volúmenes.

- En Windows Vista y versiones anteriores, la lista "Equipo" (o "Mi PC") no muestra la cantidad de espacio libre en los volúmenes montados como extraíbles (tenga en cuenta que esto es una limitación de Windows, no un error de VeraCrypt).
- En las ediciones de escritorio de Windows Vista o posteriores, los sectores de un volumen montado como medio extraíble pueden ser accesibles para todos los usuarios (incluidos los usuarios sin privilegios de administrador; consulte la sección Entorno multiusuario).

Archivos del sistema y datos de la aplicación VeraCrypt

Nota: %windir% es la ruta de instalación principal de Windows (por ejemplo, C:\WINDOWS)

Controlador VeraCrypt

%windir%\SYSTEM32\DRIVERS\veracrypt.sys

Nota: Este archivo no está presente cuando VeraCrypt se ejecuta en modo portátil.

Configuración de VeraCrypt, datos de la aplicación y otros archivos del sistema

ADVERTENCIA: Tenga en cuenta que VeraCrypt no cifra ninguno de los archivos enumerados en esta sección (a menos que cifre la partición/unidad del sistema).

Los siguientes archivos se guardan en la carpeta %APPDATA%\VeraCrypt\. En modo portátil, estos archivos se guardan en la carpeta desde la que se ejecuta el archivo VeraCrypt.exe (es decir, la carpeta donde se encuentra VeraCrypt.exe):

- “Configuration.xml” (el archivo de configuración principal).
- “System Encryption.xml” (archivo de configuración temporal utilizado durante el proceso inicial de cifrado/descifrado local de la partición/unidad del sistema).
- “Archivos de clave predeterminados.xml”
  - Nota: Este archivo puede estar ausente si no se utiliza la función VeraCrypt correspondiente.
- “Favorite Volumes.xml” o Nota: Este archivo puede estar ausente si no se utiliza la función VeraCrypt correspondiente.
- “History.xml” (la lista de los últimos veinte archivos/dispositivos que se intentaron montar como Volúmenes de VeraCrypt o que se han intentado usar como hosts para volúmenes de VeraCrypt; esta función se puede desactivar; para obtener más información, consulte la sección Nunca guardar historial)
  - Nota: Este archivo puede estar ausente si no se utiliza la función VeraCrypt correspondiente.
- “Cifrado local” • “Algoritmo de borrado de cifrado local” (archivos de configuración temporales utilizados durante el proceso inicial de cifrado/descifrado local de un volumen que no es del sistema).

- “Tarea posterior a la instalación: Tutorial”
- “Tarea posterior a la instalación: Notas de la versión”

(archivos de configuración temporales utilizados durante el proceso de instalación o actualización de VeraCrypt).

Los siguientes archivos se guardan en la carpeta %ALLUSERSPROFILE%\VeraCrypt\:

- “Cargador de sistema original” (una copia de seguridad del contenido original de la primera pista de la unidad realizada antes de que se escribiera en ella el cargador de arranque VeraCrypt). o Nota: Este archivo no está presente si la partición/unidad del sistema no se ha cifrado.

Los siguientes archivos se guardan en la carpeta %windir%\system32 (tanto en sistemas de 32 bits como en sistemas de 64 bits):

- “VeraCrypt System Favorite Volumes.xml” o Nota: Este archivo puede estar ausente si no se utiliza la función VeraCrypt correspondiente.

- “VeraCrypt.exe”
  - o Nota: Una copia de este archivo se encuentra en esta carpeta solo cuando se monta el sistema Los volúmenes favoritos están habilitados.

Cómo eliminar el cifrado

Tenga en cuenta que VeraCrypt solo puede descifrar particiones y unidades in situ (seleccione Sistema > Descifrar permanentemente la partición/unidad del sistema para la partición/unidad del sistema y Volúmenes > Descifrar permanentemente para la partición/unidad que no sea del sistema). Si necesita eliminar el cifrado (por ejemplo, si ya no lo necesita) de un volumen alojado en archivos, siga estos pasos:

1. Monte el volumen VeraCrypt.

2. Mueva todos los archivos del volumen VeraCrypt a cualquier ubicación fuera del volumen VeraCrypt (tenga en cuenta que los archivos se descifrarán sobre la marcha).

3. Desmonte el volumen VeraCrypt.

4. Elimínelo (el contenedor) tal como eliminaría cualquier otro archivo.

Si no se desea realizar el descifrado local de particiones/unidades que no son del sistema, también es posible en este caso seguir los pasos 1 a 3 descritos anteriormente.

En todos los casos, si se siguen los pasos 1-3, se pueden realizar las siguientes operaciones adicionales:

Si el volumen está alojado en una partición (también se aplica a unidades flash USB)

a. Haga clic derecho en el ícono "Equipo" (o "Mi PC") en su escritorio o en el
En el menú Inicio, seleccione Administrar. Debería aparecer la ventana "Administración del equipo" .

b. En la ventana Administración del equipo , en la lista de la izquierda, seleccione 'Disco'
'Administración' (dentro del subárbol Almacenamiento).
c. Haga clic derecho en la partición que desea descifrar y seleccione "Cambiar letra y rutas de unidad". d. Debería aparecer la ventana "Cambiar letra y rutas de unidad" . Si no se muestra ninguna letra de unidad en la
ventana, haga clic en Agregar. De lo contrario, haga clic en Cancelar.
Si hizo clic en Agregar, en la sección "Agregar letra o ruta de unidad" (que debería haber aparecido), seleccione la letra de unidad que desee asignar a la partición y haga clic en Aceptar. e. En la ventana Administración de equipos , haga clic con el botón derecho en la partición que desee descifrar.
de nuevo y seleccione Formato. Debería aparecer la ventana Formato .
f. En la ventana Formato , haga clic en Aceptar. Una vez formateada la partición, ya no será necesario montarla
con VeraCrypt para guardar o cargar archivos en ella.

Si el volumen está alojado en el dispositivo

a. Haga clic derecho en el ícono "Equipo" (o "Mi PC") en su escritorio o en el
En el menú Inicio, seleccione Administrar. Debería aparecer la ventana "Administración del equipo" .

b. En la ventana Administración del equipo , en la lista de la izquierda, seleccione 'Disco'
Administración (dentro del subárbol de Almacenamiento).
c. Debería aparecer la ventana "Inicializar disco" . Úsela para inicializar el disco. d. En la ventana "Administración de equipos" , haga clic con el botón derecho en el área que representa el espacio de almacenamiento
del dispositivo cifrado y seleccione "Nueva partición" o "Nuevo volumen simple". e. ADVERTENCIA: Antes de continuar, asegúrese de haber seleccionado el dispositivo correcto, ya que se perderán todos los archivos almacenados.
Debería aparecer la ventana "Asistente para nueva partición" o "Asistente para nuevo volumen simple" ; siga sus instrucciones para crear una nueva partición en el dispositivo. Una vez creada la partición, ya no será necesario montar el dispositivo con VeraCrypt para poder guardar o cargar archivos en él.

Desinstalación de VeraCrypt

Para desinstalar VeraCrypt en Windows XP, seleccione el menú Inicio > Configuración > Panel de control > Agregar o quitar programas > VeraCrypt > Cambiar o quitar.

Para desinstalar VeraCrypt en Windows Vista o posterior, seleccione el menú Inicio > Equipo > Desinstalar o cambiar un programa > VeraCrypt > Desinstalar.

Ningún volumen de VeraCrypt se eliminará al desinstalarlo. Podrá volver a montar sus volúmenes de VeraCrypt después de instalarlo o al ejecutarlo en modo portátil.

Firmas digitales

¿Por qué verificar las firmas digitales?

Podría ocurrir que un paquete de instalación de VeraCrypt que descargue de nuestro servidor haya sido creado o modificado por un atacante. Por ejemplo, el atacante podría explotar una vulnerabilidad en el software del servidor que utilizamos y alterar los paquetes de instalación almacenados en el servidor, o bien, podría alterar cualquiera de los archivos que le enviamos.

Por lo tanto, siempre debe verificar la integridad y autenticidad de cada paquete de distribución de VeraCrypt que descargue u obtenga de cualquier fuente. En otras palabras, siempre debe asegurarse de que el archivo fue creado por nosotros y no fue alterado por un atacante. Una forma de hacerlo es verificar las firmas digitales del archivo.

Tipos de firmas digitales que utilizamos

Actualmente utilizamos dos tipos de firmas digitales:

- Firmas PGP (disponibles para todos los paquetes binarios y de código fuente para todos los formatos compatibles) sistemas).
- Firmas X.509 (disponibles para paquetes binarios para Windows).

Ventajas de las firmas X.509

Las firmas X.509 tienen las siguientes ventajas, en comparación con las firmas PGP:

- Es mucho más fácil verificar que la clave que firmó el archivo es realmente nuestra (no la del atacante). • No es necesario descargar ni instalar ningún software adicional para verificar una firma X.509 (consulte abajo).
- No es necesario que descargues ni importes nuestra clave pública (está incrustada en el archivo firmado). • No es necesario que descargues ningún archivo de firma por separado (la firma está incrustada en el archivo firmado). el archivo firmado).

Ventajas de las firmas PGP

Las firmas PGP tienen las siguientes ventajas, en comparación con las firmas X.509:

- No dependen de ninguna autoridad de certificación (que podría estar, por ejemplo, infiltrada o controlada) por un adversario, o ser poco confiable por otras razones).

Cómo verificar firmas X.509

Tenga en cuenta que las firmas X.509 solo están disponibles actualmente para los paquetes de instalación autoextraíbles de VeraCrypt para Windows. Cada archivo incluye una firma digital X.509, junto con el certificado digital IDRIX emitido por una autoridad de certificación pública. Para verificar la integridad y autenticidad de un paquete de instalación autoextraíble para Windows, siga estos pasos:

1. Descargue el paquete de instalación autoextraíble de VeraCrypt.

2. En el Explorador de Windows, haga clic en el archivo descargado ('VeraCrypt Setup.exe') con el botón derecho del mouse y seleccione 'Propiedades' en el menú contextual.

3. En la ventana de diálogo Propiedades , seleccione la pestaña "Firmas digitales" .

4. En la pestaña 'Firmas digitales' , en la 'Lista de firmas', haga doble clic en la línea que dice "IDRIX" o "IDRIX SARL".

5. Debería aparecer la ventana de diálogo "Detalles de la firma digital" . Si ve lo siguiente: frase en la parte superior de la ventana de diálogo, entonces se habrá verificado con éxito la integridad y autenticidad del paquete:

   "Esta firma digital está bien."

   Si no ve la frase anterior, es muy probable que el archivo esté dañado. Nota: En algunas versiones obsoletas de Windows, faltan algunos de los certificados necesarios, lo que provoca un error en la verificación de firmas.

Cómo verificar firmas PGP

Para verificar una firma PGP, siga estos pasos:

1. Instale cualquier software de cifrado de clave pública compatible con firmas PGP. Para Windows, puede descargar Gpg4win. Para obtener más información, puede visitar https://www.gnupg.org/.
2. Cree una clave privada (para obtener información sobre cómo hacerlo, consulte la documentación de la software de cifrado de clave pública).
3. Descargue nuestra clave pública PGP desde el sitio web de IDRIX o desde un repositorio de clave pública confiable (ID=0x54DDD393), e importe la clave descargada a su llavero (para obtener información sobre cómo hacerlo, consulte la documentación del software de cifrado de clave pública).
   Por favor verifique que su huella digital sea 993B7D7E8E413809828F0F29EB559C7C54DDD393.
4. Firme la clave importada con su clave privada para marcarla como confiable (para obtener información sobre cómo hacerlo, consulte la documentación del software de cifrado de clave pública).
   Nota: Si omite este paso e intenta verificar cualquiera de nuestras firmas PGP, recibirá un mensaje de error indicando que la clave de firma no es válida.
5. Descargue la firma digital haciendo clic en el botón Firma PGP junto al archivo que desea. desea verificar (en una de las páginas de descarga).
6. Verifique la firma descargada (para obtener información sobre cómo hacerlo, consulte la documentación del software de cifrado de clave pública).

Solución de problemas

> Se recomienda que lea también la última versión en línea de este capítulo en:
> https://veracrypt.codeplex.com/wikipage?title=Troubleshooting

Esta sección presenta posibles soluciones a problemas comunes que puede encontrar al utilizar VeraCrypt.

Nota: Si su problema no aparece aquí, es posible que aparezca en una de las siguientes secciones:

- Incompatibilidades
- Problemas conocidos y limitaciones
- Preguntas frecuentes

> Asegúrese de utilizar la última versión estable de VeraCrypt. Si el problema se debe a un error en una versión anterior de VeraCrypt, es posible que ya se haya solucionado. Nota: Seleccione Ayuda > Acerca de para saber qué versión usa.

PROBLEMA:

La escritura/lectura hacia/desde el volumen es muy lenta aunque, según el punto de referencia, la velocidad del cifrado que estoy usando es mayor que la velocidad del disco duro.

CAUSA PROBABLE :

Probablemente esto se deba a una aplicación que interfiere.

POSIBLE SOLUCIÓN:

Primero, asegúrese de que su contenedor VeraCrypt no tenga una extensión reservada para archivos ejecutables (por ejemplo, .exe, .sys o .dll). De ser así, Windows y el software antivirus podrían interferir con el contenedor y afectar negativamente el rendimiento del volumen.

En segundo lugar, desactive o desinstale cualquier aplicación que pueda interferir, como un antivirus o una herramienta de desfragmentación automática de disco, etc. En el caso del antivirus, suele ser útil desactivar el análisis en tiempo real (al acceder) en las preferencias. Si no funciona, intente desactivar temporalmente el antivirus. Si esto tampoco funciona, intente desinstalarlo por completo y reiniciar el equipo posteriormente.

PROBLEMA:

No se puede montar un volumen VeraCrypt; VeraCrypt informa “Contraseña incorrecta o no es un volumen VeraCrypt”.

POSIBLE CAUSA:

Es posible que el encabezado del volumen haya sido dañado por una aplicación de terceros o un componente de hardware que no funciona correctamente.

POSIBLES SOLUCIONES:

• Puede intentar restaurar el encabezado del volumen desde la copia de seguridad incrustada en el volumen siguiendo estos pasos:

1) Ejecute VeraCrypt.

2) Haga clic en Seleccionar dispositivo o Seleccionar archivo para seleccionar su volumen.

3) Seleccione Herramientas > Restaurar encabezado de volumen.

PROBLEMA:

Después de montar exitosamente un volumen, Windows informa "Este dispositivo no contiene un sistema de archivos válido" o un error similar.

CAUSA PROBABLE :

Es posible que el sistema de archivos del volumen VeraCrypt esté dañado (o que el volumen no esté formateado).

POSIBLE SOLUCIÓN:

Puede usar las herramientas de reparación del sistema de archivos incluidas con su sistema operativo para intentar reparar el sistema de archivos en el volumen VeraCrypt. En Windows, es la herramienta 'chkdsk' . VeraCrypt ofrece una sencilla

Para usar esta herramienta en un volumen VeraCrypt: Primero, haga una copia de seguridad del volumen VeraCrypt (ya que la herramienta 'chkdsk' podría dañar aún más el sistema de archivos) y luego móntelo. Haga clic derecho en el volumen montado en la ventana principal de VeraCrypt (en la lista de unidades) y, en el menú contextual, seleccione 'Reparar sistema de archivos'.

PROBLEMA:

Al intentar crear un volumen oculto, su tamaño máximo posible es inesperadamente pequeño (hay mucho más espacio libre que este en el volumen externo).

CAUSAS PROBABLES :

1. El volumen externo se ha formateado como NTFS. 2.
Fragmentación. 3.
Tamaño de clúster demasiado pequeño + demasiados archivos/carpetas en el directorio raíz del volumen externo.

POSIBLES SOLUCIONES:

Soluciones relacionadas con la causa 1:

A diferencia del sistema de archivos FAT, el sistema de archivos NTFS siempre almacena los datos internos exactamente en el centro del volumen. Por lo tanto, el volumen oculto solo puede residir en la segunda mitad del volumen externo. Si esta restricción no es aceptable, realice una de las siguientes acciones:

- Reformatee el volumen externo como FAT y luego cree un volumen oculto dentro de él.

- Si el volumen externo es demasiado grande para formatearlo como FAT, divida el volumen en varios volúmenes de 2 terabytes (o volúmenes de 16 terabytes si el dispositivo utiliza sectores de 4 kilobytes) y formatee cada uno de ellos como FAT.

Solución relacionada con la causa 2:

Cree un nuevo volumen externo (la desfragmentación no es una solución, porque afectaría negativamente la posibilidad de denegación plausible; consulte la sección Desfragmentación).

Solución relacionada con la causa 3:

Nota: La siguiente solución se aplica únicamente a volúmenes ocultos creados dentro de volúmenes FAT.

Desfragmente el volumen externo (móntelo, haga clic con el botón derecho en la letra de la unidad en la ventana "Equipo" o "Mi PC" , haga clic en Propiedades, seleccione la pestaña Herramientas y haga clic en "Desfragmentar ahora"). Una vez desfragmentado el volumen, salga del Desfragmentador de disco e intente crear de nuevo el volumen oculto.

Si esto no soluciona el problema, elimine todos los archivos y carpetas del volumen externo presionando Mayús+Supr, sin formatear (no olvide desactivar previamente la Papelera de reciclaje y Restaurar sistema para esta unidad) e intente crear de nuevo el volumen oculto en este volumen externo completamente vacío (solo para probar). Si el tamaño máximo posible del volumen oculto no cambia, es muy probable que la causa del problema sea un directorio raíz extendido. Si no usó el tamaño de clúster predeterminado (el último paso del asistente), reformatee el volumen externo y, esta vez, deje el tamaño de clúster predeterminado.

Si no funciona, vuelva a formatear el volumen externo y copie menos archivos/carpetas a su carpeta raíz que la última vez. Si no funciona, siga formateando y reduciendo la cantidad de archivos/carpetas en la carpeta raíz. Si esto no es aceptable o no funciona, vuelva a formatear el volumen externo y seleccione un tamaño de clúster mayor. Si no funciona, siga formateando y aumentando el tamaño del clúster hasta que se resuelva el problema. Como alternativa, intente crear un volumen oculto dentro de un volumen NTFS.

PROBLEMA:

Se produce uno de los siguientes problemas:

No se puede montar un volumen VeraCrypt.
No se pueden crear volúmenes VeraCrypt NTFS.

Además, puede informarse el siguiente error: "El proceso no puede acceder al archivo porque está siendo utilizado por otro proceso".

CAUSA PROBABLE :

Esto probablemente se deba a una aplicación que interfiere. Tenga en cuenta que no se trata de un error de VeraCrypt. El sistema operativo informa a VeraCrypt que el dispositivo está bloqueado para el acceso exclusivo de una aplicación (por lo que VeraCrypt no puede acceder a él).

POSIBLE SOLUCIÓN:

Generalmente ayuda deshabilitar o desinstalar la aplicación que interfiere, que suele ser una utilidad antivirus, una aplicación de administración de discos, etc.

PROBLEMA:

En la pantalla del cargador de arranque VeraCrypt, intento escribir mi contraseña y/o presionar otras teclas, pero el cargador de arranque VeraCrypt no responde.

CAUSA PROBABLE :

Tiene un teclado USB (no un teclado PS/2) y la compatibilidad previa al arranque para teclados USB está deshabilitada en la configuración del BIOS.

POSIBLE SOLUCIÓN:

Debe habilitar la compatibilidad con teclados USB antes del arranque en la configuración de la BIOS. Para ello, siga estos pasos:

Reinicie el equipo, presione F2 o Supr (en cuanto vea la pantalla de inicio del BIOS) y espere hasta que aparezca la pantalla de configuración del BIOS. Si no aparece ninguna pantalla de configuración, reinicie el equipo y presione F2 o Supr repetidamente en cuanto lo haga. Cuando aparezca la pantalla de configuración del BIOS, habilite la compatibilidad con teclados USB antes del arranque. Esto suele hacerse seleccionando: Avanzado > Configuración USB > Compatibilidad con USB heredado (o USB Legacy) > Habilitado. (Tenga en cuenta que la palabra "heredado" es engañosa, ya que los componentes de prearranque de las versiones modernas de MS Windows requieren que esta opción esté habilitada para permitir la interacción y el control del usuario). A continuación, guarde la configuración del BIOS (normalmente presionando F10).

y reinicie su computadora. Para obtener más información, consulte la documentación de su BIOS/placa base o contacte con el equipo de soporte técnico del proveedor de su computadora.

PROBLEMA:

Una vez cifrada la partición/unidad del sistema, la computadora no puede iniciarse luego de reiniciarse (tampoco es posible ingresar a la pantalla de configuración del BIOS).

CAUSA PROBABLE :

Un error en el BIOS de su computadora.

POSIBLES SOLUCIONES:

Siga estos pasos:

1. Desconecte la unidad cifrada.
2. Conecte una unidad no cifrada con un sistema operativo instalado (o instálelo en el conducir).
3. Actualice el BIOS.
4. Si no ayuda, informe este error al fabricante o al proveedor de la computadora.

O

Si el fabricante/proveedor del BIOS/placa base/computadora no proporciona ninguna actualización que resuelva el problema y usted usa Windows 7 o posterior y hay una partición de arranque adicional (cuyo tamaño es menor a 1 GB) en la unidad, puede intentar reinstalar Windows sin esta partición de arranque adicional (para solucionar un error en el BIOS).

PROBLEMA:

Se produce uno de los siguientes problemas:

Después de ingresar la contraseña de autenticación previa al arranque durante la prueba previa de cifrado del sistema, El ordenador se cuelga (después de que aparece el mensaje 'Arrancando...').

Cuando la partición/unidad del sistema está cifrada (parcial o totalmente) y el sistema está Al reiniciar por primera vez desde que se inició el proceso de cifrado de la partición/unidad del sistema, la computadora se bloquea después de ingresar la contraseña de autenticación previa al arranque (después de que se muestra el mensaje "Arrancando...").

Después de clonar el sistema operativo oculto y de ingresar la contraseña, La computadora se cuelga (después de que se muestra el mensaje 'Arrancando...')

CAUSA PROBABLE :

Un error en el BIOS de su computadora o un problema con el cargador de arranque de Windows.

POSIBLES SOLUCIONES:

Actualice su BIOS (para obtener información sobre cómo hacerlo, consulte la documentación para su BIOS/placa base o comuníquese con el equipo de soporte técnico del proveedor de su computadora para obtener ayuda).

Utilice un modelo/marca de placa base diferente.

Si el fabricante/proveedor del BIOS/placa base/computadora no proporciona ninguna actualización que resuelve el problema y usa Windows 7 o posterior y hay un arranque adicional partición (cuyo tamaño sea menor a 1 GB) en la unidad, puede intentar reinstalar Windows sin esta partición de arranque adicional (para solucionar un error en el BIOS).

Existen otras dos soluciones alternativas conocidas para este problema que requieren tener un sistema operativo Windows. Disco de instalación:

- Inicie su máquina usando un disco de instalación de Windows y seleccione reparar su Computadora. Seleccione la opción "Símbolo del sistema" y, cuando se abra, escriba los siguientes comandos y reinicie el sistema:
  - BootRec /fixmbr •
    BootRec /FixBoot
- Elimine la partición reservada del sistema de 100 MB ubicada al comienzo de En su unidad, configure la partición del sistema adyacente como partición activa (ambas opciones se pueden realizar con la utilidad DiskPart, disponible en la opción de reparación del disco de instalación de Windows). Después, ejecute la Reparación de inicio después de reiniciar en el disco de instalación de Windows. El siguiente enlace contiene instrucciones detalladas: http://www.sevenforums.com/tutorials/71363-system-reserved-partition-delete.html

---

PROBLEMA:

Al montar o desmontar un volumen de VeraCrypt, el sistema se bloquea (aparece un error de "pantalla azul") aparece la pantalla o la computadora se reinicia abruptamente).

O

Desde que instalé VeraCrypt, el sistema operativo se bloquea con frecuencia.

POSIBLES CAUSAS:

Un error en una aplicación de terceros (por ejemplo, antivirus, "modificador" del sistema, etc.)
Un error en VeraCrypt
Un error en Windows o un componente de hardware que no funciona correctamente

POSIBLES SOLUCIONES:

Intente deshabilitar todas las herramientas antivirus, modificadores del sistema y cualquier otra aplicación similar. Si no ayuda, intente desinstalarlos y reiniciar Windows.

Si el problema persiste, ejecute VeraCrypt y seleccione Ayuda > 'Analizar un bloqueo del sistema'. VeraCrypt luego analizará los archivos de volcado de memoria que Windows creó automáticamente cuando Se bloqueó (si es que lo hubo). Si VeraCrypt determina que es probable que un error en un controlador de terceros... han causado el bloqueo, se mostrará el nombre y el proveedor del controlador (tenga en cuenta que Actualizar o desinstalar el controlador podría resolver el problema). Sea cual sea el resultado, Podrán optar por enviarnos información esencial sobre la falla del sistema para ayudar. Vamos a determinar si fue causado por un error en VeraCrypt.

PROBLEMA:

Al intentar cifrar la partición/unidad del sistema, durante la prueba previa, el cargador de arranque VeraCrypt siempre informa que la contraseña de autenticación previa al arranque que ingresé es incorrecta (aunque estoy seguro de que es correcta).

POSIBLES CAUSAS:

Estado diferente de la tecla Bloq Num y/o Bloq Mayús Corrupción de datos

POSIBLE SOLUCIÓN:

1. Cuando configure una contraseña de autenticación previa al arranque, recuerde si la tecla Bloq Num Las teclas Bloq Mayús están activadas o desactivadas (según el fabricante, pueden tener diferentes nombres, como Bloq Mayús). Nota: Puede cambiar el estado de cada tecla como desee antes de establecer la contraseña, pero debe recordarlos.

2. Cuando ingrese la contraseña en la pantalla VeraCrypt Boot Loader, asegúrese de que el estado de cada una de las claves es la misma que cuando se establece la contraseña.

Nota: Para otras posibles soluciones a este problema, consulte las otras secciones de este capítulo.

PROBLEMA:

Cuando la partición/unidad del sistema está cifrada, el sistema operativo se "congela" durante aproximadamente 10 a 60 segundos cada 5 a 60 minutos (puede coexistir un uso del 100 % de la CPU).

CAUSA PROBABLE :

Un problema de CPU y/o placa base.

POSIBLES SOLUCIONES:

Intente actualizar el BIOS.

Intente deshabilitar todas las funciones relacionadas con el ahorro de energía (incluida cualquier función especial mejorada por la CPU). detener funciones) en la configuración del BIOS y en el panel de control 'Opciones de energía' de Windows.

Reemplace el procesador por uno diferente (de otro tipo y/o marca).

Reemplace la placa base por una diferente (de otro tipo y/o marca).

PROBLEMA:

En Windows 7/Vista (y posiblemente versiones posteriores), la herramienta Microsoft Windows Backup no se puede utilizar para realizar copias de seguridad de datos en un volumen VeraCrypt que no sea del sistema.

CAUSA:

Un error en la herramienta de copia de seguridad de Windows.

POSIBLE SOLUCIÓN:

1. Monte el volumen VeraCrypt en el que desea realizar una copia de seguridad de los datos.
2. Haga clic derecho en una carpeta ubicada en el volumen (o haga clic derecho en su letra de unidad en la lista "Equipo") y seleccione un elemento del submenú "Compartir con" (en Windows Vista, seleccione "Compartir").
3. Siga las instrucciones para compartir la carpeta con su cuenta de usuario.
4. En la herramienta Copia de seguridad de Windows, seleccione la carpeta compartida (la ubicación/ruta de red) como el destino.
5. Inicie el proceso de copia de seguridad.

Nota: La solución anterior no se aplica a las ediciones Starter y Home de Windows 7 (y posiblemente a versiones posteriores).

PROBLEMA:

La etiqueta de un sistema de archivos en un volumen VeraCrypt no se puede cambiar desde la ventana "Equipo" en Windows Vista o una versión posterior de Windows.

CAUSA:

Un problema de Windows hace que la etiqueta se escriba solo en el archivo de registro de Windows, en lugar de escribirse en el sistema de archivos.

POSIBLES SOLUCIONES:

Haga clic con el botón derecho en el volumen montado en la ventana "Equipo", seleccione Propiedades e ingrese una nueva etiqueta para el volumen.

PROBLEMA:

No puedo cifrar una partición/dispositivo porque el Asistente de creación de volumen VeraCrypt dice que está en uso.

POSIBLE SOLUCIÓN:

Cierre, desactive o desinstale todos los programas que puedan estar usando la partición/dispositivo (por ejemplo, un antivirus). Si esto no soluciona el problema, haga clic con el botón derecho en el icono de "Equipo" (o "Mi PC") en el escritorio y seleccione Administrar > Almacenamiento > Administración de discos. A continuación, haga clic con el botón derecho en la partición que desea cifrar y haga clic en "Cambiar letra y rutas de unidad". A continuación, haga clic en "Eliminar" y en "Aceptar".
Reinicie el sistema operativo.

PROBLEMA:

Al crear un volumen oculto, el asistente informa que no se puede bloquear el volumen externo.

CAUSA PROBABLE :

El volumen externo contiene archivos que utilizan una o más aplicaciones.

POSIBLE SOLUCIÓN:

Cierre todas las aplicaciones que estén usando archivos en el volumen externo. Si esto no soluciona el problema, intente deshabilitar o desinstalar cualquier antivirus que utilice y reinicie el sistema posteriormente.

PROBLEMA:

Al acceder a un contenedor alojado en archivos compartido a través de una red, se informa el error "memoria insuficiente" o "no hay suficiente almacenamiento en el servidor disponible".

CAUSA PROBABLE :

Es posible que IRPStackSize en el registro de Windows se haya establecido en un valor demasiado pequeño.

POSIBLE SOLUCIÓN:

Localice la clave IRPStackSize en el Registro de Windows y configúrela con un valor mayor. A continuación, reinicie el sistema. Si la clave no existe en el Registro de Windows, créela en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters y configúrela con un valor 16 o superior. A continuación, reinicie el sistema. Para obtener más información, consulte: http://support.microsoft.com/kb/285089/ y http://support.microsoft.com/kb/177078/

Incompatibilidades

Se recomienda que lea también la última versión en línea de este capítulo en:
https://veracrypt.codeplex.com/wikipage?title=Incompatibilities

Activación de Adobe Photoshop® y otros productos mediante FLEXnet Publisher® / SafeCast

Nota: El problema que se describe a continuación no le afecta si utiliza un algoritmo de cifrado que no sea en cascada (es decir, AES, Serpent o Twofish).* El problema tampoco le afecta si no utiliza la autenticación previa al arranque (consulte el capítulo Cifrado del sistema).

El software de activación Acresso FLEXnet Publisher, anteriormente Macrovision SafeCast (utilizado para la activación de software de terceros, como Adobe Photoshop) , escribe datos en la primera pista de la unidad. Si esto ocurre cuando la partición o unidad del sistema está cifrada con VeraCrypt, una parte del gestor de arranque de VeraCrypt se dañará y no podrá iniciar Windows. En ese caso, siga estos pasos:

Utilice su disco de rescate VeraCrypt para recuperar el acceso a su sistema. Hay dos maneras.

Puede mantener activado el software de terceros, pero deberá iniciar el sistema desde el CD/DVD de VeraCrypt Rescue Disk cada vez. Simplemente inserte el Rescue Disk en la unidad de CD/DVD e introduzca su contraseña en la pantalla de Rescue Disk.

2. Si no desea arrancar el sistema desde el CD/DVD del Disco de Rescate VeraCrypt cada vez, puede restaurar el cargador de arranque VeraCrypt en la unidad del sistema. Para ello, en la pantalla Disco de Rescate, seleccione Opciones de reparación > Restaurar cargador de arranque VeraCrypt. Tenga en cuenta que esto desactivará el software de terceros.

Para obtener información sobre cómo utilizar su disco de rescate VeraCrypt, consulte el capítulo Disco de rescate VeraCrypt.

Posible solución permanente: descifrar la partición/unidad del sistema y luego volver a cifrarla utilizando un algoritmo de cifrado que no sea en cascada (es decir, AES, Serpent o Twofish).*

Tenga en cuenta que esto no es un error de VeraCrypt (el problema se debe al diseño inadecuado del software de activación de terceros).

*La razón es que el cargador de arranque VeraCrypt es más pequeño que el utilizado para las cascadas de cifrados y, por lo tanto, hay suficiente espacio en la primera pista de la unidad para una copia de seguridad del cargador de arranque VeraCrypt. Por lo tanto, si el cargador de arranque VeraCrypt se daña, su copia de seguridad se ejecuta automáticamente.

Problemas y limitaciones conocidos

Se recomienda encarecidamente que lea también la última versión en línea de este capítulo en:
https://veracrypt.codeplex.com/wikipage?title=Problemas y limitaciones

Problemas conocidos

- En Windows, puede suceder que se asignen dos letras de unidad a un volumen montado
  En lugar de uno solo. Esto se debe a un problema con la caché del Administrador de montaje de Windows y se puede solucionar escribiendo el comando "mountvole.exe /r" en un símbolo del sistema con privilegios elevados (ejecutado como administrador) antes de montar cualquier volumen. Si el problema persiste después de reiniciar, se puede usar el siguiente procedimiento para solucionarlo:
  - Revise la clave de registro "HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices" con regedit. Desplácese hacia abajo y encontrará entradas que empiezan por "\DosDevices\" o "\Global??\", que indican las letras de unidad que ocupa el sistema. Antes de montar cualquier volumen, haga doble clic en cada uno y elimine los que contengan "VeraCrypt" y "TrueCrypt".

    Además, hay otras entradas cuyo nombre comienza con "#{" y "\??\Volume{": double
    Haga clic en cada uno de ellos y elimine aquellos cuyo valor de datos contenga el nombre "VeraCrypt" y "TrueCrypt".

Limitaciones

- [Nota: Esta limitación no se aplica a los usuarios de Windows Vista y versiones posteriores de Windows.] En Windows XP/2003, VeraCrypt no admite el cifrado de un sistema completo Unidad que contiene particiones extendidas (lógicas). Puede cifrar una unidad completa del sistema. siempre que contenga solo particiones primarias. Las particiones extendidas (lógicas) no deben ser creado en cualquier unidad del sistema que esté parcial o totalmente cifrada (solo se pueden cifrar las particiones primarias). creado en él). Nota: Si necesita cifrar una unidad completa que contiene particiones extendidas, Puede cifrar la partición del sistema y, además, crear volúmenes VeraCrypt alojados en la partición dentro de cualquier partición que no sea del sistema en la unidad. Alternativamente, puede considerar actualizar a Windows Vista o una versión posterior de Windows.

- VeraCrypt actualmente no admite el cifrado de una unidad del sistema que se haya convertido a un disco dinámico.

- Para solucionar un problema de Windows XP, el cargador de arranque VeraCrypt siempre se inicia automáticamente. configurado para la versión del sistema operativo en el que está instalado. Cuando el La versión del sistema cambia (por ejemplo, el cargador de arranque VeraCrypt se instala cuando Si se está ejecutando Windows Vista, pero luego se utiliza para iniciar Windows XP, es posible que se encuentre con varios problemas conocidos y desconocidos (por ejemplo, en algunas computadoras portátiles, Windows XP puede fallar) para mostrar la pantalla de inicio de sesión). Tenga en cuenta que esto afecta a las configuraciones de arranque múltiple, VeraCrypt Discos de rescate y sistemas operativos señuelo/ocultos (por lo tanto, si el sistema oculto es, por ejemplo, Windows XP, el sistema señuelo también debería ser Windows XP).

- La capacidad de montar una partición que esté dentro del alcance de la clave de cifrado del sistema sin autenticación previa al arranque (por ejemplo, una partición ubicada en la unidad del sistema encriptada de otro sistema operativo que no se esté ejecutando), lo que se puede hacer, por ejemplo, seleccionando Sistema > El montaje sin autenticación previa al arranque está limitado a particiones primarias (extendidas/lógicas) Las particiones no se pueden montar de esta manera).

Debido a un problema de Windows 2000, VeraCrypt no es compatible con el Administrador de montaje de Windows. Por lo tanto, algunas herramientas integradas de Windows 2000, como el Desfragmentador de disco, no funcionan con volúmenes VeraCrypt. Además, no es posible usar los servicios del Administrador de montaje en Windows 2000; por ejemplo, asignar un punto de montaje a un volumen VeraCrypt (es decir, adjuntar un volumen VeraCrypt a una carpeta).

• VeraCrypt no admite la autenticación previa al arranque para sistemas operativos instalados dentro de archivos VHD, excepto cuando se arranca utilizando el software de máquina virtual apropiado, como Microsoft Virtual PC.

• El Servicio de instantáneas de volumen de Windows actualmente solo es compatible con particiones dentro El alcance de la clave de cifrado del sistema (por ejemplo, una partición del sistema cifrada con VeraCrypt o una partición ajena al sistema ubicada en una unidad del sistema cifrada con VeraCrypt, montada mientras se ejecuta el sistema operativo cifrado). Nota: Para otros tipos de volúmenes, el Servicio de Instantáneas de Volumen no es compatible porque la documentación de la API necesaria no está disponible.

La configuración de arranque de Windows no se puede modificar desde un sistema operativo oculto si este no arranca desde la partición donde está instalado. Esto se debe a que, por seguridad, la partición de arranque se monta como de solo lectura cuando se ejecuta el sistema oculto. Para poder modificar la configuración de arranque, inicie el sistema operativo señuelo.

• Las particiones cifradas no se pueden redimensionar, excepto las particiones de una unidad de sistema completamente cifrada que se redimensionan mientras se ejecuta el sistema operativo cifrado.

• Cuando la partición/unidad del sistema está cifrada, el sistema no se puede actualizar (por ejemplo, De Windows XP a Windows Vista) o repararse desde el entorno de prearranque (mediante un CD/DVD de instalación de Windows o el componente de prearranque de Windows). En estos casos, primero se debe descifrar la partición/unidad del sistema. Nota: Un sistema operativo en ejecución puede actualizarse (parches de seguridad, Service Packs, etc.) sin problemas, incluso con la partición/unidad del sistema cifrada.

• El cifrado del sistema solo se admite en unidades que estén conectadas localmente a través de una interfaz ATA/SCSI (tenga en cuenta que el término ATA también se refiere a SATA y eSATA).

Cuando se utiliza cifrado del sistema (esto también aplica a sistemas operativos ocultos), VeraCrypt no admite cambios en la configuración de arranque múltiple (por ejemplo, cambios en el número de sistemas operativos y sus ubicaciones). En concreto, la configuración debe permanecer igual que cuando el Asistente de creación de volúmenes de VeraCrypt comenzó a preparar el proceso de cifrado de la partición/unidad del sistema (o la creación de un sistema operativo oculto).

Nota: La única excepción es la configuración de arranque múltiple, donde un sistema operativo cifrado con VeraCrypt siempre se encuentra en la unidad 0 y es el único sistema operativo presente en la unidad (o hay un sistema operativo señuelo cifrado con VeraCrypt y un sistema operativo oculto cifrado con VeraCrypt, y ningún otro sistema operativo en la unidad), y la unidad se conecta o desconecta antes de encender el ordenador (por ejemplo, mediante el interruptor de encendido de una carcasa de unidad eSATA externa). Es posible que haya sistemas operativos adicionales (cifrados o no) instalados en otras unidades conectadas al ordenador (cuando la unidad 0 se desconecta, la unidad 1 se convierte en la unidad 0, etc.).

• Cuando la carga de la batería del portátil está baja, Windows puede omitir el envío de los mensajes apropiados a las aplicaciones que se ejecutan cuando el ordenador entra en modo de ahorro de energía.
Por lo tanto, es posible que VeraCrypt no pueda desmontar automáticamente los volúmenes en tales casos.

• No se garantiza que la conservación de cualquier marca de tiempo de cualquier archivo (por ejemplo, un contenedor o un archivo de claves) se realice de manera confiable y segura (por ejemplo, debido a los registros del sistema de archivos, las marcas de tiempo de

atributos de archivo, o el sistema operativo no lo realiza por diversos motivos documentados y razones no documentadas). Nota: Cuando escribe en un volumen oculto alojado en archivos, el La marca de tiempo del contenedor puede cambiar. Esto se puede explicar plausiblemente como si hubiera sido causado por cambiar la contraseña del volumen (externo). Tenga en cuenta también que VeraCrypt nunca... conserva las marcas de tiempo de los volúmenes favoritos del sistema (independientemente de la configuración).

• Software especial (por ejemplo, un editor de discos de bajo nivel) que escribe datos en una unidad de disco de manera que Evita los controladores en la pila de controladores de la clase 'DiskDrive' (el GUID de la clase es 4D36E967-E325-11CE-BFC1-08002BE10318) puede escribir datos no cifrados en una unidad que no sea del sistema que albergue un volumen VeraCrypt montado ('Partición0') y a particiones/unidades cifradas que se encuentran dentro de la alcance clave del cifrado del sistema activo (VeraCrypt no cifra datos escritos de esa manera). De manera similar, el software que escribe datos en una unidad de disco elude los controladores en la pila de controladores del sistema. clase 'Volumen de almacenamiento' (el GUID de la clase es 71A27CDD-812A-11D0-BEC7- 08002BE2092F) puede escribir datos no cifrados en volúmenes alojados en particiones VeraCrypt (incluso si están montados).

• Por razones de seguridad, cuando se ejecuta un sistema operativo oculto, VeraCrypt garantiza que todos Los sistemas de archivos locales sin cifrar y los volúmenes VeraCrypt no ocultos son de solo lectura. Sin embargo, esto No se aplica a sistemas de archivos en medios tipo CD/DVD ni en sistemas personalizados, atípicos o no estándar. dispositivos/medios (por ejemplo, cualquier dispositivo/medio cuya clase sea distinta a la del dispositivo de Windows) clase 'Volumen de almacenamiento' o que no cumplen los requisitos de esta clase (el GUID de la clase es 71A27CDD-812A-11D0-BEC7-08002BE2092F)).

• Los volúmenes VeraCrypt alojados en dispositivos ubicados en disquetes no son compatibles. Nota: Puede Todavía se crean volúmenes VeraCrypt alojados en archivos en disquetes.

Las ediciones de Windows Server no permiten el uso de volúmenes VeraCrypt montados como ruta para la copia de seguridad del servidor. Esto se puede solucionar activando el uso compartido del volumen VeraCrypt a través de la interfaz del Explorador (por supuesto, debe configurar los permisos correctos para evitar accesos no autorizados). Acceso) y luego seleccione la opción "Carpeta compartida remota" (no es remota, por supuesto, pero Windows necesita una ruta de red). Allí, puede escribir la ruta de la unidad compartida (por ejemplo, \\NombreServidor\nombreRecursoCompartido) y la copia de seguridad se configurará correctamente.

Debido a fallas de diseño de Microsoft en la gestión de archivos dispersos de NTFS, podrían producirse errores del sistema al escribir datos en volúmenes dinámicos grandes (de más de unos pocos cientos de GB). Para evitar esto, el tamaño recomendado para un archivo contenedor de volumen dinámico para una compatibilidad máxima es de 300 GB. El siguiente enlace ofrece más detalles sobre esta limitación: http://www.flexhex.com/docs/articles/sparse-files.phtml#msdn

Windows 8 introdujo una nueva función llamada "Arranque y apagado híbridos" para que los usuarios perciban un arranque rápido. Esta función está habilitada por defecto y tiene efectos secundarios en el uso de los volúmenes de VeraCrypt. Se recomienda deshabilitarla (este enlace explica cómo). Algunos ejemplos de problemas:

Después de apagar y reiniciar, el volumen montado continuará montándose sin necesidad de escribir la contraseña: esto se debe al hecho de que el nuevo apagado de Windows 8 no es un apagado real sino una hibernación/suspensión disfrazada.

Cuando se utiliza el cifrado del sistema y hay favoritos del sistema configurados para montarse en el momento del arranque: después de apagar y reiniciar, estos favoritos del sistema no se montarán.

No se puede crear un disco de reparación/recuperación del sistema Windows cuando un volumen de VeraCrypt se monta como disco fijo (predeterminado). Para solucionar esto, desmonte todos los volúmenes o móntelos como medios extraíbles.

• Se enumeran más limitaciones en la sección Modelo de seguridad.

Preguntas frecuentes

Nota: La última versión de las preguntas frecuentes de VeraCrypt está disponible en https://veracrypt.codeplex.com/wikipage?title=FAQ.

¿Pueden TrueCrypt y VeraCrypt ejecutarse en la misma máquina?

Sí. Generalmente no hay conflictos entre TrueCrypt y VeraCrypt, por lo que pueden instalarse y usarse en la misma máquina. Sin embargo, en Windows, si ambos se usan para montar el mismo volumen, pueden aparecer dos unidades al montarlo. Esto se puede solucionar ejecutando el siguiente comando en un símbolo del sistema con privilegios elevados (usando Ejecutar como administrador) antes de montar cualquier volumen: mountvol.exe /r.

¿Puedo usar mis volúmenes TrueCrypt en VeraCrypt?

Sí. A partir de la versión 1.0f, VeraCrypt admite el montaje de volúmenes TrueCrypt.

¿Puedo convertir mis volúmenes TrueCrypt al formato VeraCrypt?

Sí. A partir de la versión 1.0f, VeraCrypt ofrece la posibilidad de convertir contenedores TrueCrypt y particiones que no sean del sistema al formato VeraCrypt. Esto se puede lograr mediante la opción "Cambiar contraseña de volumen". o las acciones "Establecer algoritmo de derivación de clave de encabezado". Simplemente marque el "Modo TrueCrypt", ingrese su contraseña de TrueCrypt y realice la operación. Después, su volumen tendrá el formato VeraCrypt.

Antes de realizar la conversión, se recomienda hacer una copia de seguridad del encabezado del volumen con TrueCrypt. Puede eliminar esta copia de seguridad de forma segura una vez finalizada la conversión y tras comprobar que VeraCrypt haya montado correctamente el volumen convertido.

¿Cuál es la diferencia entre TrueCrypt y VeraCrypt?

VeraCrypt agrega seguridad mejorada a los algoritmos utilizados para el cifrado del sistema y de las particiones, haciéndolo inmune a nuevos desarrollos en ataques de fuerza bruta.
También soluciona numerosas vulnerabilidades y problemas de seguridad de TrueCrypt. La siguiente publicación describe parte de las principales mejoras y correcciones realizadas en la versión 1.0e: https://veracrypt.codeplex.com/discussions/569777#PostContent_1313325
Por ejemplo, cuando la partición del sistema está cifrada, TrueCrypt usa PBKDF2-RIPEMD160 con 1000 iteraciones, mientras que en VeraCrypt usamos 327661. Y para contenedores estándar y otras particiones, TrueCrypt usa como máximo 2000 iteraciones, pero VeraCrypt usa 655331 para RIPEMD160 y 500000 iteraciones para SHA-2 y Whirlpool.

Esta seguridad mejorada solo añade un retraso a la apertura de particiones cifradas, sin afectar el rendimiento durante la fase de uso de la aplicación. Esto es aceptable para el propietario legítimo, pero dificulta considerablemente el acceso de un atacante a los datos cifrados.

Olvidé mi contraseña: ¿hay alguna forma ('puerta trasera') de recuperar los archivos de mi VeraCrypt? ¿volumen?

No hemos implementado ninguna 'puerta trasera' en VeraCrypt (y nunca implementaremos ninguna incluso si una agencia gubernamental nos lo solicitara), porque frustraría el propósito del software.
VeraCrypt no permite el descifrado de datos sin conocer la contraseña o clave correctas. No podemos recuperar sus datos porque desconocemos ni podemos determinar la contraseña que eligió ni la clave que generó con VeraCrypt. La única forma de recuperar sus archivos es intentar descifrarlos.
La contraseña o la clave, pero podría tardar miles o millones de años (dependiendo de la longitud y la calidad de la contraseña o los archivos de clave, del rendimiento del software/hardware, los algoritmos y otros factores). En 2010, hubo noticias sobre el fracaso del FBI al descifrar un volumen de TrueCrypt después de...

Año de intentarlo. Si bien no podemos verificar si esto es cierto o simplemente una maniobra de "operación psicológica", en VeraCrypt hemos aumentado la seguridad de la derivación de la clave a un nivel en el que cualquier ataque de fuerza bruta a la contraseña es virtualmente imposible, siempre que se respeten todos los requisitos de seguridad.

¿Existe una “Guía de inicio rápido” o algún tutorial para principiantes?

Sí. El primer capítulo, Tutorial para principiantes, contiene capturas de pantalla e instrucciones paso a paso sobre Cómo crear, montar y utilizar un volumen VeraCrypt.

¿Puedo cifrar una partición/unidad donde está instalado Windows?

Sí (ver el capítulo Cifrado del sistema).

La prueba previa de cifrado del sistema falla porque el gestor de arranque se bloquea con el mensaje "booting" tras verificar correctamente la contraseña. ¿Cómo puedo lograr que la prueba previa sea exitosa?

Hay dos soluciones conocidas para este problema (ambas requieren tener un disco de instalación de Windows):

1. Inicie su máquina usando un disco de instalación de Windows y seleccione reparar su computadora.
   Elija la opción "Símbolo del sistema" y cuando se abra, escriba los siguientes comandos y luego reinicie su sistema:

   o BootRec /fixmbr

   o BootRec /FixBoot

2. Elimine la partición reservada del sistema de 100 MB ubicada al principio de la unidad y configure la partición del sistema contigua como partición activa (ambas opciones se pueden realizar con la utilidad DiskPart, disponible en la opción de reparación del disco de instalación de Windows). A continuación, ejecute la reparación de inicio después de reiniciar el disco de instalación de Windows. El siguiente enlace contiene instrucciones detalladas: http://www.sevenforums.com/tutorials/71363-system-reserved-partition-delete.html

La prueba preliminar de cifrado del sistema falla a pesar de que la contraseña se introdujo correctamente en el gestor de arranque. ¿Cómo puedo lograr que la prueba preliminar sea exitosa?

Esto puede deberse al controlador de TrueCrypt, que borra la memoria del BIOS antes de que VeraCrypt pueda leerla. En este caso, desinstalar TrueCrypt soluciona el problema.
Esto también puede ser causado por algunos controladores de hardware y otro software que acceden a la memoria del BIOS. No existe una solución genérica para esto y los usuarios afectados deben identificar dicho software y eliminarlo del sistema.

¿Puedo reproducir directamente un vídeo (.avi, .mpg, etc.) almacenado en un volumen VeraCrypt?

Sí, los volúmenes cifrados con VeraCrypt son como discos normales. Debe proporcionar la contraseña correcta (y/o archivo de claves) y monte (abra) el volumen VeraCrypt. Al hacer doble clic en el icono del archivo de vídeo, El sistema operativo inicia la aplicación asociada con el tipo de archivo, generalmente un medio. reproductor. A continuación, el reproductor multimedia comienza a cargar una pequeña porción inicial del archivo de vídeo desde el Volumen cifrado con VeraCrypt en la RAM (memoria) para poder reproducirlo. Mientras se reproduce la parte... Una vez cargado, VeraCrypt lo descifra automáticamente (en RAM). La parte descifrada del vídeo... (almacenado en la RAM) es reproducido por el reproductor multimedia. Mientras se reproduce esta parte, el reproductor multimedia...

El reproductor comienza a cargar otra pequeña porción del archivo de video desde el volumen cifrado con VeraCrypt a la RAM (memoria) y el proceso se repite.

Lo mismo ocurre con la grabación de vídeo: antes de escribir un fragmento de un archivo de vídeo en un volumen VeraCrypt, VeraCrypt lo cifra en la RAM y luego lo escribe en el disco. Este proceso se denomina cifrado/descifrado sobre la marcha y funciona con todo tipo de archivos (no solo con los de vídeo).

¿VeraCrypt será de código abierto y gratuito para siempre?

Sí, lo hará. Nunca crearemos una versión comercial de VeraCrypt, ya que creemos en el software de seguridad gratuito y de código abierto.

¿Es posible donar al proyecto VeraCrypt?

Sí, puedes utilizar los botones de donación en https://veracrypt.codeplex.com.

¿Por qué VeraCrypt es de código abierto? ¿Cuáles son sus ventajas?

Dado que el código fuente de VeraCrypt es público, investigadores independientes pueden verificar que no contiene ninguna falla de seguridad ni puerta trasera secreta. Si el código fuente no estuviera disponible, los revisores tendrían que aplicar ingeniería inversa a los archivos ejecutables. Sin embargo, analizar y comprender dicho código es tan difícil que resulta prácticamente imposible (especialmente cuando el código es tan extenso como el de VeraCrypt).

Observación: Un problema similar también afecta al hardware criptográfico. Es muy difícil aplicarle ingeniería inversa para verificar que no contenga ninguna falla de seguridad ni puerta trasera secreta.

VeraCrypt es de código abierto, pero ¿alguien ha revisado realmente el código fuente?

Sí. De hecho, el código fuente es revisado constantemente por numerosos investigadores y usuarios independientes. Lo sabemos porque investigadores independientes han descubierto numerosos errores y varios problemas de seguridad (incluidos algunos muy conocidos) al revisar el código fuente.

Dado que VeraCrypt es un software de código abierto, investigadores independientes pueden verificar que el código fuente no contiene ninguna falla de seguridad ni puerta trasera secreta. ¿Pueden también verificar que los archivos ejecutables oficiales se crearon a partir del código fuente publicado y no contienen código adicional?

Sí, pueden. Además de revisar el código fuente, investigadores independientes pueden compilarlo y comparar los archivos ejecutables resultantes con los oficiales. Si bien podrían encontrar algunas diferencias (por ejemplo, marcas de tiempo o firmas digitales integradas), pueden analizarlas y verificar que no formen código malicioso.

¿Cómo puedo utilizar VeraCrypt en una unidad flash USB?

Tienes tres opciones:

1) Cifre toda la unidad USB. Sin embargo, no podrá ejecutar VeraCrypt desde... la unidad flash USB.
2) Cree dos o más particiones en su unidad flash USB. Deje la primera partición sin cifrar y cifre las demás. Puede almacenar VeraCrypt en la primera partición para ejecutarlo directamente desde la unidad flash USB.

Nota: Windows solo puede acceder a la partición principal de una unidad flash USB, sin embargo, las particiones adicionales siguen siendo accesibles a través de VeraCrypt.

3) Cree un contenedor de archivos VeraCrypt en la memoria USB (para más información, consulte el capítulo " Tutorial para principiantes"). Si deja suficiente espacio en la memoria USB (elija un tamaño adecuado para el contenedor VeraCrypt), también podrá almacenar VeraCrypt en la memoria USB (junto con el contenedor, no dentro del contenedor) y ejecutar VeraCrypt desde la memoria USB (consulte también el capítulo "Modo portátil").

¿VeraCrypt también cifra nombres de archivos y carpetas?

Sí. Todo el sistema de archivos de un volumen VeraCrypt está cifrado (incluidos los nombres de archivo, los nombres de carpeta y el contenido de cada archivo). Esto aplica a ambos tipos de volúmenes VeraCrypt: contenedores de archivos (discos virtuales VeraCrypt) y particiones/dispositivos cifrados con VeraCrypt.

¿VeraCrypt utiliza paralelización?

Sí. El aumento de la velocidad de cifrado/descifrado es directamente proporcional a la cantidad de núcleos/procesadores de su equipo. Para más información, consulte el capítulo "Paralelización" en la documentación.

¿Es posible leer y escribir datos en un volumen o unidad cifrados tan rápido como si la unidad no estuviera cifrada?

Sí, ya que VeraCrypt utiliza canalización y paralelización. Para más información, consulte los capítulos Canalización y Paralelización.

¿VeraCrypt admite el cifrado acelerado por hardware?

Sí. Para obtener más información, consulte el capítulo Aceleración de hardware.

¿Es posible arrancar Windows instalado en un volumen VeraCrypt oculto?

Sí, lo es. Para más información, consulte la sección «Sistema operativo oculto».

¿Podré montar mi volumen VeraCrypt en cualquier computadora?

Sí, los volúmenes de VeraCrypt son independientes del sistema operativo. Podrá montar su volumen de VeraCrypt en cualquier ordenador donde pueda ejecutar VeraCrypt (consulte también la pregunta "¿ Puedo usar VeraCrypt en Windows si no tengo privilegios de administrador?").

¿Puedo desconectar o apagar un dispositivo de conexión en caliente (por ejemplo, una unidad flash USB o un disco duro USB) cuando hay un volumen VeraCrypt montado en él?

Antes de desconectar o apagar el dispositivo, siempre debe desmontar primero el volumen VeraCrypt y luego ejecutar la operación "Expulsar" , si está disponible (haga clic derecho en el dispositivo en la lista "Equipo" o "Mi PC"), o usar la función "Quitar hardware de forma segura" (integrada en Windows, accesible desde el área de notificaciones de la barra de tareas). De lo contrario, podría perder datos.

¿Qué es un sistema operativo oculto?

Vea la sección Sistema operativo oculto.

¿Qué es la negación plausible?

Véase el capítulo Negación plausible.

¿Podré montar mi partición/contenedor VeraCrypt después de reinstalar o actualizar el sistema operativo?

Sí, los volúmenes de VeraCrypt son independientes del sistema operativo. Sin embargo, debe asegurarse de que el instalador de su sistema operativo no formatee la partición donde reside su volumen de VeraCrypt.

Nota: Si la partición o unidad del sistema está cifrada y desea reinstalar o actualizar Windows, primero debe descifrarla (seleccione Sistema > Descifrar permanentemente la partición o unidad del sistema). Sin embargo, un sistema operativo en ejecución puede actualizarse (parches de seguridad, Service Packs, etc.) sin problemas, incluso con la partición o unidad del sistema cifrada.

¿Puedo actualizar desde una versión anterior de VeraCrypt a la última versión sin ningún problema?

Generalmente sí. Sin embargo, antes de actualizar, lea las notas de la versión. Para todas las versiones de VeraCrypt publicadas desde la suya. Si existen problemas o incompatibilidades conocidos relacionados con la actualización de su versión a una más reciente, se detallarán en las notas de la versión.

¿Puedo actualizar VeraCrypt si la partición/unidad del sistema está cifrada o tengo que descifrarla primero?

Generalmente, puede actualizar a la última versión sin descifrar la partición/unidad del sistema (simplemente ejecute el instalador de VeraCrypt y se actualizará automáticamente en el sistema). Sin embargo, antes de actualizar, lea las notas de la versión. Para todas las versiones de VeraCrypt publicadas desde la suya. Si existen problemas o incompatibilidades conocidos relacionados con la actualización de su versión a una más reciente, se detallarán en las notas de la versión. Tenga en cuenta que esta pregunta frecuente también es válida para usuarios de sistemas operativos ocultos. Además, no puede degradar VeraCrypt si la partición o unidad del sistema está cifrada.

Uso autenticación previa al arranque. ¿Puedo evitar que un adversario que me esté vigilando mientras enciendo mi ordenador sepa que uso VeraCrypt?

Sí. Para ello, inicie el sistema cifrado, inicie VeraCrypt, seleccione Configuración > Cifrado del sistema, active la opción «No mostrar ningún texto en la pantalla de autenticación previa al arranque» y haga clic en Aceptar.
Al iniciar el ordenador, el gestor de arranque VeraCrypt no mostrará ningún texto (ni siquiera si introduce una contraseña incorrecta). El ordenador parecerá estar "bloqueado" mientras escribe su contraseña. Sin embargo, es importante tener en cuenta que si el atacante analiza el contenido del disco duro, aún podría descubrir que contiene el gestor de arranque VeraCrypt.

Uso autenticación previa al arranque. ¿Puedo configurar el cargador de arranque VeraCrypt para que muestre solo un mensaje de error falso?

Sí. Para ello, inicie el sistema cifrado, inicie VeraCrypt, seleccione Configuración > Cifrado del sistema, active la opción "No mostrar texto en la pantalla de autenticación previa al arranque" e introduzca el mensaje de error falso en el campo correspondiente (por ejemplo, el mensaje "Sistema operativo faltante" , que normalmente muestra el gestor de arranque de Windows si no encuentra ninguna partición de arranque). Sin embargo, es importante tener en cuenta que si el atacante analiza el contenido del disco duro, aún podría descubrir que contiene el gestor de arranque VeraCrypt.

¿Puedo configurar VeraCrypt para que se monte automáticamente cada vez que Windows inicie un volumen VeraCrypt que no sea del sistema y que use la misma contraseña que mi partición/unidad del sistema (es decir, mi contraseña de autenticación previa al arranque)?

Sí. Para ello, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic con el botón derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione “Agregar a favoritos del sistema”.
3. Debería aparecer la ventana Organizador de Favoritos del Sistema. En esta ventana, active la opción "Montar volúmenes favoritos del sistema al iniciar Windows" y haga clic en Aceptar.

Para obtener más información, consulte el capítulo 'Volúmenes favoritos del sistema'.

¿Se puede montar automáticamente un volumen cada vez que inicio sesión en Windows?

Sí. Para ello, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione “Agregar a favoritos”.
3. Debería aparecer la ventana Organizador de favoritos. En esta ventana, active la opción 'Montar el volumen seleccionado al iniciar sesión' y haga clic en Aceptar.

Luego, cuando inicie sesión en Windows, se le solicitará la contraseña del volumen (y/o los archivos de clave) y, si es correcta, se montará el volumen.

Como alternativa, si los volúmenes están alojados en particiones/dispositivos y no necesita montarlos en letras de unidad particulares cada vez, puede seguir estos pasos:

1. Seleccione Configuración > Preferencias. Debería aparecer la ventana Preferencias.
2. En la sección 'Acciones a realizar al iniciar sesión en Windows', habilite la opción 'Montar todos los discos'. volúmenes de VeraCrypt alojados en dispositivos y haga clic en Aceptar.

Nota: VeraCrypt no le solicitará una contraseña si ha habilitado el almacenamiento en caché de la contraseña de autenticación previa al arranque (Configuración > 'Cifrado del sistema') y los volúmenes usan la misma contraseña que la partición/unidad del sistema.

¿Se puede montar automáticamente un volumen cada vez que su dispositivo host se conecta a la computadora?

Sí. Por ejemplo, si tiene un contenedor de VeraCrypt en una unidad flash USB y desea que VeraCrypt lo monte automáticamente al insertar la unidad en el puerto USB, siga estos pasos:

1. Monte el volumen (en la letra de unidad en la que desea que se monte cada vez).
2. Haga clic derecho en el volumen montado en la lista de unidades en la ventana principal de VeraCrypt y seleccione “Agregar a favoritos”.
3. Debería aparecer la ventana Organizador de Favoritos. En esta ventana, active la opción "Montar el volumen seleccionado al conectar su dispositivo host" y haga clic en Aceptar.

Luego, cuando inserte la unidad flash USB en el puerto USB, se le solicitará la contraseña del volumen (y/o los archivos de claves) (a menos que esté almacenado en caché) y, si es correcta, se montará el volumen.

Nota: VeraCrypt no le solicitará una contraseña si ha habilitado el almacenamiento en caché de la contraseña de autenticación previa al arranque (Configuración > 'Cifrado del sistema') y el volumen usa la misma contraseña que la partición/unidad del sistema.

¿Se puede almacenar en caché mi contraseña de autenticación previa al arranque para poder usarla para montar volúmenes que no sean del sistema durante la sesión?

Sí. Seleccione ‘Configuración’ > ‘Cifrado del sistema’ y habilite la siguiente opción: ‘Almacenar en caché la contraseña de autenticación previa al arranque en la memoria del controlador’.

Vivo en un país que viola los derechos humanos fundamentales de sus ciudadanos. ¿Es posible usar VeraCrypt sin dejar rastros en Windows sin cifrar?

Sí. Esto se puede lograr ejecutando VeraCrypt en modo portátil bajo BartPE. o en un entorno similar. BartPE significa "Entorno Preinstalado de Bart", que es básicamente el sistema operativo Windows preparado para que pueda almacenarse completamente y arrancarse desde un CD/DVD (el registro, los archivos temporales, etc., se almacenan en la RAM; el disco duro no se utiliza en absoluto y ni siquiera es necesario que esté presente). El programa gratuito Bart's PE Builder Puede transformar un CD de instalación de Windows XP en un CD de BartPE. Tenga en cuenta que no necesita ningún complemento especial de VeraCrypt para BartPE. Siga estos pasos:

1. Cree un CD de BartPE e inícielo. (Nota: Debe realizar cada uno de los siguientes pasos) desde dentro de BartPE.)
2. Descargue el paquete autoextraíble de VeraCrypt al disco RAM (que BartPE crea automáticamente).

   Nota: Si el adversario puede interceptar los datos que envía o recibe a través de Internet y necesita evitar que el adversario sepa que descargó VeraCrypt, considere descargarlo a través de I2P, Tor o una red de anonimización similar.
3. Verifique las firmas digitales del archivo descargado (consulte la sección Firmas digitales) (para más información).

4. Ejecute el archivo descargado y seleccione Extraer (en lugar de Instalar) en la segunda página del Asistente de configuración de VeraCrypt. Extraiga el contenido al disco RAM.

5. Ejecute el archivo VeraCrypt.exe desde el disco RAM.

Nota: También puede considerar la creación de un sistema operativo oculto (consulte la sección Sistema operativo oculto) . Sistema operativo). Véase también el capítulo Negación plausible.

¿Puedo cifrar mi partición/unidad del sistema si no tengo un teclado estadounidense?

Sí, VeraCrypt es compatible con todas las distribuciones de teclado. Por exigencia de la BIOS, la contraseña de prearranque se escribe con la distribución de teclado estadounidense. Durante el proceso de cifrado del sistema, VeraCrypt cambia el teclado a la distribución estadounidense de forma automática y transparente para garantizar que la contraseña introducida coincida con la introducida en el modo de prearranque. Por lo tanto, para evitar errores de contraseña, se debe escribir la contraseña con las mismas claves que se usaron al crear el cifrado del sistema.

¿Puedo guardar datos en la partición del sistema señuelo sin correr el riesgo de dañar el sistema oculto? ¿dividir?

Sí. Puede escribir datos en la partición del sistema señuelo en cualquier momento sin riesgo de que se pierdan los datos ocultos. El volumen se dañará (porque el sistema señuelo no está instalado dentro de la misma partición) como el sistema oculto). Para más información, consulte la sección Sistema operativo oculto.

¿Puedo usar VeraCrypt en Windows si no tengo privilegios de administrador?

Ver el capítulo Usar VeraCrypt sin privilegios de administrador.

¿VeraCrypt guarda mi contraseña en un disco?

No.

¿Cómo verifica VeraCrypt que se ingresó la contraseña correcta?

Consulte el capítulo Detalles técnicos, sección Esquema de cifrado.

¿Puedo cifrar una partición/unidad sin perder los datos almacenados actualmente en ella?

Sí, pero se deben cumplir las siguientes condiciones:

- Si desea cifrar una unidad de sistema completa (que puede contener varias particiones) o una partición del sistema (en otras palabras, si desea cifrar una unidad o partición donde Windows está instalado), puede hacerlo siempre que utilice Windows XP o una versión posterior de Windows (como Windows 7) (seleccione 'Sistema' > 'Cifrar partición/unidad del sistema' y luego siga las instrucciones del asistente).
- Si desea cifrar una partición que no es del sistema, puede hacerlo siempre que contiene un sistema de archivos NTFS y que utiliza Windows Vista o una versión posterior de Windows (por ejemplo, Windows 7) (haga clic en 'Crear volumen') > 'Cifrar una partición que no sea del sistema' > 'Volumen estándar' > 'Seleccionar dispositivo' > 'Cifrar partición en el lugar' y luego siga las instrucciones del asistente).

¿Puedo ejecutar VeraCrypt si no lo instalo?

Sí, consulte el capítulo Modo portátil.

Algunos programas de cifrado usan TPM para prevenir ataques. ¿VeraCrypt también lo usará?

No. Estos programas usan TPM para protegerse contra ataques que requieren que el atacante tenga privilegios de administrador o acceso físico al equipo, y el atacante necesita que usted lo use después de dicho acceso. Sin embargo, si se cumple alguna de estas condiciones, es imposible proteger el equipo (ver más abajo) y, por lo tanto, debe dejar de usarlo (en lugar de confiar en TPM).

Si el atacante tiene privilegios de administrador, puede, por ejemplo, reiniciar el TPM, capturar el contenido de la RAM (que contiene las claves maestras) o el contenido de los archivos almacenados en volúmenes VeraCrypt montados (descifrados sobre la marcha), que luego pueden enviarse al atacante a través de Internet o guardarse en una unidad local sin cifrar (desde la que el atacante podría leerlos más tarde, cuando obtenga acceso físico a la computadora).

Si el atacante puede acceder físicamente al hardware de la computadora (y usted la usa después de dicho acceso), puede, por ejemplo, adjuntarle un componente malicioso (como un registrador de pulsaciones de teclas de hardware) que capturará la contraseña, el contenido de la RAM (que contiene claves maestras) o el contenido de los archivos almacenados en volúmenes VeraCrypt montados (descifrados sobre la marcha), que luego pueden enviarse al atacante a través de Internet o guardarse en una unidad local sin cifrar (desde la cual el atacante puede leerlos más tarde, cuando vuelva a obtener acceso físico a la computadora).

Lo único que TPM casi garantiza es una falsa sensación de seguridad (incluso el nombre mismo, "Módulo de Plataforma Segura", es engañoso y crea una falsa sensación de seguridad). En cuanto a la seguridad real, TPM es redundante (e implementar funciones redundantes suele ser una forma de crear el llamado bloatware). Este tipo de funciones a veces se denomina "teatro de seguridad" [6].

Para obtener más información, consulte las secciones Seguridad física y Malware.

¿Por qué Windows Vista (y versiones posteriores de Windows) me pide permiso para ejecutar VeraCrypt cada vez que lo ejecuto en modo "portátil"?

Al ejecutar VeraCrypt en modo portátil, este necesita cargar e iniciar el controlador de dispositivo. VeraCrypt necesita un controlador de dispositivo para proporcionar cifrado/descifrado transparente sobre la marcha, y los usuarios sin privilegios de administrador no pueden iniciar controladores de dispositivo en Windows. Por lo tanto, Windows Vista y versiones posteriores de Windows solicitan permiso para ejecutar VeraCrypt con privilegios de administrador.

Tenga en cuenta que si instala VeraCrypt en el sistema (en lugar de ejecutar VeraCrypt en modo portátil), no se le pedirá permiso cada vez que lo ejecute.

¿Tengo que desmontar los volúmenes de VeraCrypt antes de apagar o reiniciar Windows?

No. VeraCrypt desmonta automáticamente todos los volúmenes de VeraCrypt montados al apagar o reiniciar el sistema.

¿Qué tipo de volumen de VeraCrypt es mejor: partición o contenedor de archivos?

Los contenedores de archivos son archivos normales, por lo que puedes trabajar con ellos como con cualquier archivo normal (los contenedores de archivos se pueden, por ejemplo, mover, renombrar y eliminar de la misma manera que los archivos normales). Las particiones/unidades pueden tener mejor rendimiento. Tenga en cuenta que leer y escribir en un contenedor de archivos puede tardar mucho más si este está muy fragmentado. Para solucionar este problema, desfragmente el sistema de archivos donde se almacena el contenedor (cuando se desmonte el volumen VeraCrypt).

¿Cuál es la forma recomendada de realizar una copia de seguridad de un volumen VeraCrypt?

Consulte el capítulo Cómo realizar copias de seguridad de forma segura.

¿Qué pasará si formateo una partición de VeraCrypt?

Consulte la pregunta “¿Es posible cambiar el sistema de archivos de un volumen cifrado?” en estas preguntas frecuentes.

¿Es posible cambiar el sistema de archivos de un volumen cifrado?

Sí, una vez montados, los volúmenes VeraCrypt se pueden formatear como FAT12, FAT16, FAT32, NTFS o cualquier otro sistema de archivos. Los volúmenes VeraCrypt se comportan como dispositivos de disco estándar, por lo que puede hacer clic con el botón derecho en el icono del dispositivo (por ejemplo, en la lista "Equipo" o "Mi PC") y seleccionar "Formatear". Se perderá el contenido del volumen. Sin embargo, todo el volumen permanecerá cifrado. Si formatea una partición cifrada con VeraCrypt cuando el volumen VeraCrypt que aloja la partición no está montado, el volumen se destruirá y la partición dejará de estar cifrada (estará vacía).

¿Es posible montar un contenedor VeraCrypt almacenado en un CD o DVD?

Sí. Sin embargo, si necesita montar un volumen VeraCrypt almacenado en un medio de solo lectura (como un CD o DVD) en Windows 2000, el sistema de archivos dentro del volumen VeraCrypt debe ser FAT (Windows 2000 no puede montar un sistema de archivos NTFS en medios de solo lectura).

¿Es posible cambiar la contraseña de un volumen oculto?

Sí, el cuadro de diálogo para cambiar la contraseña funciona tanto para volúmenes estándar como ocultos. Simplemente escriba la contraseña del volumen oculto en el campo "Contraseña actual" del cuadro de diálogo "Cambiar contraseña de volumen".

Observación: VeraCrypt primero intenta descifrar el encabezado del volumen estándar y, si falla, intenta descifrar el área dentro del volumen donde podría estar almacenado el encabezado del volumen oculto (si existe un volumen oculto). Si tiene éxito, el cambio de contraseña se aplica al volumen oculto. (Ambos intentos utilizan la contraseña ingresada en el campo "Contraseña actual").

Cuando uso HMAC-RIPEMD-160, ¿el tamaño de la clave de cifrado del encabezado es solo de 160 bits?

No, VeraCrypt nunca utiliza la salida de una función hash (ni de un algoritmo HMAC) directamente como clave de cifrado. Consulte la sección " Derivación de claves de encabezado, sal y número de iteraciones" para obtener más información.

¿Cómo puedo grabar un contenedor VeraCrypt de más de 2 GB en un DVD?

El software de grabación de DVD que utilice debería permitirle seleccionar el formato del DVD. Si es así, seleccione el formato UDF (el formato ISO no admite archivos de más de 2 GB).

¿Puedo utilizar herramientas como chkdsk, Desfragmentador de disco, etc. en el contenido de un volumen VeraCrypt montado?

Sí, los volúmenes de VeraCrypt se comportan como dispositivos de disco físicos reales, por lo que es posible utilizar cualquier herramienta de verificación, reparación o desfragmentación del sistema de archivos en el contenido de un volumen de VeraCrypt montado.

¿VeraCrypt es compatible con versiones de 64 bits de Windows?

Sí.

¿Puedo montar mi volumen VeraCrypt en Windows, Mac OS X y Linux?

Sí, los volúmenes de VeraCrypt son totalmente multiplataforma.

¿Es posible instalar una aplicación en un volumen VeraCrypt y ejecutarla desde allí?

Sí.

¿Qué sucederá cuando una parte de un volumen de VeraCrypt se corrompa?

En datos cifrados, un bit dañado suele corromper todo el bloque de texto cifrado en el que se produjo. El tamaño de bloque de texto cifrado que utiliza VeraCrypt es de 16 bytes (es decir, 128 bits). El modo de operación de VeraCrypt garantiza que, si se produce corrupción de datos dentro de un bloque, los bloques restantes no se vean afectados. Consulte también la pregunta "¿Qué hago si el sistema de archivos cifrado de mi volumen VeraCrypt está dañado?".

¿Qué hago cuando el sistema de archivos cifrados en mi volumen VeraCrypt está dañado?

El sistema de archivos de un volumen VeraCrypt puede dañarse de la misma forma que cualquier sistema de archivos normal sin cifrar. En ese caso, puede usar las herramientas de reparación del sistema de archivos incluidas con su sistema operativo para solucionarlo. En Windows, se utiliza la herramienta "chkdsk" . VeraCrypt ofrece una forma sencilla de usar esta herramienta en un volumen VeraCrypt: haga clic con el botón derecho en el volumen montado en la ventana principal de VeraCrypt (en la lista de unidades) y, en el menú contextual, seleccione "Reparar sistema de archivos".

Usamos VeraCrypt en un entorno corporativo. ¿Hay alguna forma de que un administrador restablezca la contraseña de un volumen o la contraseña de autenticación previa al arranque si un usuario la olvida (o pierde un archivo de claves)?

Sí. Tenga en cuenta que VeraCrypt no tiene ninguna puerta trasera. Sin embargo, existe una forma de restablecer las contraseñas/archivos de claves de los volúmenes y las contraseñas de autenticación previa al arranque. Después de crear un volumen, haga una copia de seguridad de su encabezado en un archivo (seleccione Herramientas > Copiar encabezado de volumen) antes de permitir que un usuario no administrador lo use. Tenga en cuenta que el encabezado del volumen (que está cifrado con una clave de encabezado derivada de una contraseña/archivo de claves) contiene la clave maestra con la que se cifra el volumen. A continuación, pida al usuario que elija una contraseña y configúrela (Volúmenes > Cambiar contraseña de volumen); o genere un archivo de claves de usuario para él. Después, puede permitir que el usuario use el volumen y cambie la contraseña/archivos de claves sin su ayuda/permiso. En caso de que olvide su contraseña o pierda su archivo de claves, puede restablecer la contraseña/archivos de claves del volumen a su contraseña/archivos de claves de administrador original restaurando el encabezado del volumen desde el archivo de copia de seguridad (Herramientas > Restaurar encabezado de volumen).

De igual forma, puede restablecer una contraseña de autenticación previa al arranque. Para crear una copia de seguridad de los datos de la clave maestra (que se almacenarán en un disco de rescate VeraCrypt y se cifrarán con su contraseña de administrador), seleccione "Sistema" > "Crear disco de rescate". Para establecer una contraseña de autenticación previa al arranque, seleccione "Sistema" > "Cambiar contraseña". Para restaurar su contraseña de administrador, inicie el disco de rescate VeraCrypt, seleccione "Opciones de reparación" > "Restaurar datos de clave" e introduzca su contraseña de administrador. Nota: No es necesario grabar cada imagen ISO del disco de rescate VeraCrypt en un CD/DVD. Puede mantener un repositorio central de imágenes ISO para todas las estaciones de trabajo (en lugar de un repositorio de CD/DVD). Para obtener más información, consulte la sección " Uso de la línea de comandos" (opción /noisocheck).

¿Puede nuestra empresa comercial utilizar VeraCrypt de forma gratuita?

Siempre que cumpla con los términos y condiciones de la Licencia de VeraCrypt , Puede instalar y ejecutar VeraCrypt de forma gratuita en un número arbitrario de computadoras.

Compartimos un volumen en red. ¿Hay alguna forma de restaurar el recurso compartido de red automáticamente al reiniciar el sistema?

Consulte el capítulo Compartir en red.

¿Es posible acceder a un solo volumen de VeraCrypt simultáneamente desde múltiples sistemas operativos (por ejemplo, un volumen compartido a través de una red)?

Consulte el capítulo Compartir en red.

¿Puede un usuario acceder a su volumen VeraCrypt a través de una red?

Consulte el capítulo Compartir en red.

Cifré una partición que no es del sistema, pero su letra de unidad original aún aparece en la lista "Mi PC". Al hacer doble clic en ella, Windows me pregunta si quiero formatearla. ¿Hay alguna forma de ocultarla o liberarla?

Sí, para liberar la letra de unidad siga estos pasos:

1. Haga clic derecho en el ícono 'Equipo' (o 'Mi PC') en su escritorio o en el Menú Inicio y seleccione Administrar. Debería aparecer la ventana "Administración de equipos" .
2. En la lista de la izquierda, seleccione “Administración de discos” (dentro del subárbol Almacenamiento).
3. Haga clic derecho en la partición/dispositivo cifrado y seleccione “Cambiar letra de unidad y rutas”.
4. Haga clic en Eliminar.
5. Si Windows le solicita que confirme la acción, haga clic en Sí.

Cuando conecto mi unidad flash USB cifrada, Windows me pregunta si quiero formatearla.
¿Hay alguna manera de evitar eso?

Sí, pero deberá eliminar la letra de unidad asignada al dispositivo. Para obtener información sobre cómo...
Para ello, consulte la pregunta 'Encripté una partición que no es del sistema, pero su letra de unidad original aún está visible'.
en la lista 'Mi PC'.

¿Cómo elimino o deshago el cifrado si ya no lo necesito? ¿Cómo lo desactivo permanentemente?
¿descifrar un volumen?

Consulte la sección Cómo eliminar el cifrado.

¿Qué cambiará cuando habilite la opción 'Montar volúmenes como medios extraíbles'?

Consulte la sección Volumen montado como medio extraíble.

¿Tengo que “borrar” el espacio libre y/o los archivos en un volumen VeraCrypt?

Observación: "borrar" = borrar de forma segura; sobrescribir datos confidenciales para hacerlos irrecuperables.

Si cree que un adversario podrá descifrar el volumen (por ejemplo, que hará
revelas la contraseña), entonces la respuesta es sí. De lo contrario, no es necesario, porque la
El volumen está completamente cifrado.

¿Cómo sabe VeraCrypt qué algoritmo de cifrado ha sido utilizado en mi volumen VeraCrypt?
encriptado con?

Consulte la sección Esquema de cifrado (capítulo Detalles técnicos).

¿Cómo puedo realizar una copia de seguridad integrada de Windows en un volumen VeraCrypt? El volumen VeraCrypt no aparece en la lista de rutas de copia de seguridad disponibles.

La utilidad de copia de seguridad integrada de Windows solo busca el controlador físico, por lo que no muestra el volumen VeraCrypt. Sin embargo, aún puede hacer una copia de seguridad en un volumen VeraCrypt con un truco: active el uso compartido en el volumen VeraCrypt a través de la interfaz del Explorador (por supuesto, debe configurar los permisos correctos para evitar accesos no autorizados) y luego seleccione la opción "Carpeta compartida remota" (no es remota, por supuesto, pero Windows necesita una ruta de red). Allí puede escribir la ruta de la unidad compartida (por ejemplo, \\NombreServidor\nombreRecursoCompartido) y la copia de seguridad se configurará correctamente.

¿El cifrado utilizado por VeraCrypt es vulnerable a ataques cuánticos?

VeraCrypt utiliza cifrados de bloque (AES, Serpent, Twofish) para su cifrado. Los ataques cuánticos contra estos cifrados de bloque son simplemente un ataque de fuerza bruta más rápido, ya que el ataque más conocido contra estos algoritmos...

Es una búsqueda exhaustiva (los ataques a claves relacionadas son irrelevantes en nuestro caso, ya que todas las claves son aleatorias e independientes). Dado que VeraCrypt siempre utiliza claves aleatorias e independientes de 256 bits, garantizamos un nivel de seguridad de 128 bits contra algoritmos cuánticos, lo que hace que el cifrado de VeraCrypt sea inmune a dichos ataques.

¿Cómo hacer que un volumen VeraCrypt esté disponible para la indexación de búsqueda de Windows?

Para poder indexar un volumen de VeraCrypt mediante la Búsqueda de Windows, este debe montarse al arrancar (Favoritos del sistema) o reiniciar los servicios de Búsqueda de Windows después de montarlo. Esto es necesario porque la Búsqueda de Windows solo puede indexar las unidades disponibles al iniciarse.

Detalles técnicos

Notación

do	Bloque de texto cifrado
DK()	Algoritmo de descifrado mediante clave de cifrado/descifrado K
I()	Algoritmo de cifrado que utiliza la clave de cifrado/descifrado K
H()	Función hash
i	Índice de bloque para bloques de n bits; n depende del contexto
K	Clave criptográfica
PAG	Bloque de texto sin formato
^	Operación OR exclusiva bit a bit (XOR) Módulo 2 Además, donde n es el tamaño de bits del operando más a la izquierda y del valor resultante (por ejemplo, si el operando izquierdo es un valor de 1 bit y el operando derecho es un Valor de 2 bits, entonces: 1 0 = 1; 1 1 = 0; 1 2 = 1; 1 3 = 0; 0 0 = 0; 0 1 = 1; 0 2 = 0; 0 3 = 1) Multiplicación modular de dos polinomios sobre el campo binario GF(2) módulo $x^{128}+x^{7}+x^{2}+x+1$ (GF significa Campo de Galois)
||	Concatenación

Esquema de cifrado

Al montar un volumen VeraCrypt (suponiendo que no hay contraseñas/archivos de claves almacenados en caché) o al realizar la autenticación previa al arranque, se realizan los siguientes pasos:

1. Los primeros 512 bytes del volumen (es decir, la cabecera del volumen estándar) se leen en la RAM, de los cuales los primeros 64 bytes constituyen la sal (véase la Especificación del Formato de Volumen de VeraCrypt). Para el cifrado del sistema (véase el capítulo Cifrado del Sistema), los últimos 512 bytes de la primera pista de la unidad lógica se leen en la RAM (el gestor de arranque de VeraCrypt se almacena en la primera pista de la unidad del sistema o en el disco de rescate de VeraCrypt).

2. Los bytes 65536–66047 del volumen se leen en la RAM (véase la sección " Especificación del formato de volumen de VeraCrypt"). Para el cifrado del sistema, se leen los bytes 65536–66047 de la primera partición ubicada detrás de la partición activa* (véase la sección " Sistema operativo oculto"). Si hay un volumen oculto dentro de este volumen (o dentro de la partición detrás de la partición de arranque), se ha leído su encabezado; de lo contrario, se han leído datos aleatorios (para determinar si hay un volumen oculto, se debe intentar descifrar estos datos; para más información, consulte la sección " Volumen oculto").

3. VeraCrypt intenta descifrar el encabezado del volumen estándar leído en (1). Todos los datos utilizados Los datos generados durante el proceso de descifrado se guardan en la RAM (VeraCrypt nunca los guarda en el disco). Los siguientes parámetros son desconocidos† y deben determinarse mediante ensayo y error (es decir, probando todas las combinaciones posibles de los siguientes):

   a. PRF utilizada por la función de derivación de clave de encabezado (como se especifica en PKCS #5 v2.0; consulte la sección Derivación de clave de encabezado, sal y número de iteraciones), que puede ser una de las
   siguientes: HMAC-SHA-512, HMAC-SHA-256, HMAC-RIPEMD-160 o HMAC-Whirlpool. Si el usuario especifica explícitamente una PRF, se utilizará directamente sin probar las demás posibilidades.

   Una contraseña introducida por el usuario (a la que se pueden haber aplicado uno o más archivos de claves; consulte la sección Archivos de claves), un valor PIM (si se especifica) y la sal leída en (1) se pasan a la función de derivación de clave de encabezado, que genera una secuencia de valores (consulte la sección Derivación de clave de encabezado, sal y número de iteraciones) a partir de la cual se forman la clave de cifrado de encabezado y la clave de encabezado secundaria (modo XTS). (Estas claves se utilizan para descifrar el encabezado del volumen).

   b. Algoritmo de cifrado: AES-256, Serpent, Twofish, AES-Serpent, AES-Twofish-Serpiente, etc.

   c. Modo de funcionamiento: solo se admite XTS.

   d. Tamaño(s) de clave

---

* Si el tamaño de la partición activa es inferior a 256 MB, los datos se leen desde la segunda partición detrás de la activa (Windows 7 y posteriores, de forma predeterminada, no arrancan desde la partición en la que están instalados).

† Estos parámetros se mantienen en secreto no para aumentar la complejidad de un ataque, sino principalmente para que los volúmenes de VeraCrypt sean inidentificables (indistinguibles de datos aleatorios), lo cual sería difícil de lograr si estos parámetros se almacenaran sin cifrar en el encabezado del volumen. Tenga en cuenta también que si se utiliza un algoritmo de cifrado no en cascada para el cifrado del sistema, este se conoce (puede determinarse analizando el contenido del cargador de arranque de VeraCrypt sin cifrar, almacenado en la primera pista de la unidad lógica o en el disco de rescate de VeraCrypt).

4. El descifrado se considera exitoso si los primeros 4 bytes de los datos descifrados contienen el Cadena ASCII "VERA", y si la suma de comprobación CRC-32 de los últimos 256 bytes de los datos descifrados (encabezado del volumen) coincide con el valor del byte 8 de los datos descifrados (este valor es desconocido para un atacante porque está cifrado; consulte la sección " Especificación del formato de volumen de VeraCrypt"). Si no se cumplen estas condiciones, el proceso continúa desde (3), pero esta vez, en lugar de los datos leídos en (1), se utilizan los datos leídos en (2) (es decir, posible encabezado de volumen oculto). Si no se cumplen las condiciones, se finaliza el montaje (contraseña incorrecta, volumen dañado o volumen no VeraCrypt).

5. Ahora sabemos (o asumimos con gran probabilidad) que tenemos la contraseña, el algoritmo de cifrado, el modo, el tamaño de clave y el algoritmo de derivación de clave de encabezado correctos. Si desciframos correctamente los datos leídos en (2), también sabemos que estamos montando un volumen oculto y que su tamaño se obtiene de los datos leídos en (2) descifrados en (3).

6. La rutina de cifrado se reinicializa con la clave maestra principal* y la secundaria Clave maestra (modo XTS; consulte la sección "Modos de operación"), que se recupera del encabezado del volumen descifrado (consulte la sección " Especificación del formato de volumen de VeraCrypt"). Estas claves permiten descifrar cualquier sector del volumen, excepto el área del encabezado del volumen (o el área de datos de clave, para el cifrado del sistema), que se ha cifrado con las claves del encabezado. El volumen está montado.

Consulte también la sección Modos de operación y la sección Derivación de clave de encabezado, sal y recuento de iteraciones, y también el capítulo Modelo de seguridad.

* Las claves maestras se generaron durante la creación del volumen y no se pueden modificar posteriormente. El cambio de contraseña del volumen se realiza volviendo a cifrar el encabezado del volumen con una nueva clave de encabezado (derivada de una nueva contraseña).

Modos de operación

El modo de operación utilizado por VeraCrypt para particiones, unidades y volúmenes virtuales cifrados es XTS.

El modo XTS es en realidad el modo XEX [12], que fue diseñado por Phillip Rogaway en 2003, con una modificación menor (el modo XEX utiliza una sola tecla para dos propósitos diferentes, mientras que el modo XTS utiliza dos teclas independientes).

En 2010, el NIST aprobó el modo XTS para proteger la confidencialidad de los datos en dispositivos de almacenamiento [24]. En 2007, el IEEE también lo aprobó para la protección criptográfica de datos en dispositivos de almacenamiento orientados a bloques (IEEE 1619).

Descripción del modo XTS:

$$Ci = EK1 (Pi \oplus (EK2 (n) \alpha^{i})) \oplus (EK2 (n) a^{i})$$

Donde:

denota la multiplicación de dos polinomios sobre el campo binario GF(2) módulo $x^{128}+x^{7}+x^{2}+x+1$ K1 es la clave de cifrado (256 bits para cada cifrado compatible; es decir, AES, Serpent y Twofish)

K2 es la clave secundaria (256 bits para cada cifrado compatible, es decir, AES, Serpent y Twofish) i es el índice del bloque de cifrado dentro de una unidad de datos; para el primer bloque de cifrado dentro de una unidad de datos, i = 0 n es el índice de la unidad de datos dentro del alcance de K1; para la primera unidad de datos, n = 0 α es un elemento primitivo del campo de Galois (2128) que corresponde al polinomio x (es decir, 2)

El tamaño de cada unidad de datos es siempre de 512 bytes (independientemente del tamaño del sector).

Para obtener más información sobre el modo XTS, consulte, por ejemplo, [12] y [24].

Derivación de clave de encabezado, sal y recuento de iteraciones

La clave de encabezado se utiliza para cifrar y descifrar el área cifrada del encabezado del volumen VeraCrypt (por ejemplo, cifrado del sistema, del área de datos clave), que contiene la clave maestra y otros datos (véase la secciones Esquema de cifrado y Especificación del formato de volumen VeraCrypt). En volúmenes creados por VeraCrypt (y para el cifrado del sistema), el área está cifrada en modo XTS (consulte la sección Modos deOperación). El método que VeraCrypt utiliza para generar la clave de encabezado y la clave de encabezado secundaria (modo XTS) es PBKDF2, especificado en PKCS #5 v2.0; consulte Referencias.

Se utiliza sal de 512 bits, lo que significa que hay 2^{512} claves para cada contraseña. Esto reduce significativamente vulnerabilidad a ataques de diccionario "fuera de línea"/"tabla arco iris" (precomputación de todas las claves para un El diccionario de contraseñas es muy difícil cuando se utiliza una sal) [7]. La sal consiste en valores aleatorios generado por el generador de números aleatorios VeraCrypt durante el proceso de creación del volumen. El La función de derivación de claves de encabezado se basa en HMAC-SHA-512, HMAC-SHA-256, HMAC-RIPEMD-160 o HMAC-Whirlpool (véase [8, 9, 20, 22]); el usuario selecciona cuál. La longitud de la clave derivada...
La clave no depende del tamaño de la salida de la función hash subyacente. Por ejemplo, una clave de encabezado para el cifrado AES-256 siempre tiene 256 bits, incluso si se utiliza HMAC-RIPEMD-160 (en modo XTS, se utiliza una clave de encabezado secundaria adicional de 256 bits; por lo tanto, se utilizan dos claves de 256 bits para AES-256 en total). Para más información, consulte [7]. Se requiere un gran número de iteraciones de la función de derivación de claves para derivar una clave de encabezado, lo que aumenta el tiempo necesario para realizar una búsqueda exhaustiva de contraseñas (es decir, un ataque de fuerza bruta) [7].

Antes de la versión 1.12, VeraCrypt siempre utilizaba un número fijo de iteraciones según el tipo de volumen y el algoritmo de derivación utilizado:

- Para el cifrado de partición del sistema (cifrado de arranque), se utilizan 200000 iteraciones para la función de derivación HMAC-SHA-256 y 327661 iteraciones para HMAC-RIPEMD-160. • Para contenedores estándar y otras particiones, se utilizan 655331 iteraciones para HMAC-RIPEMD-160 y 500000 iteraciones para HMAC-SHA-512, HMAC-SHA-256 y HMAC-Whirlpool.

A partir de la versión 1.12, el PIM campo (Multiplicador de iteraciones personales) Permite a los usuarios tener más control sobre la cantidad de iteraciones utilizadas por la función de derivación de claves.
Cuando un PIM Si no se especifica el valor o es igual a cero, VeraCrypt utiliza los valores predeterminados expresados anteriormente.
Cuando un PIM El valor lo proporciona el usuario, el número de iteraciones de la función de derivación de clave se calcula de la siguiente manera:

- Para el cifrado de la partición del sistema (cifrado de arranque): Iteraciones = PIM x 2048
- Para contenedores estándar y otras particiones: Iteraciones = 15000 + (PIM x 1000)

Las claves de encabezado utilizadas por los cifrados en una cascada son mutuamente independientes, aunque se derivan A partir de una única contraseña (a la que se pueden haber aplicado archivos de claves). Por ejemplo, para la cascada AES-Twofish-Serpent, la función de derivación de clave de encabezado recibe instrucciones para derivar una clave de 768 bits. clave de cifrado a partir de una contraseña dada (y, para el modo XTS, además, un encabezado secundario de 768 bits) clave de la contraseña dada). La clave de encabezado de 768 bits generada se divide en tres claves de 256 bits. (para el modo XTS, la clave de encabezado secundaria también se divide en tres claves de 256 bits, por lo que la cascada en realidad utiliza seis claves de 256 bits en total), de las cuales la primera clave es utilizada por Serpent, la segunda clave es utilizada por Twofish, y el tercero por AES (además, para el modo XTS, la primera clave secundaria la utiliza Serpent, la segunda clave secundaria la utiliza Twofish y la tercera clave secundaria la utiliza AES).
Por lo tanto, incluso cuando un adversario tiene una de las claves, no puede usarla para derivar las otras claves, ya que no existe ningún método viable para determinar la contraseña de la que se derivó la clave (excepto ataque de fuerza bruta montado sobre una contraseña débil).

Generador de números aleatorios

El generador de números aleatorios (RNG) VeraCrypt se utiliza para generar la clave de cifrado maestra, la clave secundaria (modo XTS), la sal y los archivos de claves. Crea un conjunto de valores aleatorios en la memoria RAM. Este conjunto, de 320 bytes de longitud, contiene datos de las siguientes fuentes:

- Movimientos del ratón
- Pulsaciones de teclas
- Mac OS X y Linux: Valores generados por el RNG integrado (tanto /dev/random como /dev/urandom)
- Solo MS Windows: MS Windows CryptoAPI (recopilado regularmente en intervalos de 500 ms)
- Solo MS Windows: Estadísticas de interfaz de red (NETAPI32)
- Solo MS Windows: Varios controladores Win32, variables de tiempo y contadores (recopilados regularmente en intervalos de 500 ms)

Antes de escribir en el pool un valor obtenido de cualquiera de las fuentes mencionadas, se divide en bytes individuales (p. ej., un número de 32 bits se divide en cuatro bytes). Estos bytes se escriben individualmente en el pool mediante la operación de suma módulo 28 (sin reemplazar los valores antiguos) en la posición del cursor. Tras escribir un byte, la posición del cursor se avanza un byte. Cuando el cursor llega al final del pool, su posición se establece en el byte 16 escrito; la función de mezcla del pool es el inicio del pool. Después de cada byte, se aplica automáticamente a todo el pool (véase más adelante).

Función de mezcla de piscina

El propósito de esta función es realizar difusión [2]. La difusión distribuye la influencia de los bits de entrada individuales "sin procesar" sobre la mayor parte posible del estado del pool, lo que también oculta las relaciones estadísticas . El decimosexto byte escrito en el pool se aplica a todo el pool. Después de cada

Descripción de la función de mezcla del grupo: 1.

Sea R el grupo de aleatoriedad.

2. Sea H la función hash seleccionada por el usuario (SHA-512, RIPEMD-160 o Whirlpool). 3. l = tamaño en bytes de la salida de la función hash H (es decir, si H es RIPEMD-160, entonces l = 20; si H es SHA-512, entonces l = 64). 4. z = tamaño en bytes del conjunto de aleatoriedad R (320 bytes). 5. q = z / l – 1 (p. ej., si H es Whirlpool, entonces q = 4).

6. R se divide en bloques de 1 byte B0...Bq.

Para 0 ˜ i ˜ q (es decir, para cada bloque B) se realizan los siguientes pasos:

a. M = H (B0 || B1 || ... || Bq) [es decir, el conjunto de aleatoriedad se ha codificado utilizando la función hash H, que produce un hash M] b. Bi = Bi ^ M 7. R = B0 || B1 || ... || Bq

Por ejemplo, si q = 1, el grupo de aleatoriedad se mezclaría de la siguiente manera:

1. (B0 || B1) = R 2. B0 = B0 ^ H(B0 || B1)
3. B1 = B1 ^ H(B0 || B1)
4. R = B0 || B1

Valores generados

El contenido del grupo de RNG nunca se exporta directamente (ni siquiera cuando VeraCrypt le indica que genere y exporte un valor). Por lo tanto, incluso si el atacante obtiene un valor generado por el RNG, no le es posible determinar ni predecir (utilizando el valor obtenido) ningún otro valor generado por el RNG durante la sesión (es imposible determinar el contenido del grupo a partir de un valor generado por el RNG).

El RNG garantiza esto realizando los siguientes pasos cada vez que VeraCrypt le indica que genere y exporte un valor:

1. Los datos obtenidos de las fuentes enumeradas anteriormente se agregan al grupo como se describe anteriormente.
2. La cantidad solicitada de bytes se copia del grupo al búfer de salida (el proceso de copia comienza desde la posición del cursor del grupo; cuando se llega al final del grupo, la copia continúa desde el principio del grupo; si el número de bytes solicitado es mayor que el tamaño del grupo, no se genera ningún valor y se devuelve un error).
3. El estado de cada bit del grupo se invierte (es decir, 0 cambia a 1 y 1 cambia a 0).
4. Los datos obtenidos de algunas de las fuentes enumeradas anteriormente se agregan al grupo como se describe más arriba.
5. El contenido del pool se transforma mediante la función de mezcla de pools. Nota: Esta función utiliza una función hash unidireccional criptográficamente segura, seleccionada por el usuario (para más información, consulte la sección " Función de mezcla de pools" más arriba).
6. El contenido transformado del grupo se procesa mediante XOR en el búfer de salida de la siguiente manera:
    a. El cursor de escritura del búfer de salida se establece en 0 (el primer byte del búfer).
    b. El byte en la posición del cursor del pool se lee desde el pool y se aplica una operación XOR en el byte en el buffer de salida en la posición del cursor de escritura del buffer de salida.
    c. La posición del cursor del grupo avanza un byte. Si se llega al final del grupo, La posición del cursor se establece en 0 (el primer byte del grupo).
    d. La posición del cursor de escritura del búfer de salida avanza un byte.
    e. Los pasos b–d se repiten para cada byte restante del búfer de salida (cuya longitud es igual al número de bytes solicitado).
7. Se exporta el contenido del buffer de salida, que es el valor final generado por el RNG.

Orígenes del diseño

El diseño e implementación del generador de números aleatorios se basan en los siguientes trabajos: • Software Generation of Practically Strong Random Numbers de Peter Gutmann [10] • Cryptographic Random Numbers de Carl Ellison [11]

El archivo de claves de VeraCrypt es un archivo cuyo contenido se combina con una contraseña. El usuario puede usar cualquier tipo de archivo como archivo de claves de VeraCrypt. También puede generar un archivo de claves con el generador de archivos de claves integrado, que utiliza el RNG de VeraCrypt para generar un archivo con contenido aleatorio (para más información, consulte la sección " Generador de números aleatorios").

El tamaño máximo de un archivo de claves es ilimitado; sin embargo, solo se procesan sus primeros 1 048 576 bytes (1 MB) (los bytes restantes se ignoran debido a problemas de rendimiento asociados con el procesamiento de archivos extremadamente grandes). El usuario puede proporcionar uno o más archivos de claves (el número de archivos de claves es ilimitado).

Los archivos de claves se pueden almacenar en tokens de seguridad y tarjetas inteligentes compatibles con PKCS-11 [23] protegidos por múltiples códigos PIN (que se pueden ingresar usando un teclado PIN de hardware o a través de la GUI de VeraCrypt).

Los archivos de clave se procesan y se aplican a una contraseña mediante el siguiente método:

1. Sea P una contraseña de volumen de VeraCrypt proporcionada por el usuario (puede estar vacía)
2. Sea KP el conjunto de archivos de claves.
3. Sea kpl el tamaño del conjunto de archivos de claves KP, en bytes (64, es decir, 512 bits); kpl debe ser un múltiplo del tamaño de salida de una función hash H.
4. Sea pl la longitud de la contraseña P, en bytes (en la versión actual: 0 ˜ pl ˜ 64).
5. Si kpl > pl, añadir (kpl – pl) cero bytes a la contraseña P (por lo tanto, pl = kpl).
6. Llene el grupo de archivos de claves KP con bytes cero de kpl .
7. Para cada archivo de claves, realice los siguientes pasos: a. Coloque el cursor del archivo de claves al principio del grupo. b. Inicialice la función hash H. c. Cargue todos los bytes del archivo de claves uno por uno y, para cada byte cargado, realice los siguientes pasos: i. Genere un hash del byte cargado utilizando la función hash H sin inicializarlo, para obtener un hash intermedio (estado) M. No finalice el hash (el estado se conserva para la siguiente ronda). ii. Divida el estado M en bytes individuales.

   Por ejemplo, si el tamaño de salida del hash es de 4 bytes, (T0 || T1 || T2 || T3) = M iii. Escriba estos bytes (obtenidos en el paso 7.c.ii) individualmente en el grupo de archivos de claves mediante la operación de suma módulo 28 (sin reemplazar los valores antiguos del grupo) en la posición del cursor del grupo. Después de escribir un byte, la posición del cursor del grupo avanza un byte. Cuando el cursor llega al final del grupo, su posición se establece al principio del mismo.

8. Aplique el contenido del grupo de archivos de claves a la contraseña P mediante el siguiente método: a. Divida la contraseña P en bytes individuales B0...Bpl-1. Tenga en cuenta que si la contraseña era más corta que el conjunto de archivos de claves, se rellenó con cero bytes hasta la longitud del conjunto en el paso 5 (por lo tanto, en este punto, la longitud de la contraseña siempre es mayor o igual que la longitud del conjunto de archivos de claves). b. Divida el conjunto de archivos de claves KP en bytes individuales G0...Gkpl-1. c. Para 0 ˜ i kpl , realice: Bi = Bi Gi . d. P = B0 || B1 || ... || Bpl-2 || Bpl-1.

9. La contraseña P (después de aplicarle el contenido del grupo de archivos de claves) se pasa a la función de derivación de claves de encabezado PBKDF2 (PKCS #5 v2), que la procesa (junto con la sal y otros datos) mediante un algoritmo hash criptográficamente seguro seleccionado por el usuario (p. ej., SHA-512). Consulte la sección Derivación de claves de encabezado, sal y número de iteraciones para obtener más información.

La función hash H se limita a realizar la difusión [2]. Se utiliza CRC-32 como función hash H. Cabe destacar que la salida de CRC-32 se procesa posteriormente mediante un algoritmo hash criptográficamente seguro: el contenido del conjunto de archivos de claves (además de su hash mediante CRC-32) se aplica a la contraseña, que luego se pasa a la función de derivación de claves de encabezado PBKDF2 (PKCS #5 v2), que lo procesa (junto con la sal y otros datos) mediante un algoritmo hash criptográficamente seguro seleccionado por el usuario (p. ej., SHA-512). Los valores resultantes se utilizan para formar la clave de encabezado y la clave de encabezado secundaria (modo XTS).

PIM

PIM significa "Multiplicador de Iteraciones Personales". Es un parámetro introducido en VeraCrypt 1.12.
Y cuyo valor controla el número de iteraciones utilizadas por la función de derivación de claves de encabezado. Este valor se puede especificar mediante el cuadro de diálogo de contraseña o en la línea de comandos.

Si no se especifica ningún valor PIM, VeraCrypt utilizará el número predeterminado de iteraciones utilizadas en versiones anteriores a 1.12 (ver Derivación de clave de encabezado).

Cuando se especifica un valor PIM, el número de iteraciones se calcula de la siguiente manera:

- Para el cifrado del sistema: Iteraciones = PIM x 2048
- Para cifrado no sistémico y contenedores de archivos: Iteraciones = 15000 + (PIM x 1000)

Antes de la versión 1.12, la seguridad de un volumen de VeraCrypt solo se basaba en la fortaleza de la contraseña porque VeraCrypt utilizaba un número fijo de iteraciones.
Con la introducción de PIM, VeraCrypt cuenta con un espacio de seguridad bidimensional para volúmenes basado en la pareja de datos (Contraseña, PIM). Esto proporciona mayor flexibilidad para ajustar el nivel de seguridad deseado, a la vez que controla el rendimiento de la operación de montaje/arranque.

Uso de PIM

No es obligatorio especificar un PIM.

Al crear un volumen o al cambiar la contraseña, el usuario tiene la posibilidad de especificar un valor PIM marcando la casilla de verificación "Usar PIM", lo que a su vez hará que un campo PIM esté disponible en la GUI para que se pueda ingresar un valor PIM.

El PIM se considera un valor secreto que el usuario debe introducir cada vez junto con la contraseña. Si se especifica un valor PIM incorrecto, la operación de montaje/arranque fallará.

El uso de valores PIM altos genera una mejor seguridad gracias al mayor número de iteraciones, pero conlleva tiempos de montaje y arranque más lentos.
Con valores PIM pequeños, el montaje/arranque es más rápido, pero esto podría disminuir la seguridad si se utiliza una contraseña débil.

Durante la creación de un volumen o el cifrado del sistema, VeraCrypt fuerza el valor del PIM a ser mayor o igual a un valor mínimo cuando la contraseña tiene menos de 20 caracteres. Esta comprobación se realiza para garantizar que, en el caso de contraseñas cortas, el nivel de seguridad sea al menos igual al predeterminado de un PIM vacío.

El valor mínimo de PIM para contraseñas cortas es 98 para cifrado del sistema y 485 para cifrado no relacionado con el sistema y contenedores de archivos. Para contraseñas de 20 caracteres o más, el valor mínimo de PIM es 1. En todos los casos, dejar el PIM vacío o establecer su valor en 0 hará que VeraCrypt utilice el número alto de iteraciones predeterminado, como se explica en la sección " Derivación de claves de encabezado".

Las motivaciones detrás del uso de un valor PIM personalizado pueden ser:

- Agregue un parámetro secreto adicional (PIM) que un atacante tendrá que adivinar
- Aumente el nivel de seguridad mediante el uso de grandes valores PIM para frustrar el desarrollo futuro de ataques de fuerza bruta. ataques.

Acelerar el arranque o el montaje mediante el uso de un valor PIM pequeño (menos de 98 para el cifrado del sistema y menos de 485 para los demás casos)

Las capturas de pantalla a continuación muestran el paso para montar un volumen utilizando un PIM igual a 231:

Cambiar/borrar el PIM

El PIM de un volumen o del cifrado del sistema se puede cambiar o borrar mediante la función de cambio de contraseña. Las capturas de pantalla a continuación muestran un ejemplo de cómo cambiar el PIM del valor predeterminado vacío a un valor igual a 3 (esto es posible ya que la contraseña tiene más de 20 caracteres). Para... Para ello, el usuario debe primero marcar la casilla "Usar PIM" en la sección "Nuevo" para revelar el campo PIM.

Caso de volumen normal

Caso de cifrado del sistema

Especificación del formato de volumen de VeraCrypt

Compensar (bytes)	Tamaño (bytes)	Cifrado Estado*	Descripción
	64	Sin cifrar‡	Sal
0		Encriptado	Cadena ASCII “VERA”
64	4 2	Encriptado	Versión del formato del encabezado del volumen (2)
68	2	Encriptado	Versión mínima del programa requerida para abrir el volumen
70	4	Encriptado	Suma de comprobación CRC-32 de los bytes (descifrados) 256–511
72	16	Encriptado	Reservado (debe contener ceros)
76	8	Encriptado	Tamaño del volumen oculto (establecido en cero en no oculto)
92	8	Encriptado	volúmenes) Tamaño del volumen
100	8	Encriptado	Desplazamiento de bytes del inicio del ámbito de la clave maestra
108	8	Encriptado	Tamaño del área cifrada dentro del alcance de la clave maestra
116 124	4	Encriptado	Bits de bandera (bit 0 establecido: cifrado del sistema; bit 1 establecido: volumen no cifrado en el lugar del sistema; los bits 2 a 31 están reservados)
128		Encriptado	Tamaño del sector (en bytes)
132	4	Encriptado	Reservado (debe contener ceros)
252		Encriptado	Suma de comprobación CRC-32 de los bytes (descifrados) 64–251
256	120	Encriptado	Claves maestras primarias y secundarias concatenadas§
512	4 Var. 65024	Encriptado	Reservado (para el cifrado del sistema, este elemento se omite††)
65536	65536	Encriptado / Sin cifrar‡	Área para encabezado de volumen oculto (si no hay ninguno oculto) Volumen dentro del volumen, esta área contiene elementos aleatorios datos**). Para el cifrado del sistema, se omite este elemento.†† Ver bytes 0–65535.
131072	Nuestro.	Encriptado	Área de datos (ámbito de la clave maestra). Para el cifrado del sistema, El desplazamiento puede ser diferente (dependiendo del desplazamiento del sistema) dividir).
S–131072†	65536	Encriptado / Sin cifrar‡	Encabezado de respaldo (encriptado con una clave de encabezado diferente) derivado usando una sal diferente). Para el cifrado del sistema, †† este elemento se omite. Ver bytes 0–65535.
S–65536	65536	Encriptado / Sin cifrar‡	Encabezado de respaldo para volumen oculto (encriptado con un clave de encabezado diferente derivada usando una sal diferente). Si no hay ningún volumen oculto dentro del volumen, esta área contiene datos aleatorios.** Para el cifrado del sistema, este †† Se omite el elemento. Ver bytes 0–65535.

* Las áreas cifradas del encabezado del volumen se cifran en modo XTS mediante las claves de encabezado principal y secundaria. Para más información
Para obtener más información, consulte la sección Esquema de cifrado y la sección Derivación de clave de encabezado, sal y recuento de iteraciones.

† S denota el tamaño del volumen host (en bytes).

‡ Tenga en cuenta que no es necesario cifrar la sal, ya que no es necesario mantenerla en secreto [7] (la sal es una secuencia de valores aleatorios).

§ Aquí se almacenan varias claves maestras concatenadas cuando el volumen se cifra mediante una cascada de cifrados (claves maestras secundarias)
se utilizan para el modo XTS).

** Consulte a continuación en esta sección para obtener información sobre el método utilizado para llenar el espacio de volumen libre con datos aleatorios cuando el volumen es creado.

†† Aquí, el significado de "cifrado del sistema" no incluye un volumen oculto que contenga un sistema operativo oculto.

El formato de los volúmenes alojados en archivos es idéntico al de los volúmenes alojados en particiones o dispositivos (sin embargo, el encabezado del volumen, o datos clave, de una partición o unidad del sistema se almacena en los últimos 512 bytes de la primera pista lógica de la unidad). Los volúmenes VeraCrypt no tienen firma ni cadenas de identificación. Hasta que se descifran, parecen consistir únicamente en datos aleatorios.

El espacio libre en cada volumen VeraCrypt se llena con datos aleatorios al crearlo.* Los datos aleatorios se generan de la siguiente manera: Justo antes de que comience el formateo del volumen VeraCrypt, el generador de números aleatorios genera una clave de cifrado temporal y una clave secundaria temporal (modo XTS) (consulte la sección "Generador de números aleatorios"). El algoritmo de cifrado seleccionado por el usuario se inicializa con las claves temporales. A continuación, el algoritmo de cifrado se utiliza para cifrar bloques de texto plano compuestos por ceros. El algoritmo de cifrado funciona en modo XTS (consulte la sección "Generador de números aleatorios").
Volumen oculto). Los bloques de texto cifrado resultantes se utilizan para rellenar (sobrescribir) el espacio libre del volumen. Las claves temporales se almacenan en la RAM y se borran al finalizar el formateo.

Tenga en cuenta que esta especificación se aplica a los volúmenes creados con VeraCrypt 1.0b o posterior. El formato de los volúmenes alojados en archivos es idéntico al de los volúmenes alojados en particiones/dispositivos (sin embargo, el encabezado de volumen, o datos clave, de una partición/unidad del sistema se almacena en los últimos 512 bytes de la primera unidad lógica).
Los volúmenes de VeraCrypt no tienen firma ni cadenas de identificación. Hasta que se descifran, parecen consistir únicamente en datos aleatorios.

El espacio libre en cada volumen de VeraCrypt se llena con datos aleatorios cuando se crea el volumen. *
Los datos aleatorios se generan de la siguiente manera: Justo antes de que comience el formateo del volumen de VeraCrypt,
La clave de cifrado temporal y una clave secundaria temporal (modo XTS) se generan aleatoriamente.
generador de números (ver la sección Generador de números aleatorios). El algoritmo de cifrado que el
El usuario seleccionado se inicializa con las claves temporales. El algoritmo de cifrado se utiliza para...
Cifrar bloques de texto plano compuestos por ceros. El algoritmo de cifrado funciona en modo XTS (véase
la sección Modos de Operación). Los bloques de texto cifrado resultantes se utilizan para llenar (sobrescribir) el espacio libre.
Espacio en el volumen. Las claves temporales se almacenan en la RAM y se borran después del formateo.
acabados.

Los campos ubicados en el byte #0 (sal) y #256 (claves maestras) contienen valores aleatorios generados por el generador de números aleatorios (ver la sección Generador de números aleatorios) durante la creación del volumen proceso. Si un volumen de VeraCrypt aloja un volumen oculto (dentro de su espacio libre), el encabezado del El volumen oculto se encuentra en el byte n.° 65536 del volumen del host (el encabezado del host/volumen externo es ubicado en el byte n.° 0 del volumen del host (consulte la sección Volumen oculto). Si no hay ningún volumen oculto volumen dentro de un volumen VeraCrypt, bytes 65536–131071 del volumen (es decir, el área donde se encuentra el El encabezado de un volumen oculto puede contener datos aleatorios (consulte más arriba para obtener información sobre el método utilizado para llenar el espacio libre del volumen con datos aleatorios cuando se crea el volumen). El diseño de El encabezado de un volumen oculto es el mismo que el de un volumen estándar (bytes 0–65535).

El tamaño máximo posible del volumen de VeraCrypt es de 263 bytes (8 589 934 592 GB). Sin embargo, debido a Por razones de seguridad (con respecto al tamaño de bloque de 128 bits utilizado por los algoritmos de cifrado), El tamaño máximo de volumen permitido es 1 PB (1.048.576 GB).

---

* Siempre que las opciones Formato rápido y Dinámico estén deshabilitadas y que el volumen no contenga un sistema de archivos que haya sido cifrado en su lugar (tenga en cuenta que VeraCrypt no permite al usuario crear un volumen oculto dentro de dicho sistema). volumen).

Encabezados de copia de seguridad integrados

Cada volumen de VeraCrypt contiene un encabezado de copia de seguridad integrado, ubicado al final del volumen (ver arriba). Esta copia de seguridad del encabezado no es una copia del encabezado del volumen, ya que está cifrada con una clave de encabezado diferente, derivada con una sal distinta (ver la sección " Derivación de claves de encabezado, sal y número de iteraciones").

Cuando se modifican la contraseña del volumen y/o el PIM y/o los archivos de claves, o cuando se restaura el encabezado desde la copia de seguridad del encabezado integrado (o externo), tanto el encabezado del volumen como el encabezado de la copia de seguridad (integrado en el volumen) se vuelven a cifrar con claves de encabezado diferentes (derivadas mediante sales recientemente generadas: la sal para el encabezado del volumen es diferente de la sal para el encabezado de la copia de seguridad).
Cada sal es generada por el generador de números aleatorios de VeraCrypt (ver la sección Generador de números aleatorios).

Para obtener más información sobre las copias de seguridad del encabezado, consulte la subsección Herramientas > Restaurar encabezado de volumen en el capítulo Ventana principal del programa.

Cumplimiento de normas y especificaciones

Según nuestro conocimiento, VeraCrypt cumple con los siguientes estándares, especificaciones y recomendaciones:

- ISO/IEC 10118-3:2004 [21]
- FIPS 197 [3]
- FIPS 198 [22]
- FIPS 180-2 [14]
- FIPS 140-2 (XTS-AES, SHA-256, SHA-512, HMAC) [25]
- NIST SP 800-38E [24]
- PKCS #5 v2.0 [7]
- PKCS #11 v2.20 [23]

La exactitud de las implementaciones de los algoritmos de cifrado se puede verificar utilizando vectores de prueba (seleccione Herramientas > Vectores de prueba) o examinando el código fuente de VeraCrypt.

Código fuente

VeraCrypt es software libre y de código abierto. El código fuente completo de VeraCrypt (escrito en C, C++ y ensamblador) está disponible gratuitamente para revisión por pares en:

https://veracrypt.codeplex.com/SourceControl/latest https://
sourceforge.net/p/veracrypt/code/ci/master/tree/ https://github.com/
veracrypt/VeraCrypt https://bitbucket.org/
veracrypt/veracrypt/src

El código fuente de cada versión se puede descargar desde la misma ubicación que los binarios de la versión.

Desarrollo futuro

Para ver la lista de características planificadas para una versión futura, consulte: https://veracrypt.codeplex.com/wikipage?title=Future%20Development

Contacto

Puede contactarnos enviando un mensaje a veracrypt [at] idrix dot fr, que está asociado con la clave PGP del equipo VeraCrypt.
También puede utilizar la dirección veracrypt-contact [at] lists dot sourceforge.net.

Para contactar directamente con IDRIX, puede utilizar nuestro formulario de contacto.

Información legal

Licencia

El texto de la licencia bajo la cual se distribuye VeraCrypt está contenido en el archivo License.txt que se incluye en los paquetes de distribución del código fuente y binario de VeraCrypt.

Puede encontrar más información sobre la licencia en https://veracrypt.codeplex.com/wikipage?title=VeraCrypt%20License

Información de derechos de autor

Este software en su conjunto:

Partes de este software: Copyright

Para obtener más información, consulte los avisos legales adjuntos a partes del código fuente.

Información de marca registrada

Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos dueños.

Historial de versiones

1.18 (17 de agosto de 2016)

- Ventanas:
  - Soporte para cifrado de sistema EFI (limitaciones: sin sistema operativo oculto, sin arranque personalizado) mensaje)
  - Se corrige la vulnerabilidad de TrueCrypt que permite detectar la presencia de volúmenes ocultos (informado por Ivanov Aleksey Mikhailovich, alekc96 [at] mail dot ru)
  - Agregar soporte para el estándar de cifrado japonés Camellia, incluido el sistema cifrado.
  - Añadir soporte para los estándares de cifrado y hash rusos Kuznyechik, Magma y Streebog incluido para el cifrado del sistema EFI.
  - Añadir evaluación comparativa de algoritmos hash y PRF con PIM (incluso para prearranque).
  - Mover el sistema de compilación a Visual C++ 2010 para lograr una mejor estabilidad.
  - Solucione problemas de arranque en algunas máquinas aumentando la memoria requerida en 1 KiB
  - Solución alternativa para la compatibilidad con AES-NI en Hyper-V en Windows Server 2008 R2.
  - Protección mejorada contra ataques de secuestro de DLL.
  - Elimine correctamente el archivo del controlador veracrypt.sys durante la desinstalación en Windows de 64 bits.
  - Implementar el paso del PIN de la tarjeta inteligente como argumento de línea de comando (/tokenpin) cuando montar explícitamente un volumen.
  - Cuando no se especifica ninguna letra de unidad, elija A: o B: solo cuando no haya otra letra de unidad libre disponible.
  - Reducir el uso de CPU causado por la opción de deshabilitar el uso de la red desconectada unidades.
  - Agregar un nuevo mecanismo de identificación de volumen que se utilizará para identificar discos/particiones en lugar de sus Nombre del dispositivo.
  - Agregar opción para evitar la solicitud de PIM en la autenticación previa al arranque almacenando el valor de PIM sin cifrar en MBR.
  - Agregar opción y cambio de línea de comando para ocultar el diálogo de espera al ejecutar operaciones.
  - Agregue una casilla de verificación en la GUI del asistente "Formato VeraCrypt" para omitir la verificación del disco de rescate durante el procedimiento de cifrado del sistema.
  - Permitir arrastrar y soltar archivos cuando VeraCrypt se ejecuta como proceso elevado.
  - Correcciones menores de GUI y traducciones.

• Linux:

◦ Solucionar el problema de montaje en Fedora 23.

◦ Se corrige el error de montaje al compilar el código fuente usando gcc 5.x.

◦ Cumpla con la especificación de escritorio XDG utilizando XDG_CONFIG_HOME para determinar Ubicación de los archivos de configuración.

• Mac OSX:

◦ Resuelve el problema de compatibilidad con versiones más nuevas de OSXFuse.

1.17 (13 de febrero de 2016)

• Todos los sistemas operativos:

o Admite contraseñas UNICODE: ahora se aceptan todos los caracteres en las contraseñas (excepto el cifrado del sistema de Windows)

o Reduce el tiempo de montaje/arranque a la mitad gracias a una inteligente optimización de la derivación de claves (encontrado por Xavier de Carné de Carnavalet)

o Optimizar el código de Whirlpool mediante el uso de ensamblaje (ganancia de velocidad del 25 % en comparación con el código anterior).

o Agregar soporte para crear volúmenes exFAT.

o Agregar indicador GUI para la cantidad de aleatoriedad recopilada usando el mouse movimiento.

o Incluir nuevos iconos y gráficos aportados por Andreas Becker (http://www.andreasbecker.de)

• Ventanas:

o Se soluciona el problema de secuestro de dll que afecta al instalador que permite la ejecución de código con elevación de privilegio (CVE-2016-1281). Reportado por Stefan Kanthak (http://home.arcor.de/skanthak/)

o Firme binarios utilizando SHA-1 y SHA-256 para seguir las nuevas recomendaciones de Microsoft.

o Solucionar problemas en Comodo/Kaspersky al ejecutar una aplicación desde un Volumen de VeraCrypt (informado y corregido por Robert Geisler)

o Cargador de arranque: proteja la longitud de la contraseña/PIM rellenando los campos con la longitud máxima con '*' después de ENTER

o Resuelve el problema con los favoritos del sistema que no se pueden montar en la unidad A:

o Solucionar problemas de pérdida de foco después de mostrar el cuadro de diálogo de espera

- o Resuelve un problema poco común en el que algunas particiones estaban asociadas con un disco incorrecto en el cuadro de diálogo "Seleccionar dispositivo".

Implementar el almacenamiento en caché PIM, tanto para el cifrado del sistema como para los volúmenes normales. Añadir opciones para activarlo.

- o No intente montar utilizando contraseñas almacenadas en caché si la contraseña y/o el archivo de clave se especifican en la línea de comando.

- o Reescritura interna para hacer de VeraCrypt una aplicación UNICODE nativa.

- o Solución alternativa para evitar la detección de falsos positivos por parte de algún software antivirus.

Ocultar las unidades de red desconectadas en la lista de unidades disponibles. Añadir una opción para que estén disponibles para su montaje.

- o Solucionar el problema que provocaba que en algunos casos los archivos XML de configuración e historial se actualizaran incluso cuando no era necesario.

- o Se corrige la fuga de ruta de los archivos clave seleccionados en la RAM.

- o Se solucionó que la unidad TB no se pueda deseleccionar en VeraCryptExpander.

- o Agregue el atajo de teclado Alt+i para la casilla de verificación "Usar PIM".

- o Correcciones menores de GUI y traducciones.

• Linux/MacOSX:

- o Se solucionó el problema de la opción --stdin que no manejaba correctamente las contraseñas que contienen un espacio personaje (reportado y corregido por el usuario de Codeplex horsley1953).

- o Se soluciona el problema al crear volúmenes usando la línea de comandos con un sistema de archivos distinto de FAT.

- o Admite sufijos K/M/G/T para el interruptor --size para indicar la unidad a utilizar para el valor de tamaño.

1.16 (7 de octubre de 2015)

• Ventanas:

- o Modificar el parche para la vulnerabilidad CVE-2015-7358 para resolver los efectos secundarios en el administrador de montaje de Windows y al mismo tiempo hacer que sea muy difícil abusar del manejo de letras de unidad.

- o Se solucionó el error al restaurar el encabezado de volumen desde un archivo externo en algunas configuraciones.

- o Agregar opción para deshabilitar la detección del ataque "Evil Maid" para aquellos que se encuentran con ataques falsos. casos positivos (por ejemplo, problema con FLEXnet/Adobe).

- De forma predeterminada, no intente montar usando una contraseña vacía cuando el archivo de clave predeterminado Configurado o archivo de claves especificado en la línea de comandos. Se agregó una opción para restaurar el comportamiento anterior.

  Si es necesario montar con una contraseña vacía, especifíquelo explícitamente en la línea de comando usando: /p ""

1.15 (26 de septiembre de 2015)

- Ventanas:
  - Se corrigen dos vulnerabilidades de TrueCrypt informadas por James Forshaw (Proyecto Google Cero)
    - CVE-2015-7358 (crítico): elevación local de privilegios en Windows mediante el abuso del manejo de letras de unidad.
    - CVE-2015-7359: Elevación local de privilegios en Windows causada por Manejo incorrecto del token de suplantación.
  - Se corrige la regresión en el montaje de volúmenes favoritos al iniciar sesión el usuario.
  - Corregir la visualización de algunos idiomas Unicode (por ejemplo, chino) en el asistente de formato.
  - Establezca el foco del teclado en el campo PIM cuando "Usar PIM" esté marcado.
  - Permitir que la tecla de aplicación abra el menú contextual en la lista de letras de unidad
  - Admite la especificación del tamaño de los volúmenes en TB en la GUI (línea de comandos ya disponible apoya esto)

1.14 (16 de septiembre de 2015)

- Todos nosotros:
  - Enmascare y desenmascare el valor PIM en la GUI y el cargador de arranque como la contraseña.
- Ventanas:
  - Solucione el error de disco de rescate dañado al usar cifrados en cascada y SHA256 para cifrado del sistema.
  - Soluciona que la opción "Contraseña de caché en la memoria del disco" esté siempre deshabilitada incluso si marcado en preferencias
  - Se soluciona que el cambio de idioma de la interfaz de usuario no se tenga en cuenta para las nuevas instalaciones a menos que se cambie una preferencia.
  - Implementar la creación de contenedores de archivos mediante la línea de comandos.
  - Controlador: deshabilite el soporte de IOCTL_STORAGE_QUERY_PROPERTY de forma predeterminada y agregar opción para habilitarlo.

o Controlador: Admite la devolución de StorageDeviceProperty si
Se admite IOCTL_STORAGE_QUERY_PROPERTY.

o Admite la configuración de la etiqueta de volumen en el Explorador a través de la opción de montaje o etiqueta favorita
valor.

o Corrección del problema del cuadro de diálogo de asignación de teclas de acceso rápido donde siempre se muestra
OEM-233 y no se puede cambiar.

o Copie siempre los binarios ejecutables de 32 y 64 bits durante la instalación y en la configuración del disco Traveler.

Traveler Disk volverá a utilizar el exe de 32 bits de manera predeterminada, aunque también ofrecerá 64 bits.
bit.exe.

En Windows de 64 bits, ahora están disponibles los archivos exe de 32 bits (por ejemplo, si es necesario).
utilice dll PKCS#11 de 32 bits)

o Incluir expansor de volumen en la configuración del disco Traveler.

o No ofrezca la creación de un punto de restauración si está deshabilitado en Windows.

o Agregar posibilidad de verificar un archivo de imagen ISO de disco de rescate.

o Correcciones menores en el instalador, la GUI y el controlador.

1.13 (9 de agosto de 2015)

• Ventanas:

o Resuelve el bloqueo de TOR cuando se ejecuta desde un volumen VeraCrypt.

1.12 (5 de agosto de 2015)

• Todos los sistemas operativos:

o Implementar el “Modo Dinámico” mediante el soporte de un Multiplicador de Iteraciones Personales (PIM).

• Ventanas:

o Detectar la manipulación del cargador de arranque (ataques "Evil Maid") para el cifrado del sistema y
proponer opciones de recuperación.

o Detectar la manipulación del cargador de arranque (ataques "Evil Maid") para el cifrado del sistema y
proponer opciones de recuperación.

o Se solucionó el problema de desbordamiento del búfer y otros errores relacionados con la memoria al analizar el lenguaje.
Archivos XML.

o Reparar sectores defectuosos informados incorrectamente por chkdsk causados por un error en
Manejo de IOCTL_DISK_VERIFY.

o Se solucionó el problema de privacidad causado por los archivos de configuración e historial que se actualizaban
cada vez que se usa VeraCrypt (informado por Liran Elharar)

- o Se soluciona que los favoritos del sistema no siempre se monten después del arranque en frío.
- o Solucionar el error del instalador al actualizar VeraCrypt en Windows 10.
- o Implementar el descifrado de particiones/unidades que no sean del sistema.
- o Incluya archivos exe de 64 bits en el instalador e impleméntelos en máquinas de 64 bits para obtener un mejor rendimiento.
- o Permitir el uso de las letras de unidad A: y B: para montar volúmenes
- o Hacer que el análisis de argumentos de la línea de comandos sea más estricto y sólido (por ejemplo, /lz rechazado, debe ser /lz)
- o Agregar posibilidad de mostrar la contraseña de cifrado del sistema en la GUI de Windows y cargador de arranque
- o Solucionar el error "La clase ya existe" que les ocurría a algunos usuarios.
- o Solucionar algunos elementos del menú y campos de la GUI que no son traducibles
- o Hacer que los volúmenes informen correctamente el tamaño del sector físico a Windows.
- o Detectar correctamente las operaciones de desconexión de usuario/RDP para el desmontaje automático en sesiones bloqueadas.
- o Agregar selección manual de partición al reanudar el cifrado en el lugar.
- o Agregar opción de línea de comando (/cache f) para almacenar en caché temporalmente la contraseña durante el montaje de favoritos.
- o Agregue un cuadro de diálogo de espera para las operaciones de montaje automático de dispositivos para evitar que la GUI se congele.
- o Agregue información adicional al mensaje de error que se muestra para ayudar a analizar los problemas informados.
- o Deshabilitar la entrada del menú para cambiar el cifrado PRF del sistema ya que aún no está implementado.
- o Se solucionó el error al cambiar la contraseña cuando se requería UAC (heredado de TrueCrypt)
- o Correcciones y cambios menores (consulte el historial de Git para obtener más detalles)

• Linux:

- o Solucionar el problema del instalador en KDE cuando xterm no está disponible
- o Se corrigen las advertencias en los diálogos acerca de/LegalNotice cuando los wxWidgets se vinculan dinámicamente (N/A para binario oficial)
- o Admite nombres hash con '-' en la línea de comandos (sha-256, sha-512 y ripemd-160)

- Eliminar la opción "--current-hash" y agregar "--new-hash" para ser más coherente con las opciones existentes.

- Cuando solo se especifica el archivo clave en la línea de comandos, no intente montarlo usando un archivo vacío contraseña.

  Si es necesario realizar un montaje utilizando una contraseña vacía, especifíquelo explícitamente utilizando: -p

Para obtener una lista de cambios en versiones anteriores, consulte: https://veracrypt.codeplex.com/wikipage?title=Release%20Notas

Expresiones de gratitud

Nos gustaría agradecer a las siguientes personas:

El equipo de desarrolladores de TrueCrypt ha realizado un trabajo excepcional durante 10 años. Sin su arduo trabajo, VeraCrypt no existiría hoy.

A Paul Le Roux por poner a disposición su código fuente de E4M. TrueCrypt 1.0 se derivó de E4M y algunas partes de este código aún se incorporan a la última versión del código fuente de VeraCrypt.

Brian Gladman, quien escribió las excelentes rutinas AES, Twofish y SHA-512.

Peter Gutmann por su artículo sobre números aleatorios y por crear su cryptlib, que fue la fuente de partes del código fuente del generador de números aleatorios.

Wei Dai, quien escribió las rutinas Serpent, RIPEMD-160 y Whirlpool.

Tom St Denis, autor de LibTomCrypt, que incluye rutinas compactas SHA-256.

Mark Adler et al., quien escribió la rutina Inflate y la biblioteca Info-ZIP.

Los diseñadores de los algoritmos de cifrado, los algoritmos hash y el modo de operación: Horst Feistel, Don Coppersmith, Walt Tuchmann, Lars Knudsen, Ross Anderson, Eli Biham, Bruce Schneier, David Wagner, John Kelsey, Niels Ferguson, Doug Whiting, Chris Hall, Joan Daemen, Vincent Rijmen, Carlisle Adams, Stafford Tavares, Phillip Rogaway, Hans Dobbertin, Antoon Bosselaers, Bart Preneel, Paulo SLM Barreto.

Andreas Becker por el diseño del logotipo y los íconos de VeraCrypt.

Xavier de Carné de Carnavalet, quien propuso una optimización de velocidad para PBKDF2 que redujo el tiempo de montaje/arranque a la mitad.

kerukuro para la biblioteca cppcrypto (http://cppcrypto.sourceforge.net/) de donde se tomó la implementación del cifrado de Kuznyechik.

Lucian Wischik y Hans Dietrich, quienes crearon la biblioteca XZip-XUnzip.

A todos los demás que han hecho posible este proyecto, a todos los que nos han apoyado moralmente y a todos los que nos han enviado informes de errores o sugerencias para mejorarlo.

Muchas gracias.

Referencias

[1] Comité de Estados Unidos sobre Sistemas de Seguridad Nacional (CNSS), Política nacional sobre el uso del Estándar de cifrado avanzado (AES) para proteger los sistemas de seguridad nacional y la información de seguridad nacional, Política CNSS N.º 15, Hoja informativa N.º 1, junio de 2003, disponible en http://csrc.nist.gov/groups/STM/cmvp/documents/CNSS15FS.pdf.

[2] CE Shannon, Teoría de la comunicación de los sistemas secretos, Bell System Technical Journal, v. 28, n. 4 de 1949

[3] NIST, Estándar de cifrado avanzado (AES), Estándares federales de procesamiento de información Publicación 197, 26 de noviembre de 2001, disponible en http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[4] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, NIST, Informe sobre el desarrollo del estándar de cifrado avanzado (AES), 2 de octubre de 2000, Journal of Research of the National Institute of Standards and Technology, vol. 106, n.º 3, mayo-junio de 2001, disponible en http://nvl.nist.gov/pub/nistpubs/jres/106/3/j63nec.pdf.

[5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, Comentarios finales del equipo Twofish sobre la selección de AES, 15 de mayo de 2000, disponible en http://csrc.nist.gov/archive/aes/round2/comments/20000515-bschneier.pdf.

[6] Bruce Schneier, Más allá del miedo: pensar sensatamente sobre la seguridad en un mundo incierto, Springer, 2003

[7] RSA Laboratories, PKCS #5 v2.0: Estándar de criptografía basado en contraseñas, Datos RSA Security, Inc. Estándares de criptografía de clave pública (PKCS), 25 de marzo de 1999, disponible en http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-5-password-based-cryptography-standard.htm .

[8] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing para autenticación de mensajes, RFC 2104, febrero de 1997, disponible en http://www.ietf.org/rfc/rfc2104.txt.

[9] M. Nystrom, RSA Security, Identificadores y vectores de prueba para HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 y HMAC-SHA-512, RFC 4231, diciembre de 2005, disponible en http://www.ietf.org/rfc/rfc4231.txt.

[10] Peter Gutmann, Generación de software de números aleatorios prácticamente fuertes, presentado en Simposio de seguridad Usenix de 1998, disponible en http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix98.pdf.

[11] Carl Ellison, Números aleatorios criptográficos, originalmente un apéndice del estándar P1363, disponible en http://world.std.com/~cme/P1363/ranno.html.

[12] P. Rogaway, Instanciaciones eficientes de cifrados de bloque modificables y refinamientos de los modos OCB y PMAC, Asiacrypt 2004. LNCS vol. 3329. Springer, 2004. También disponible en: http://www.cs.ucdavis.edu/~rogaway/papers/offsets.pdf.

[13] J. Kelsey, Informe técnico n.° 7 de Twofish: Separación de claves en Twofish, comentario público de la segunda ronda de AES, 7 de abril de 2000

[14] NIST, Secure Hash Standard, FIPS 180-2, 1 de agosto de 2002, disponible en http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

[15] U. Maurer, J. Massey, Cifrados en cascada: la importancia de ser el primero, Journal of Criptología, vol. 6, n.º 1, 1993

[16] Bruce Schneier, Criptografía aplicada, segunda edición, John Wiley & Sons, 1996

[17] Peter Gutmann, Eliminación segura de datos de memoria magnética y de estado sólido, primera Publicado en las Actas del Sexto Simposio de Seguridad USENIX, San José, California, 22 al 25 de julio de 1996, disponible en http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

[18] Página de inicio de Serpent: http://www.cl.cam.ac.uk/~rja14/serpent.html.

[19] ME Smid, AES Issues, AES Round 2 Comments, 22 de mayo de 2000, disponible en http://csrc.nist.gov/archive/aes/round2/comments/20000523-msmid-2.pdf.

[20] A. Menezes, P. van Oorschot, S. Vanstone, Manual de criptografía aplicada, CRC Press, octubre de 1996

[21] Organización Internacional de Normalización (ISO), Tecnología de la información – Técnicas de seguridad – Funciones hash – Parte 3: Funciones hash dedicadas, ISO/IEC 10118-3:2004, 24 de febrero de 2004

[22] NIST, Código de autenticación de mensajes con clave hash (HMAC), Publicación 198 de las Normas Federales de Procesamiento de Información, 6 de marzo de 2002, disponible en http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

[23] RSA Laboratories, PKCS #11 v2.20: Estándar de interfaz de token criptográfico, RSA Security, Inc. Estándares de criptografía de clave pública (PKCS), 28 de junio de 2004, disponible en http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm . PDF disponible en http://www.cryptsoft.com/pkcs11doc/STANDARD/pkcs-11v2-20.pdf

[24] Morris Dworkin, Recomendación para modos de operación de cifrado de bloques: el modo XTS-AES para confidencialidad en dispositivos de almacenamiento, Publicación especial NIST 800-3E, enero de 2010, disponible en http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

[25] NIST, Funciones de seguridad aprobadas para FIPS PUB 140-2, Requisitos de seguridad para módulos criptográficos, 8 de octubre de 2010, disponible en http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

[25] TC 26 Funciones de seguridad aprobadas para FIPS PUB 140-2, Requisitos de seguridad para Módulos criptográficos, 8 de octubre de 2010, disponible en