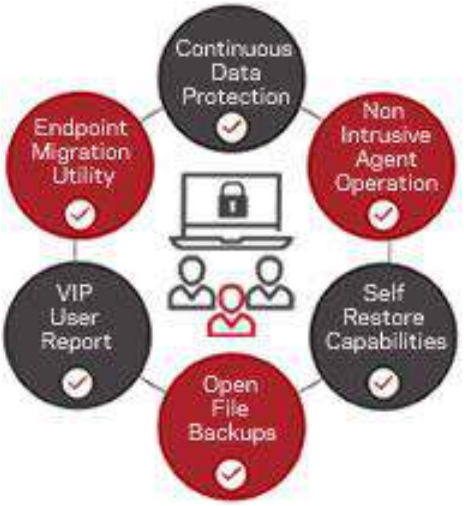
Veritas Desktop and Laptop Option

Veritas™ Desktop and Laptop Option es una solución de copia de seguridad, centrada en el usuario, que proporciona implementación flexible y administración centralizada para la copia de seguridad y la recuperación de equipos portátiles y de escritorios Windows y Mac de una organización. Esta solución altamente escalable al disponer de componentes distribuibles, es adecuada para entornos de cualquier tamaño y topología (una o varias ubicaciones, oficinas locales o remotas…) y permite implementar una protección continua hasta de los archivos más recientes de sus usuarios.

Entre las funciones integradas más importantes, se incluyen:

- La eliminación de datos duplicados en origen basada en el contenido de los archivos PST de Outlook o NSF.
- La selección automática de la red de interconexión para una experiencia de copia de seguridad no intrusiva, que permite cambiar entre los modos offline, online y backup por Internet.
- Capacidades de restauración delegada a través de agente, explorador web y aplicación móvil.
- Emisión automática de informes detallados.

Nota: Veritas DLO está orientado a proteger archivos de datos de usuario en equipos de escritorio. No está diseñado para proporcionar copias de seguridad completas del sistema.



Características clave

Copias de seguridad sin VPN a través de Internet

Selección automática de red que garantiza copias de seguridad sin interrupciones a través de Internet disponible conexión cuando las computadoras no están conectadas a la red corporativa.

Copias de seguridad incrementales

Realiza copias de seguridad solo de los cambios que se realizan en los archivos (incrementales), lo que garantiza la eficiencia en uso de la red y el almacenamiento.

Panel del administrador

Interfaz de usuario muy intuitiva que proporciona una visualización gráfica en tiempo real de los endpoints desde de punto de vista de operaciones, implementación y planificación de la capacidad.

Informe del estado de la copia de seguridad

Informe predictivo que permite a los administradores monitorizar el estado de las copias de seguridad en toda la organización pudiéndose además configurar para su generación automática periódica.

Rollback Restore

Capacidades de restauración mejoradas con posibilidad recuperación en un punto del pasado e informes detallados de actividad.

Alertas y Notificaciones

Proporciona a los administradores y usuarios específicos alertas y notificaciones detalladas con actualizaciones regulares del entorno de backup de los endpoitns.

Seguimiento de auditoría

Permite a las organizaciones el cumplimiento normativo al proporcionar registro de las acciones realizadas sobre el entorno de backup de los endpoints.

Utilidad de migración de los desktop

Facilita a los usuarios las actualizaciones del hardware de sus equipos con opciones para migrar efectivamente sus archivos de un equipo a otro.

Principales beneficios

Copias de seguridad no intrusivas automatizadas

Los equipos de escritorio y portátiles son protegidos automáticamente, independientemente de la conexión de red disponibles, sin necesidad de intervención del usuario.

Protección continua de datos

Copias de seguridad continuas con RPO de segundos e incluyendo soporte para documentos de trabajo en edición.

Implementación flexible

Componentes distribuibles para adaptarse a necesidades y tamaño de la organización con la capacidad de instalar de forma remota los agentes en equipos de escritorio y portátiles.

Estrategia de recuperación ante ransomware

Copia de seguridad altamente personalizable con configuraciones que garantizan un plan ante desastres contra amenazas tipo ransomware.

Administración centralizada

Consola de control centralizado con visualización gráfica de los entornos protegidos.

Seguridad y resistencia integradas

Cifrado AES de 256 bits integrado con verificaciones automáticas de integridad de datos y tolerancia a interrupciones.

Almacenamiento y copias de seguridad eficientes en la red

Capacidades integradas de deduplicación global de datos en origen y limitación de ancho de banda para ajustar el rendimiento de la copia de seguridad.

Informes automatizados

Informes detallados sobre los entornos protegidos con informes de estado predictivos que posibilitan una monitorización realmente efectiva.

Capacidades de restauración delegada

Capacite a los usuarios finales para navegar y restaurar sus archivos respaldados sin asistencia de soporte.

Acceso online a los archivos respaldados

Aplicación móvil para plataformas Ios y Android para acceso online a los ficheros respaldados.

Capacidades de recuperación

Las capacidades de recuperación se han diseñado teniendo en cuenta el aumento de los ataques de ransomware que están afectando a los equipos de escritorio de las organizaciones. La estrategia de protección contra ransomware consta de dos pilares fundamentales: en primer lugar, una correcta política de copias de seguridad que nos permita estar preparado para el ataque de ransomware y, en segundo lugar, las capacidades de restauración en caso de un ataque real.

En lo que respecta a las políticas de backups, la capacidad de copias programadas y automáticas y las capacidades de control de versiones de DLO, pueden aprovecharse para crear diferentes imágenes de los datos desde las cuales el cliente puede restaurar en un punto anterior al ataque del ransomware. DLO permite mantener versiones diarias de los ficheros pudiendo el administrador configurar un cierto número de días como ventana de recuperación (Windows Rollback). La última versión de cada día se mantendrá en la carpeta de datos del usuario.

En caso de un ataque, es posible que los archivos se cifren, lo cual tendrá como resultado un cambio de archivo del que se realizará una copia de seguridad. Por ello, es posible que el administrador quiera evitar que se realicen más copias de seguridad antes de proceder con las restauraciones, para lo cual se pueden usar las opciones de desactivación.

En lo referente a las capacidades de restauración, además de disponer de una interfaz de usuario simplificada e intuitiva, permiten realizar la recuperación de las últimas versiones disponibles de los archivos en una fecha determinada. Una vez completadas los procesos de restauración, se puede revisar el resumen detallado.

Nota: Estas capacidades de recuperación no son compatibles con versiones de DLO anteriores a 9.1. La configuración de la ventana de recuperación no se admite en para equipos Mac.

Lo nuevo de la versión 9.3.3

Panel de administrador mejorado

DLO ahora mejora el panel de gestión con un nuevo gráfico que proporciona una vista en tiempo real del porcentaje de finalización de la copia de seguridad, que ayuda a trazar el progreso de las copias de seguridad durante la fase de implementación.

Copia de seguridad adaptadas a Windows 10

DLO dispone de políticas de backup predefinidas donde se define una selección de carpetas de datos a proteger en línea con los nombres de las carpetas de usuario de Windows 10, lo que ayuda al administrador en la definición de las políticas de backup en este tipo de entornos.

Componentes de DLO

La arquitectura de DLO está formada por los siguientes componentes:

- Servidor de administración de DLO

- Consola de administración de DLO
- Servidor de mantenimiento de DLO
- Servidor de eliminación de datos duplicados de DLO
- Base de Datos de DLO
- Servidor perimetral de DLO
- Servidor IO de DLO
- Agente DLO (Desktop Agent)

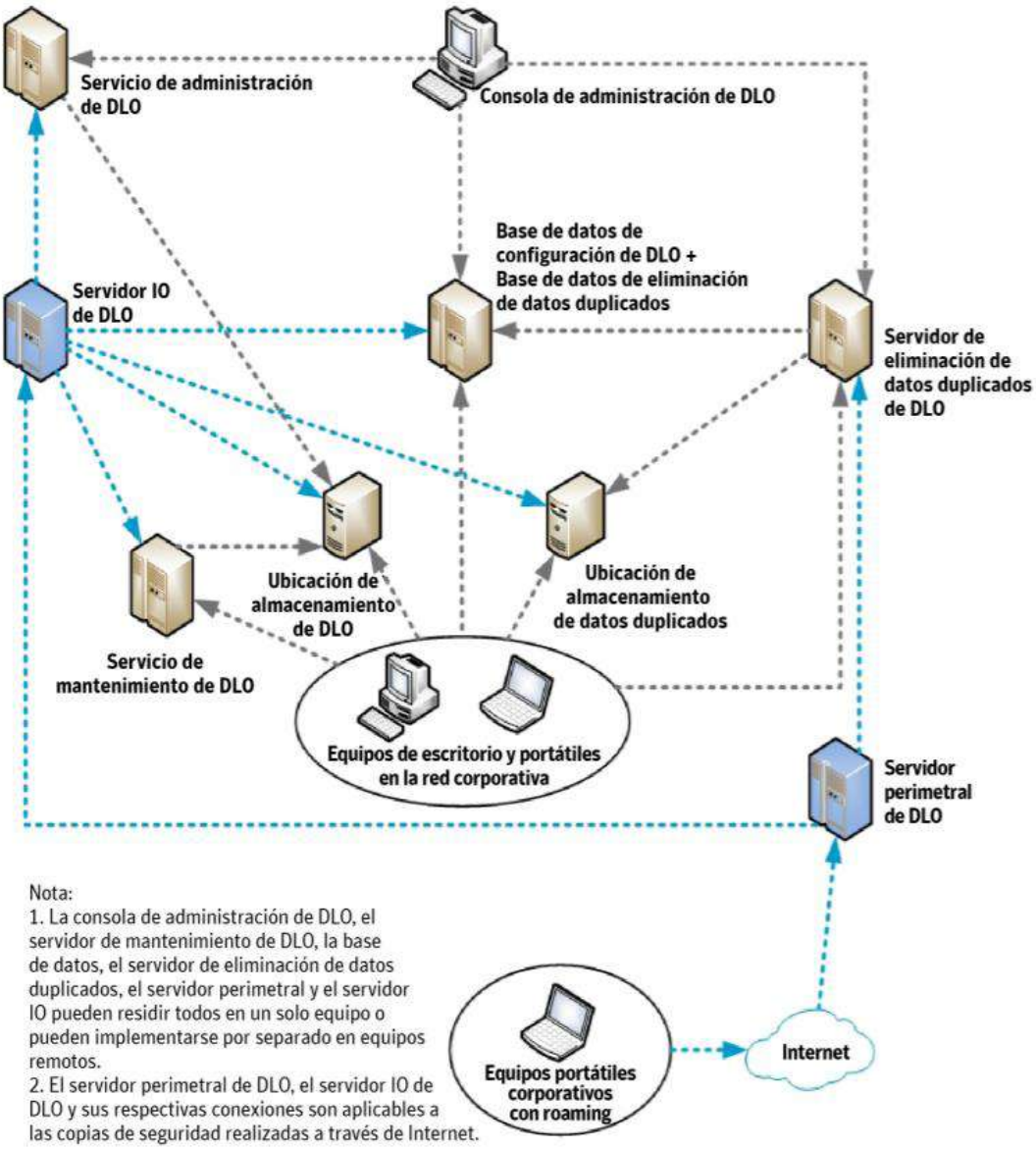


Figura 1-1 Componentes de Veritas Desktop and Laptop Option

Servidor de administración de DLO

El servidor de administración de DLO es un servicio que se ejecuta en segundo plano. El servidor de mantenimiento de DLO, las ubicaciones de almacenamiento (servidor de archivos) y la

Consola de administración de DLO pueden residir en el equipo donde está instalado el servidor de administración.

Consola de administración de DLO

La consola de administración de DLO es la interfaz gráfica de usuario desde la que el administrador puede realizar las siguientes tareas:

- Crear perfiles para grupos de usuarios o equipos. Los perfiles le permiten controlar el nivel de interacción del usuario del equipo de escritorio con Desktop Agent, definir los tipos de archivos de los que se pueden hacer copias de seguridad, definir la programación de las copias de seguridad y configurar las opciones adicionales para Desktop Agent.
- Crear carpetas de datos de usuario de la red. Las carpetas de datos de usuario de la red son ubicaciones de la red donde se almacenan los datos de equipos de escritorio.
- Crear asignaciones automáticas de usuarios que determinan la ubicación del almacenamiento de DLO y el perfil al que se asignan los usuarios cuando instalan Desktop Agent.

Nota: Las asignaciones automáticas de usuarios no se utilizan si los usuarios se agregan de forma manual a DLO.

- Agregar usuarios de forma manual a DLO. En lugar de utilizar las asignaciones de usuario automatizadas, puede agregar usuarios de forma manual a DLO y asignarles un perfil y una ubicación de almacenamiento de DLO. Esto resulta especialmente útil cuando ya existen recursos compartidos de red para almacenar datos de usuario. Los usuarios se pueden agregar de forma individual o se pueden agregar varios usuarios al mismo tiempo importando los nombres de usuario de una lista.
- Ver los archivos del registro de historial, recibir alertas y restaurar archivos a un equipo de escritorio desde la consola de administración.
- Configurar y administrar el servidor de eliminación de datos duplicados.
- Configurar y gestionar el servidor perimetral.

Servidor de mantenimiento de DLO

El servidor de mantenimiento se encarga de eliminar las revisiones antiguas de archivos delta que haya en las ubicaciones de almacenamiento. El servidor de mantenimiento solo hace falta si se activa la opción Transferencia de archivos delta, si bien se instala de forma predeterminada durante la instalación de DLO. Aunque es suficiente un servidor de mantenimiento, en infraestructuras grandes quizá resulte más eficaz contar con un servidor de mantenimiento por cada host de ubicación de almacenamiento (es decir, servidor de archivos).

Servidor de eliminación de datos duplicados

El servidor de eliminación de datos duplicados es un servicio web alojado en el servidor web Tomcat. Mantiene la tabla de hash global y ayuda a Desktop Agent a identificar los datos que ya existen en la ubicación de almacenamiento de datos duplicados.

El servidor de eliminación de datos duplicados también se puede instalar en el mismo servidor en el que se han instalado los demás componentes de DLO.

Pueden instalarse múltiples Dedupe Servers que pueden configurarse en DLO donde puede configurarse cada Ubicación de Almacenamiento con Soporte para Transacciones Duplicadas a nivel sitio.

Base de datos

La base de datos tiene dos componentes: la base de datos de DLO y la base de datos de eliminación de datos duplicados.

- Base de datos de DLO: La base de datos de DLO contiene detalles relacionados con la implementación de los componentes de DLO. Por ejemplo, dónde está instalada la base de datos (en un equipo remoto o host), dónde está el servidor de mantenimiento, etc.
- Base de datos de eliminación de datos duplicados: La base de datos de eliminación de datos duplicados es el almacenamiento de datos que utiliza el servidor de eliminación de datos duplicados para mantener la configuración relacionada con la eliminación de datos duplicados y la tabla hash global.

La base de datos de eliminación de datos duplicados siempre se instala en el mismo servidor que la base de datos de DLO en todas las configuraciones compatibles de DLO.

Servidor perimetral

Se trata de un servidor Web Apache que se utiliza para servidores de aplicaciones frontales, como servidores IO de DLO y servidores de eliminación de datos duplicados. Los servidores de aplicaciones residen en la red privada y sólo se puede acceder a través del servidor perimetral.

Desktop Agent se comunica con el servidor perimetral que, a su vez, se comunica con el servidor IO y el servidor de eliminación de datos duplicados de copia de seguridad y operaciones de restauración en caso de que el equipo con Desktop Agent instalado quede fuera de la red corporativa y esté conectado a cualquier otra red pública.

Es posible instalar varios servidores perimetrales en una configuración de DLO para el flujo optimizado de la copia de seguridad para usuarios de office distribuidos geográficamente conectados a través de internet.

Servidor IO

El servidor IO es un servicio web alojado en el servidor web Tomcat. Este componente es un servidor de aplicaciones que reside dentro de la red corporativa.

El servidor IO pone a disposición todos los recursos de DLO situados fuera de la red corporativa. Para acceder a la ubicación de almacenamiento en la red pública, debe asignarse al servidor IO. Varios servidores IO se pueden instalar en una configuración de DLO. Es posible asignar varios servidores IO Servers a un único servidor perimetral y varias ubicaciones de almacenamiento a un único servidor IO.

Desktop Agent

Desktop Agent reside en equipos de escritorio y portátiles que desea proteger. El nivel de interacción del usuario del equipo de escritorio con Desktop Agent puede variar según cómo haya configurado el administrador el perfil asignado al usuario. Desktop Agent puede ejecutarse en segundo plano, con lo que los archivos se protegen automáticamente.

Solicita ahora una prueba gratuita de 90 días