Veeam Backup & Replication

¿Novedades en la V11?

Veeam® Backup & Replication™ v11 proporciona una plataforma única una gestión de datos integral que sea lo suficientemente potente y flexible para proteger cada etapa del ciclo de vida de los datos, gestionando a un tiempo todas las complejidades de un entorno multi-cloud híbrido. A continuación, se incluye una lista con las nuevas características principales y mejoras añadidas en la V11.

Continuous Data Protection (CDP)

Elimine el tiempo de inactividad y reduzca la pérdida de datos para sus cargas de trabajo Tier 1 de VMware vSphere, y realice recuperaciones inmediatas al último estado o punto en el tiempo deseado con la funcionalidad de protección continua de datos (CDP) integrada, y consiga cumplir de esta forma los RTO y RPO más exigentes.

Entre los beneficios exclusivos de la implementación **CDP de Veeam** se incluyen:

- **Sin snapshots de VM —** Veeam CDP captures todo el tráfico E/S de escritura directamente en la ruta de datos con el *controlador de filtro de E/S certificado por VMware*, lo que elimina la necesidad de crear snapshots (instantáneas) de las VM del mismo modo que los trabajos de replicación tradicionales. Y con el seguimiento del nivel de E/S, solo se envían al sitio de DR los datos que realmente han cambiado, al contrario de lo que ocurre con los grandes bloques de disco virtual que devuelve la funcionalidad changed block tracking.
- **Sin dependencia de las cargas de trabajo o hardware —** Proteja CUALQUIER sistema operativo y aplicaciones que puedan ejecutarse en una VM de vSphere. Al contrario que con la replicación basada en el almacenamiento, Veeam CDP funciona con matrices de almacenamiento no coincidentes, soluciones de almacenamiento hiperconvergente e incluso almacenamiento local vSphere ESXi.
- **Replicación asincrónica —** Al contrario de la replicación sincrónica basada en cabinas de almacenamiento, Veeam CDP puede usarse a cualquier distancia y con un ancho de banda significativamente menor, gracias a la consolidación de E/S cuando el mismo bloque se sobrescribe varias veces y a la compresión del tráfico de la red.
- **Protección basada en políticas —** Al contrario que con los trabajos de replicación habituales, no tiene que preocuparse en absoluto de la programación. Simplemente defina el RPO necesario (pérdida de datos máxima permitida en caso de producirse un desastre) y la política CDP se ocupará de ejecutar los ciclos de sincronización que sean necesarios. Además, para reducir el spam de eventos en la monitorización, puede

El NUEVO Veeam Backup & Replication™ v11 elimina la pérdida de datos y el ransomware con un ahorro veinte veces mayor en sus costes de retención de archivos a largo plazo. La solución 4 en 1 que combina backup, replicación, snapshots de almacenamiento y la NUEVA protección de datos continua (Continuous Data Protection o CDP) bajo una única plataforma, proporciona protección de datos, recuperación y opciones de retención más flexibles y rápidas. La versión 11 proporciona un nivel de resiliencia sin precedentes para empresas de cualquier tamaño y ofrece más de 200 nuevas características y mejoras, que permiten:

- Eliminar la pérdida de datos con **Veeam CDP**
- Eliminar el ransomware con los backups inmutables en un repositorio **Linux reforzado (Hardened)**
- Eliminar el tiempo de parada con **Instant Recovery para NAS, Microsoft SQL y Oracle**
- Lograr un entorno de almacenamiento **archive-to-cloud a largo plazo con un coste más de veinte veces menor en AWS S3 Glacier y Azure Blob Archive**
- Unificar **la protección de cargas de trabajo nativas de la nube con AWS y Azure**
- Superar cualquier complejidad que encuentre en su camino con **los servicios BaaS y DRaaS con tecnología de Veeam**

Complemente **Veeam Backup & Replication v11** con la información, informes y visibilidad en profundidad que ofrece **Veeam ONE™ v11** en un paquete empresarial, **Veeam Availability Suite™ v11**, para dar respuesta a sus necesidades de protección y análisis.

Añada con **Veeam Disaster Recovery Orchestrator v4** la posibilidad de automatizar la recuperación del sitio y realización de pruebas, para generar una avanzada combinación que proporciona continuidad de negocio con orquestación a cualquier escala.

Entornos compatibles

Para acceder al listado de entornos compatibles, consulte las Notas de la versión del producto.

definir umbrales de incumplimiento de RPO aceptables de forma que cuando se produzcan problemas de conexión de forma esporádica no se traduzcan estos en las alarmas correspondientes.

- **Retención flexible —** Defina por separado la política de *retención a corto plazo*, que permite realizar restauraciones consistentes en cuanto a bloqueos a un punto del tiempo con granularidad del periodo de RPO, y la de *retención a largo plazo* con puntos de restauración periódicos opcionales coherentes con las aplicaciones, para ofrecer una capa adicional de protección.
- **Modelos de implementación flexible —** En función de la cantidad de datos protegidos, puede optar por proxies CDP virtuales o usar *proxies CDP físicos dedicados* para liberar por completo a sus hosts de vSphere de toda la carga de procesamiento de datos, y eliminar el impacto en su ratio de consolidación de VM. En cada caso, solo se necesita un proxy por clúster de vSphere, y los proxies adicionales proporcionan redundancia y un incremento en la escalabilidad.
  Nota: El proxy CDP es el nuevo rol que puede compartir un servidor con otros componentes de Veeam.
- **Asistente de implementación —** Una calculadora de implementación integrada elimina el trabajo de investigación fijándose en el historial de tráfico de E/S de todas las VMs seleccionadas para proteger en la política de CDP y estimar el ancho de banda necesario para lograr el RPO y evaluar si los recursos del proxy CDP disponible actualmente son suficientes para la tasa de cambio histórica.
- **Sin costes extras —** Veeam CDP se incluye en su licencia universal junto con los métodos de protección de datos para VMs de vSphere: backup o replicación basada en el host, backup basado en agentes, backup y snapshots de almacenamiento a nivel de aplicación. Igual que antes, *usar varios métodos de protección en la misma VM no consume licencias adicionales*. Ya no hay que seleccionar y escoger qué VMs hay que asignar a una costosa licencia CDP de un tercero. A partir de ahora, su creatividad con la planificación de la estrategia de DR estará únicamente limitada por el ancho de banda disponible.

NOTA: La funcionalidad de Veeam CDP requiere el despliegue del filtro de E/S para el clúster vSphere de origen y destino. Esto puede hacerse haciendo clic con botón derecho en recientemente añadida vista del árbol de clústers en la pestaña Backup Infrastructure (infraestructura de backup).

Veeam CDP está incluido en la licencia **Veeam Universal License.** Si se usa una licencia tradicional por socket, se necesita la edición **Enterprise *Plus***.

Repositorio reforzado o protegido

Mantenga sus backups a salvo en repositorios protegidos a prueba de malware y hackers, con backups inmutables que evitan el cifrado y borrado por parte del ransomware y personas malintencionadas. Esto puede conseguirse a través de las siguientes mejoras en los repositorios de backup de Linux:

- **Credenciales de un solo uso —** Las credenciales de un solo uso, que se necesitan para el repositorio reforzado (protegido), las suministra el usuario de forma interactiva en el momento inicial de la implementación y cuando se instalan las actualizaciones de producto, pero nunca se almacenan en la base de datos de configuración. Esto elimina cualquier posibilidad de que los hackers puedan extraer dichas credenciales desde un servidor de backup en compromiso y usarlas para conectarse al repositorio.
- **Sin dependencia del protocolo SSH —** El uso del protocolo SSH anterior se ha encapsulado en el protocolo de transporte ampliado. Como resultado, la conectividad SSH se requiere únicamente en el momento de la implementación inicial y cuando se instalan actualizaciones del producto. Esto permite a los clientes proteger SSH con la autenticación multifactor interactiva (MFA) o incluso desactivar el servidor SSH por completo para proteger su repositorio, incluso de la vulnerabilidades futuras de día cero.

- **Backups inmutables —** Olvídese de los borrados accidentales del backup, el ransomware y los hackers. Ahora puede hacer inmutables sus backups a nivel de imagen para el periodo de tiempo especificado con los backups GFS protegidos para la duración completa de su política de retención. Esta funcionalidad usa la característica de inmutabilidad de archivos nativa de Linux, que restringe la modificación y eliminación de los archivos con el correspondiente conjunto de marcadores (flags). El marcador solo puede eliminarlo un usuario con privilegios root, pero las credenciales de un solo uso aseguran que las credenciales root no se almacenen en el servidor de backup. Así que asegúrese de que no se guardan en ninguna otra aplicación y mantenga también vacía la lista del archivo sudoers.

  Por cuestiones de redundancia, la marca de tiempo (timestamp) de vencimiento de la inmutabilidad se almacena dos veces: 1) en el archivo especial de configuración y 2) en el atributo extendido de cada archivo de backup. El primero se amplía automáticamente a medida que se añaden puntos de restauración incrementales a la cadena de backup y también pueden aumentarse (pero nunca reducirse) de forma manual con fines de retención o suspensión legal usando PowerShell. La segunda marca de tiempo permanece como se definió originalmente, como consecuencia de ser una parte del archivo que ya es inmutable. La marca o flag de inmutabilidad es eliminada de archivo de backup solo cuando la hora local del servidor del repositorio supera *ambos* valores.

La V11 superó con éxito la evaluación de una entidad independiente en relación con el cumplimiento con las normativas reguladoras de la industria financiera de EE.UU. para el caso del almacenamiento WORM (Write Once Read Many). Una configuración de repositorio reforzado o protegido (hardened) conforme asegura la protección de los datos de backup frente a la manipulación y cumple con los requisitos de almacenamiento que impida la alteración y la eliminación de registros, según se especifica en las normativas SEC 17a-4(f), FINRA 4511(c) y CFTC 1.31(c)-(d). La evaluación de cumplimiento fue realizada por la empresa Cohasset Associates.

NOTA: Dado que no podemos dar soporte a ningún modo de backup que implique la modificación de los archivos de backup existentes en repositorios inmutables, esto limita su capacidad de elección al clásico backup incremental con backups completos periódicos. Esto hace de XFS el sistema de archivo ideal para este tipo de repositorios, gracias a la tecnología de respaldo synthetic full spaceless que ofrece nuestra avanzada integración de XFS (una característica de V10).

Soporte de almacenamiento de objetos ampliado

Reduzca los costes del archivado de datos a largo plazo hasta en veinte veces, reemplace la gestión de cinta manual y logre una gestión del ciclo de vida del backup de principio a fin con el soporte ampliado para almacenamiento de objetos caliente (hot) en el Capacity Tier y el soporte de almacenamiento de objetos frío (cold) en el NUEVO Archive Tier de Scale-Out Backup Repository™ (SOBR).

Para Capacity Tier y archivado de versiones de ficheros NAS, además de la amplia variedad de opciones disponibles, ahora puede usar **Google Cloud Storage (GCS)** como el repositorio de almacenamiento de objetos. La integración nativa se basa en el uso de la API de almacenamiento de objetos GCS propietaria, pero no es compatible con los backups inmutables por el momento, debido a la falta de funcionalidad object lock en GCS.

Para Archive Tier, estamos ofreciendo soporte de Archive Tier para **Amazon S3 Glacier** (incluido Deep Archive) y **Microsoft Azure Blob Storage** con el nuevo Archive Tier de SOBR. Al contrario del tipo de almacenamiento de objetos caliente en la nube, estos niveles más fríos son más adecuados y están ajustados para el caso de uso "Write Once Read Never" (escribir una vez, leer casi nunca) y por ello son idóneos para el archivado a largo plazo de backups GFS. Los costes significativamente más elevados de la API y recuperación, así como los tiempos de recuperación que se miden en horas, conducen a la creación del Archive Tier dedicado para asegurar una gestión del ciclo de vida del backup rentable, pero fluido.

A continuación, se enumeran las características clave de Archive Tier:

- **Backups inmutables —** Para ayudar en el cumplimiento de los requisitos normativos, en Amazon S3 Glacier, los backups archivados pueden hacerse inmutables de manera opcional para la duración completa de la política o directiva de retención.
- **Descarga basada en política —** De igual forma que con Capacity Tier, no hay trabajos de descarga que gestionar. Simplemente defina su ventana de archivado lo suficientemente alta para asegurase de que únicamente los puntos de restauración a los que probablemente no vuelva a acceder nuevamente (exceptuando circunstancias especiales), y siendo un almacenamiento inteligente definido por software el SOBR se ocupará del movimiento de datos por sí mismo en todos los niveles (tiers). Simplemente vigile el informe de estado de SOBR diario para cerciorarse de que todo está en verde.
- **Archivado rentable —** Debido al elevado costes de la API de los tiers de almacenamiento de objetos cold, los bloques de datos descargados se reempaquetan en objetos más grandes (hasta un tamaño de 512 MB) usando appliances de ayuda aprovisionados automáticamente en la nube pública para la duración de la sesión de archivado. Además, para evitar la penalización en caso de producirse una eliminación anticipada, omitimos automáticamente los puntos de restauración que les quede un periodo de retención por debajo de la duración mínima del almacenamiento de datos de la clase de almacenamiento utilizada.
- **Métodos de almacenamiento flexible —** Para reducir sus costes, la descarga del Archive Tier usa por omisión un enfoque siempre incremental donde solo se carga una delta desde el punto de restauración previo que se almacena para cada punto de restauración archivado. Sin embargo, para políticas de retención con periodos extremadamente largos, también proporcionamos una opción para almacenar cada backup completo GFS de forma independiente. Esto le permite evitar que la cadena de backup incremental abarque décadas, mientras mantiene sus costes generales dentro de un margen razonable mediante el uso de clases de almacenamiento como Amazon S3 Glacier Deep Archive.
- **Archivos autosuficientes —** Los backups archivados son autosuficientes y no dependen de ningún tipo de metadato externo, permitiéndose su importación incluso si el servidor de backup local se ha perdido. Es más, no existe bloqueo del proveedor (lock-in) porque los backups archivados pueden importarse desde el almacenamiento de objetos y restaurarse en cualquier punto futuro en el tiempo usando una instalación de Veeam Backup & Replication *Community Edition*, que no requiere de una licencia válida. En otras palabras, no mantenemos sus datos secuestrados.
- **Sin costes extra —** Al contrario de los proveedores de appliances de almacenamiento secundario que obviamente odian ver que los datos abandonen el costoso hardware de sus instalaciones, Veeam no cobra una suscripción por TB para el archivado de datos en almacenamiento de objetos. En otras palabras, ¡no cobramos una tasa por uso en la nube!

SOBR Archive Tier se incluye en la licencia **Veeam Universal License**. Si se usa una licencia tradicional por socket, se necesita la edición **Enterprise *Plus***.

Instant Recovery ampliado

Habilite la disponibilidad de más cargas de trabajo del centro de datos con la restauración sin problemas de las siguientes nuevas cargas de trabajo del pionero de Instant VM Recovery®:

- **Recuperación instantánea de bases de datos Microsoft SQL Server y Oracle** — ¿No se inicia la base de datos? ¿Los desarrolladores han borrado accidentalmente una tabla crítica? No hay problema Recupere cualquier base de datos desde el backup al estado más reciente o uno más alejado en el tiempo, a cualquier servidor de bases de datos de producción o clúster (físico o virtual) en cuestión de minutos con independencia de su tamaño.

  Las bases de datos seleccionadas están disponibles para las aplicaciones de producción y clientes de la base de datos al instante y pueden modificarse de forma normal preservando todos los cambios en la caché,

mientras el backup, obviamente nunca cambia. Veeam restaura automáticamente los archivos de bases de datos en segundo plano al almacenamiento de producción, y sigue sincronizando el estado de los archivos de base de datos actuales (modificados).

Para finalizar la recuperación, necesitará cambiar la base de datos para que esta se ejecute desde el almacenamiento de producción, algo que puede hacerse con una interrupción mínima, equivalente al tiempo de reiniciar simplemente la base de datos. Este cambio puede realizarse de manera manual o programarse para que se produzca de forma automática, tan pronto como se actualice la sincronización o durante la siguiente ventana de mantenimiento.

Al contrario de la funcionalidad interactiva Publish, la recuperación instantánea de la base de datos hace uso de una arquitectura basada en servicios, y no depende de la interfaz de usuario del Veeam Explorer™ en ejecución. Y si durante la recuperación al instante se reiniciara cualquier componente de la infraestructura de backup, el transportador de Instant Recovery se recupera automáticamente cuando todos los servidores necesarios vuelven a conectarse (en caso de que las interrupciones sean más largas de una hora, puede reanudar la recuperación instantánea manualmente usando la interfaz de usuario de Veeam Explorer).

La recuperación instantánea de bases de datos se incluye en la licencia **Veeam Universal License**. Si se usa una licencia tradicional por socket, se necesita la edición **Enterprise** o superior.

- **Publicación instantánea de backups de NAS —** ¿Ha perdido su NAS o su servidor de archivos? ¿Ha eliminado todo un recurso de archivos compartido por accidente? No hay problema. Simplemente publique recursos compartidos de archivos SMB desde el backup al estado más reciente, o a uno más alejado en el tiempo, en el servidor montado seleccionado, para permitir a sus usuarios acceder al instante a sus datos en este recurso compartido de archivos SMB temporal mientras soluciona el problema o restaura los datos.

  Otros casos de uso descubiertos por nuestros beta testers de la V11 involucran la habilitación de aplicaciones de terceros y scripts para acceder instantáneamente al contenido de cualquier backup de NAS con fines de data mining y otros escenarios de **reutilización de datos**, para evitar que se bloqueen archivos e impactar en su entorno de producción, gracias a la delegación de esta actividad en el hardware de almacenamiento de backup que normalmente se mantienen inactivo durante las horas de producción. Los prototipos fueron desarrollados por miembros de la comunidad especializados en los siguientes campos: Machine Learning (ML o aprendizaje automático), búsqueda de información de identificación personal (PII por sus siglas en inglés) para ayudar en los procesos de cumplimiento de normativa, y RGPD y detección de malware (análisis de seguridad automatizado de los archivos para malware durmiente con aplicaciones antivirus adicionales).

- **Recuperación al instante de CUALQUIER cosa a Microsoft Hyper-V —** V11 habilita casos de uso adicionales para la recuperación de datos y portabilidad, permitiéndole recuperar al instante CUALQUIER servidor físico, estación de trabajo, máquina virtual y backups de instancias en la nube a una VM de Microsoft Hyper-V, con independencia de qué producto de Veeam se utilizara para crear el backup. No se requiere curva de aprendizaje, ya que la recuperación simplemente funciona, gracias a la lógica de conversión P2V/V2V integrada, que habilita las restauraciones y migraciones con nuevos niveles de velocidad y flexibilidad y convierte el DR en la nube híbrida en una realidad.

  Dado que el servidor de backup de Veeam se ejecuta en Microsoft Windows, el host de Hyper-V es creado directamente en cada servidor de backup y está preparado y disponible para que lo use cualquiera. También ofrecemos soporte a Windows 10 Hyper-V como destino para esta funcionalidad, que en particular habilita a los proveedores de servicios gestionados (MSP) para crear appliances de DR de bajo coste todo en uno con tecnología de Veeam basados en Windows 10 para su implementación en los sitios de los clientes.

Otras mejoras

Además de las nuevas características antes mencionadas, la V11 incluye otras más de 200 mejoras como respuesta a los comentarios y sugerencias de clientes, y lo aprendido en el proceso de investigación y desarrollo en curso, de las cuales indicamos a continuación, las más significativas.

General

Motor de backup

V11 más que duplica el rendimiento del backup para las implementaciones de Veeam todo en uno en hardware de servidor de propósito general, permitiendo a los clientes superar la velocidad de backup de 11GB/s por nodo, siempre que la SAN y las cabinas de almacenamiento primarios puedan soportar el ritmo. Este importante salto de rendimiento se logra a través de varias mejoras orientadas a servidores y almacenamientos de clase empresarial:

- **Omisión de la caché del sistema —** Con la V11, los data movers de destino omitirán la caché del SO para asegurar que no interfiera con la caché del controlador y las avanzadas optimizaciones de E/S de los controladores RAID de clase empresarial, reduciendo ambos el uso de la CPU del repositorio de backup e incrementando el rendimiento hasta en un 50 %.
- **Escritura alineada —**Las escrituras no alineadas afectan al uso y rendimiento de la CPU de almacenamiento, por lo que la V11 lo evitan alineando cada bloque de datos del archivo de backup a un límite de 4KB. Esta característica está habilitada de forma predeterminada para repositorios recién creados y pueden habilitarse en masa en los repositorios existentes con el cmdlet Set-VBRBackupRepository. Para que el nuevo ajuste tenga efecto no es necesario un respaldo active full.
- **Mejora en el transporte de la memoria compartida —** A una velocidad de procesamiento de datos que se acerca a los 100 Gbps, incluso la velocidad de la moderna RAM empieza a marcar la diferencia para el rendimiento general del procesamiento de datos. La V11 optimiza las interacciones de memoria RAM, mejorando significativamente la velocidad a la que los datos pasan de la fuente a los data movers de destino cuando se ejecutan en el mismo servidor.
- **Reconocimiento de NUMA —** Para evitar la congestión del bus interno del tráfico cruzado de nodos NUMA, en servidores multiprocesador, los procesos dependientes deberían idealmente ubicarse en el mismo nodo. V11 implementa el reconocimiento completo de NUMA y garantiza que los data movers de origen y destino nunca acaben en nodos diferentes.
- **Mejoras de compresión óptimas —** Actualizamos la implementación de nuestro algoritmo de compresión por omisión, proporcionando una tasa de compresión ligeramente mejor y un desempeño de descompresión significativamente más rápido. Por ejemplo, la ejecución de una consulta SQL que devuelve 30 GB de datos frente a una base de datos Stack Overflow ejecutándose en una VM recuperada al instante ahora requiere de un 28 % menos de tiempo comparado con la V10.
- **Mejoras del programador de recursos —** Hemos aplicado numerosas optimizaciones a nuestro programador de recursos de la infraestructura de backup, reduciendo el tiempo que necesita para publicar el recurso hasta en un 50 %, lo que acelera de manera significativa el tiempo de inicio del trabajo de backup. La mejora debería sentirse especialmente significativa en entornos con un número grande de proxies de backup y extensiones SOBR.

Motor de restauración

Tras recibir numerosos comentarios positivos al añadir nuestra avanzada tecnología de búsqueda de datos a la funcionalidad de exportación completa de cinta virtual en los repositorios de backup basados en Windows en la V10, hemos extendido este motor a los repositorios basados en Linux. Además, ahora la estamos usando para TODAS las características y funcionalidades que leen contenido de archivos de backup desde los repositorios de Veeam. Las mejoras más importantes deberían observarse en el hardware de almacenamiento de nivel empresarial y en la funcionalidad que involucre un movimiento masivo de datos, como restauraciones completas de imagen, copias de backup, descargas de almacenamiento de obejtos, etc.

PowerShell

- **Módulo PowerShell —** Debido a la gran demanda del público, cambiamos del complemento de PowerShell al módulo Powershell, que puede usarse en cualquier máquina con la consola de backup instalada. Tampoco se necesita tener instalado PowerShell 2.0 en el servidor de backup, que es algo con lo que muchos clientes tenían problemas.
- **Nuevo cmdlet PowerShell —** V11 añade 184 nuevos cmdlets para la nuevas funcionalidades añadidas y la ampliación de cobertura de las características existentes, centrándose particularmente en la funcionalidad de restauración.

API RESTful

- **API RESTful para el servidor de backup —** Nuestra API RESTful de Veeam Backup Enterprise Manager muestra la funcionalidad disponible solo en la interfaz de usuario Web de EM, con lo que ahora también añadimos la API RESTful al mismo servidor de backup, donde nos centraremos en las necesidades de gestión del servidor de backup más comunes. V11 proporciona la nueva API REST para abordar los casos de uso más comunes de nuestros clientes y partners, que incluye la gestión de los trabajos de backup y de la infraestructura y la importación/exportación en masa para una implementación simplificada y migración de las infraestructuras y trabajos de backup. Para ayudarnos a priorizar funcionalidades, deje sus comentarios en los Foros R&D (I+D) indicando qué es lo siguiente que le gustaría que se contemplara.

  La API RESTful está incluida en la licencia **Veeam Universal License**. Si se usa una licencia tradicional por socket, se necesita la edición **Enterprise *Plus***.

Seguridad

- **Cumplimiento con FIPS —** V11 usa módulos de cifrado compatibles con FIPS también en la compilación del producto base. De manera predeterminada, el modo de operaciones conforme con FIPS está desactivado para permitir el procesamiento de las versiones de la plataforma antiguas donde la interacción conforme con FIPS no es posible (como las versiones de VMware vSphere previas a la 6.5 debido a su dependencia con las versiones de VDDK no conformes con FIPS), así como para evitar el impacto en el rendimiento de las comprobaciones de integridad del módulo en tiempo real requeridas por la certificación FIPS. Puede activar el modo de operación conforme con FIPS en la pestaña Security de Global Options (opciones globales).

Backup

Procesamiento con reconocimiento de aplicaciones

- **Agente invitado (guest) persistente —** Ahora puede usar de manera opcional un agente persistente para VMs Windows implementando uno a través de la directiva de grupo (Group Policy) o su herramienta de distribución de software estándar. Este enfoque reduce el consumo de puertos de red a tan solo unos pocos puertos estáticos (dependiendo de la funcionalidad usada) y facilita los requisitos de privilegios para superar el control de cuentas de usuario (UAC) para desplegar un proceso en tiempo real en el guest,

a la vez que reduce el tráfico de red y el tiempo de procesamiento del guest. Solo necesita distribuirse un diminuto componente instalador a los guests; el resto de los componentes se desplegará (y se mantendrá actualizado) automáticamente.

- **Integración de SQL Server —** El motor de procesamiento con reconocimiento de aplicaciones ahora usará el proveedor nativo MSOLEDBSQL si está disponible en servidor SQL, habilitando el procesamiento de los servidores SQL forzando TLS 1.2 sin necesidad de editar el registro. Además, las preferencias de backup de las bases de datos para los grupos de alta disponibilidad (HA) ahora se respetarán.
- **Visibilidad mejorada en la protección de bases de datos SQL —** La nueva opción experimental para SQL Serve le permite suspender la sesión de backup a nivel de imagen si el backup del log de transacción no puede inicializarse o si no se encuentran bases de datos SQL. Use el valor de registro *AAIPSQLShowExperimentalOptions* (DWORD, 1en el servidor de backup para hacer visible la correspondiente casilla de verificación en los ajustes de procesamiento con reconocimiento de aplicaciones. Deje sus comentarios sobre esta nueva opción en los foros R&D (investigación y desarrollo).

Trabajos de backup

- **Trabajos de alta prioridad —** Ahora puede designar algunos trabajos de backup como de alta prioridad. Estos trabajos colocarán sus tareas pendientes en la cola dedicada del programador de recursos que se ofrece para los recursos de la infraestructura de backup antes de la cola usada para los trabajos de prioridad normal. Use este ajuste para los trabajos de backup que protegen cargas de trabajo para las que es importante la hora de inicio de sus backups o para trabajos periódicos con requisitos de RPO exigentes.
- **Retención GFS en segundo plano —** La retención de backup completo GFS es ahora procesada de forma independiente a la ejecución del backup como una actividad del sistema en segundo plano en el repositorio de Veeam. Esto asegura que los backups completos vencidos no seguirán consumiendo espacio de disco en el repositorio si el trabajo de backup se desactiva para periodos de tiempo ampliados.
- **Retención de backups GFS huérfanos —** La política de retención se aplica ahora a los backups GFS que ya no tienen un trabajo asociado, basándose en la última política de retención conocida. Esto elimina la necesidad de buscar soluciones alternativas, como la de mantener trabajos que ya no son necesarios, protegiendo una única máquina ficticia.
- **Mejoras en la retención de VM eliminadas —** La retención de VM eliminadas ya no se aplicará más si el trabajo de backup no pudo crear la lista de máquinas procesadas para evitar eliminaciones de backups causadas por problemas temporales de la infraestructura.

Trabajos de copia de backup

Los trabajos de copia de backup ahora usan la misma lógica de retención GFS que los trabajos de backup primario. Esto garantiza la consistencia en todo el producto y habilita la compatibilidad con las nuevas características, como los backups inmutables del repositorio protegido (hardened) o la retención de backups GFS en segundo plano. Específicamente, esto implica los siguientes cambios:

- **Retención GFS basada en tiempo —** La retención GFS para la copia de backup ahora se basa en el tiempo, en lugar de en el número de puntos de restauración en cada generación. Esto garantiza que los puntos de restauración de GFS no se mantendrán por menos tiempo del necesario, incluso en el caso de la creación de un backup GFS manual por accidente.
- **Momento de creación de backups completos GFS —** Lo backups completos GFS ahora se crean y sellan directamente en el día programado, en lugar de cuando el punto de restauración correspondiente se convierte en el más antiguo en la cadena de backup incremental. Esto debería eliminar la confusión continua existente y la preocupación de nuestros clientes con respecto a este proceso.

- **Sin backups trimestrales —** Para mantener la consistencia con los trabajos de backup primarios GFS, ya no se proporciona una opción de backup trimestral. Las programaciones trimestrales existentes se convertirán a mensuales incrementando su valor de retención de la forma adecuada durante la actualización a V11. Los trabajos de copia de backup existentes con la retención GFS activada se actualizarán automáticamente el upgrade de versión.

Entre otras mejoras de los trabajos de backup se incluyen:

- **Repositorio como fuente —** Ahora puede seleccionar todo el repositorio como fuente para los trabajos de copia de backup en el modo de copia inmediata.
- **Retención diaria —** Elija entre restauración basada en punto de restauración y la nueva retención de días basada en tiempo para los backups recientes creados por el trabajo de copia de backup.

Trabajos de replicación

- **Soporte de repositorio NFS —** Ahora puede especificar un repositorio de backup basado en NFS en el asistente de trabajo de replicación para albergar los metadatos de la réplica.

Trabajos Quick Migration (replicación rápida)

- **Umbral SmartSwitch —** Nuestras pruebas internas mostraron que Quick Migration en el modo SmartSwitch requiere de gran cantidad de tiempo para VMs con mucha RAM — hasta un punto de que ya no tiene sentido. La causa de origen en el tiempo que necesita para transferir el estado de la memoria sobre el protocolo NFC. Consecuencia de ello es que, a partir de la V11, forzaremos la migración cold (mediante el apagado) para máquinas con más de 8 GB de RAM. Puede usar el valor de registro *QMSmartSwitchRAMThresholdGB* (DWORD) en el servidor de backup para anular este valor.

Restaurar

API de integración de datos

- **Soporte de destino Linux —** La API de integración de datos (DIAPI por sus siglas en inglés) se ha ampliado para permitir el montado del contenido de backup directamente en el servidor de Linux.
- **Soporte de plataforma ampliada —** La V11 permite backups de imagen de todas las plataformas compatibles con Veeam para su publicación a través de la DIAPI. Esto incluye backups nativos de la nube para AWS, Microsoft Azure y Google Cloud Platform, así como backups de Nutanix AHV y VMware Cloud Director.

Recuperación a nivel de archivos (FLR por sus siglas en inglés)

- **Linux FLR sin appliance asistente —** FLR (File-Level Restore) desde los sistemas de archivo Linux puede ahora llevarse a cabo montando el backup desde CUALQUIER máquina Linux: dedicada, de destino o la original (lo que siempre está garantizado para comprender el sistema de archivo desde el que está intentando restaurar). Este enfoque elimina la necesidad de que un host vSphere o Hyper-V ejecute el appliance asistente FLR, al mismo tiempo que elimina las complejidades de red y los problemas de seguridad alrededor del appliance. También permite a los clientes ejecutar la FLR directamente donde de las ofertas de infraestructura VMware basadas en la nube.

  NOTA: El appliance asistente todavía se mantiene disponible como una opción, por ejemplo, desde los backups archivados con sistemas de archivos que ya no está usando en el entorno de producción.

- **Mejoras de rendimiento de Linux FLR —** El rendimiento de la FLR desde sistemas de archivo no Windows se han incrementado hasta un 50 % si está haciendo recuperación con o sin el appliance asistente.

Veeam Explorer *for Microsoft Active Directory*

- **Restauración de la configuración DFS —** Ahora puede ejecutar restauraciones de la configuración de Distributed File System (DFS) en el contenedor del sistema.

Veeam Explorer *for Microsoft Teams*

- **Restauración de elementos de Microsoft Teams —** Restaure elementos de Microsoft Teams directamente desde el backup a nivel de imagen del servidor de backup de Veeam Backup for Microsoft Office 365.

Infraestructura de backup

Repositorio de backup

- **Rendimiento synthetic full mejorado en ReFS —** Los backups completos sintéticos ahora deberán completarse hasta dos veces más rápido en ReFS, gracias al uso reducido de la llamada a la API de Windows de ejecución prolongada para la creación del nuevo archivo de backup completo sintético.
- **Deshabilitar los flujos de integridad de ReFS —** Ahora puede desactivar los flujos de integridad ReFS para archivos de backup de Veeam usando el valor de registro *DisableRefsIntegrityStreams* (DWORD, 1) en el servidor de backup. Aunque no recomendamos desactivar los flujos de integridad porque la integridad de datos es vital en la protección de datos, algunos clientes insistieron en contar con la posibilidad de controlar este ajuste para mejorar el rendimiento.

Scale-out Backup Repository

- **Organización por niveles de VeeamZIP™ y los backups exportados —** Los backups completos creados con VeeamZIP y Export Backup, así como los backups huérfanos, ahora se procesan con las políticas de Capacity Tier y Archive Tier de igual forma que los backups normales y pueden copiarse o descargarse a almacenamiento de objetos de la forma habitual. Los backups importados no se organizarán por niveles como hasta ahora.
- **Reconocimiento de clonación rápida —** El programador de extensiones de SOBR ahora tendrá en cuenta que el archivo de backup completo sintético recién creado tiene que clonarse rápidamente y no requerirá que la extensión home (preferida) posee suficiente espacio libre en disco para albergar los archivos de backup completos sintéticos que no son de clonación rápida. En las versiones anteriores, esto podía provocar la "explosión del repositorio SOBR cuando determinadas extensiones se acercaban a su capacidad porque el programador empieza a asignar todos los backups completos sintéticos a extensiones no home.
- **Descargar operaciones en el log de eventos de Windows —** Las operaciones de descarga y copia de Capacity Tier y Archive Tier ahora crean los eventos correspondientes en el log de eventos del sistema para conseguir una mejor visibilidad de estos procesos para usuarios que llevan a cabo la supervisión basada en el registro de eventos.

Repositorio de almacenamiento de objetos

- **Límite de tareas —** Se ha añadido la capacidad de limitar el número de tareas simultáneas para mejorar la compatibilidad con el almacenamiento de objetos local, que puede desbordarse fácilmente por un gran número de solicitudes de API simultáneas. No habría necesidad de usar este límite para la mayor parte del almacenamiento de objetos en la nube pública, dato que puede escalarse de forma ilimitada. Sin embargo, un caso de uso donde este límite puede resultar de utilidad es cuando especifica un servidor gateway en los ajustes del repositorio de almacenamiento de objetos para acceder mediante proxy a Internet, puesto que al depender de la cantidad de CPU y RAM disponible, este servidor puede quedarse sin recursos de computación cuando se procesan muchas tareas simultáneas.

- **Rendimiento de restauración —** El rendimiento de restauración desde el almacenamiento de objetos local apoyado por hardware lento se ha mejorado significativamente.
- **El permiso ListAllMyBuckets ya no es necesario —** Los buckets de S3 y el almacenamiento de objetos de Google ahora pueden especificarse manualmente en el asistente Object Storage Repository sin tener que buscarlos. Esto permite a los proveedores de servicios crear buckets individuales para sus clientes y delegar los permisos con una política de IAM sin exponer una lista de todos sus clientes (en los nombres del bucket) a otros clientes.
- **Descomprimir los bloques antes de almacenar —** Ahora puede tener bloques de datos de backup descomprimidos antes de que se copien al almacenamiento de objetos. Esto permite que los dispositivos de almacenamiento de objetos locales que disponen de características integradas de deduplicación pueda procesar los datos de backup de una manera más eficiente. Para habilitar este comportamiento, cree la entrada de registro *ObjectStorageDisableCompression* (DWORD, 1) en el servidor de backup.

Veeam Cloud Connect

- **Modo MSP del backup de Cloud Connect —** Cuando la casilla "Allow this Veeam Backup & Replication installation to be managed by the service provider" se selecciona en el asistente del proveedor de servicios en el servidor de backup del lado del cliente, los metadatos del backup, como los nombres de las máquinas, no quedan ocultos en el servidor de backup del lado del proveedor, permitiendo a los MSP el prestar los servicios de backup gestionados de una forma más eficiente.
- **Tenants (cliente) basado en Microsoft Active Directory —** Para simplificar la protección de portátiles y estaciones de trabajo con un Veeam Agent *for Microsoft Windows* independiente en un entorno empresarial, Veeam Cloud Connect incluye ahora soporte para cuitas de cliente o suscriptores (tenants) basados en cuentas de Active Directory (AD). Esto permite a los usuarios aprovechar sus cuentas de AD para conectar a un repositorio cloud en la que la infraestructura de Cloud Connect autentica al suscriptor o tenant a través de AD. La autenticación en curso durante los backups usa una clave secundaria para evitar que backups perdidos provoquen cambios de contraseñas. Sin embargo, la recuperación completa (bare-metal) desde un repositorio en la nube siempre requiere que la cuenta sea autenticada correctamente con AD usando la contraseña actual antes de permitir el acceso a los backups. También, si la cuenta de AD está bloqueada, ni será posible realizar ninguna operación de backup ni de restauración.
- **Evacuación de tenants (cliente o suscriptor) —** Los tenants ahora pueden evacuarse de las extensiones de Scale-out Backup Repository usando el cmdlet Start-VBRCloudTenantBackupEvacuation.
- **Limitación del acelerador de la WAN —** El ajuste "Limit incoming traffic from this tenant" (limitar el tráfico entrante de este tenant) ahora se aplica también a los tenants que transfieren datos a través de los aceleradores de WAN integrados. Anteriormente funcionaba solamente para el modo de transferencia de datos directa.
- **Consumo de RAM del servidor Cloud Connect —** Hemos reducido significativamente el consumo de RAM en el servidor Cloud Connect durante la actividad entrante del trabajo de replicación.

  El acceso a Veeam Cloud Connect *for Service Providers* requiere de una **licencia de alquiler**. Para acceder a Veeam Cloud Connect *for the Enterprise*, póngase en contacto con su representante de ventas de Veeam.

Plataformas

Google Cloud Platform (GCP)

- **Integración de Veeam Backup *for Google Cloud Platform* —** Registe buckets de Google Cloud Storage (GCS) con backups creados por Veeam Backup *for Google Cloud Platform* como repositorios externos, que le permiten ejecutar todo tipo de restauraciones y copiar sus backups de VM de GCP a repositorios de backup locales, o a cinta, con fines de recuperación ante desastres y para el cumplimiento de la regla 3-2-1.

Linux

- **Data mover persistente para Linux —** Los componentes de transporte ahora se despliegan de forma persistente cuando registra un servidor de Linux con Veeam. Esto mejora el rendimiento y la escalabilidad, puesto que los data movers no necesitan insertarse ya en el servidor cada vez que comienza una tarea. Las reglas necesarias para los firewalls incluidos de Linux se crean automáticamente para la duración del trabajo de backup (se admiten iptables, ufw y firewalld).

  NOTA: Para los hosts de Linux que todavía no son compatibles con el data mover persistente, como appliances de almacenamiento con la integración del data mover de Veeam, la V11 sigue usando el data mover run-time.

- **Seguridad del data mover mejorada —** Cuando se usan credenciales de un solo uso, el data mover persistente se ejecutará como el usuario limitado del conjunto de credenciales con el que se desplegó. Como consecuencia, cualquier vulnerabilidad potencial que exista en la API del data mover interno no podrá ser utilizada por los ciberdelincuentes para alcanzar el sistema operativo.

- **Autenticación basada en certificado —** En lugar de usar las credenciales guardadas de Linux, ahora aprovecharemos la tecnología de infraestructura de clave pública (PKI) para la autenticación entre el servidor de backup y los componentes de transporte durante el procesamiento de las tareas de backup con los pares de claves generadas automáticamente en el momento de la implementación del transporte.

- **Criptografía de curva elíptica —** Para conseguir un nivel de seguridad sin precedentes, la V11 añade soporte para los pares de claves SSH basados en curva elíptica (EC), como Ed25519 o ECDSA, para establecer las conexiones SHH a los servidores Linux. Si descifrar una clave RSA de 228 bits requiere menos energía que para hacer hervir una cucharada de agua, una clave EC de 228 bits necesitaría la energía de hacer hervir todo el agua sobre el planeta tierra, proporcionando un nivel de seguridad equivalente a la clave RSA 2380 bits.

Microsoft Azure

- **Backup nativo de Azure totalmente integrado —** La protección de datos de Azure nativa de la nube ahora se construye directamente en la consola de Veeam Backup & Replication. Esto requiere Veeam Backup *for Microsoft Azure* v2.

- **Soporte de Azure Stack HCI —** Se ha añadido el soporte del nuevo sistema operativo de infraestructura hiperconvergente (HCI) de Microsoft, que es en esencia una infraestructura local Hyper-V ofrecido como servicio de Azure.

- **Restaure a VM generación 2 —** Se ha añadido soporte experimental para Direct Restore *to Microsoft Azure* para aprovisionar una VM generación 2 como destino. Para habilitar esta funcionalidad, cree la entrada de registro *AzureEnableGeneration2VMRestore* (DWORD, 1) en el servidor de backup.

Nutanix AHV

- **Veeam Backup *for Nutanix AHV* 2.1 —** La nueva funcionalidad incluye la exclusión de disco en los trabajos de backup, mejor integración con Nutanix Volume Groups para restauración, mejoras de la interfaz de usuario y mucho más. Para consultar el listado completo de características nuevas, refiérase al documento Notas de la versión.

VMware vSphere

- **Recuperación instantánea de disco de primera clase (FCD) —** Cuando se lleva a cabo una recuperación de disco instantánea, los usuarios pueden elegir entre restaurar un disco desde backups como VMDK estándar asignado a la VM vSphere específica o como disco de primera clase o First Class Disk (FCD), que puede gestionarse independientemente de las VMs vSphere y consumido directamente por la última generación de aplicaciones basadas en contenedores.

- **Y para etiquetas vSphere —** Además de poder especificar múltiples etiquetas individuales vSphere como el ámbito de un trabajo, ahora puede usar una combinación de etiquetas vSphere, en cuyo caso, solo las VM con todas las etiquetas seleccionadas asignadas serán procesadas (comportamiento clásico del operador Y). Cuando se usa este enfoque, hay que tener gran cuidado de monitorizar las VMs no protegidas, por ejemplo con Veeam ONE™, ya que esta configuración hace mucho más fácil que se pierdan VMs de manera no intencionada desde el ámbito de protección y que se acabe con la falta de backups recientes de ellas.

- **Failback de dos pasos —** Para hacer el tiempo de failback más predecible para VMs grandes y reducir el tiempo de inactividad, hemos mejorado el control del proceso de failback. En la primera etapa del proceso, que es la que consume la mayor parte del tiempo, la VM de réplica sigue estando en ejecución mientras se calculan resúmenes y la máquina de destino de failback se restaura al estado de snapshot previo al failback. Una vez que se completa este proceso, la réplica de VM se coloca en el estado Ready to Switch y se puede hacer failback con el mínimo tiempo de inactividad requerido para la transferencia de la delta final. La operación de cambio puede realizarse manual o automáticamente, bien sea tan pronto como la réplica esté preparada para hacer el cambio o bien en el momento programado durante la siguiente ventana de mantenimiento.

- **Modos de transporte del proxy Linux —** Los modos de transporte soportados ahora incluyen Direct Storage Access (para el almacenamiento en bloque y NFS), Network (NBD/NBDSSL) y Backup from Storage Snapshots (solo para almacenamiento en bloque). Además, el rendimiento del modo de transporta hot-add ya existente se ha mejorado significativamente con la tecnología de extracción, anteriormente aprovechada solo por los proxies basados en Windows.

- **Restauración CBT del proxy Linux —** Se ha añadido compatibilidad para la funcionalidad Quick Rollback a los proxies de backup basados en Linux para la restauración de VM completa y failback a la ubicación original.

- **Multi-threading NBD —** El motor de backup ahora es capaz de establecer múltiples conexiones NBD por VMDK para obtener un mejor rendimiento del modo de transporte de red. Al mismo tiempo, debido al límite bajo del número máximo de conexiones NBD por host ESXi, existen problemas de fiabilidad con el incremento del número de este tipo de conexiones. Aunque nuestro programador de recursos hace un seguimiento de las tareas NBD por host para asegurar que permanecen dentro de los límites, decidimos que un beneficio de rendimiento marginal no justifica el riesgo de habilitar este comportamiento para toda nuestra base de clientes inmediatamente, ya que puede haber también conexiones NBD externas. Sin embargo, puede usar el valor del registro *VMwareNBDConnectionsPerDisk* (DWORD) en el servidor de backup para probar esta funcionalidad. Nuestras pruebas desvelaron que el mejor rendimiento se consigue con dos conexiones NBD por disco. Comparta sus resultados en los foros Veeam R&D para ayudarnos a decidir si habilitar esta funcionalidad de forma predeterminada en futuras actualizaciones.

- **Compatibilidad con VMware Remote Console —** La funcionalidad de la interfaz de usuario que permite abrir una consola de VM ahora usa la consola VMware Remote Console que es más segura. Se le ofrecerá la oportunidad de descargar e instalar la consola tras el primer intento de usar cualquier funcionalidad relacionada.

- **Actualización de versión de VDDK —** VDDK 6.7 se ha actualizado a la versión 6.7.3, que entre otras cuestiones, debería reparar los problemas con el uso de E/S NBD asíncrono.

VMware Cloud Director

- **Replicación de Cloud Director —** Este nuevo tipo de trabajo de replicación específico permite a los proveedores de servicios realizar la replicación de vApp dentro y entre instancias de Cloud Director (VCD). Los procesos de replicación procesan las VMs y metadatos de la vApp (como redes o el orden de inicio de la VM) para crear una vApp de réplica lista para usar en el Cloud Director de destino que puede usarse inmediatamente en caso de desastre.
- **Plug-in Native Cloud Director —** Esta funcionalidad permite a los proveedores de servicios ampliar la IU del tenant de Cloud Director para incluir la funcionalidad de Veeam Backup & Replication, permitiendo a los tenants (clientes) gestionar sus propios backups y restauraciones sin abandonar la comodidad de la consola web de Cloud Director. Esta integración se basa en el portal de backup en modo autoservicio Cloud Director ya existente de Veeam.
- **Compatibilidad para múltiples servidores Cloud Director —** El portal de backup en modo autoservicio de Cloud Director ahora admite entornos con múltiples servidores VCD registrados con Veeam Backup & Replication, y puede seleccionar el servidor deseado al crear la configuración para su organización.
- **Compatibilidad para múltiples configuraciones —** El portal de backup en modo autoservicio de Cloud Director ahora admite la creación de múltiples configuraciones en modo autoservicio para la misma organización VCD.
- **Flexibilidad de acceso al portal Cloud Director mejorada —** Ahora puede especificar roles VCD personalizados en los valores del registro *vCloudPortalBackupAdminRole* (STRING) y *vCloudPortalRestoreOperatorRole* (STRING) en el servidor de backup para permitir a todos los usuarios de VCD con el correspondiente rol VCD, acceder al portal de backup en modo autoservicio para su organización con el rol Administrador de backup u Operador de restauración. Si no se incluyen estos valores en las entradas del registro, el comportamiento se mantiene como en las versiones anteriores: solo los usuarios de VCD con permisos de administración en la organización de VCD pueden acceder al portal de backup en modo autoservicio para la organización correspondiente con el rol del portal Administrador de backup.
- **Compatibilidad con Cloud Director 10.2 —** Compatibilidad total para las instalaciones locales (on-premises) e implementaciones basadas en la nube con el servicio VMware Cloud Director.

Integraciones con almacenamiento primario

General

- **Recuperación de disco instantánea desde snapshots de almacenamiento —** Reduzca su superficie de recuperación instantánea restaurando únicamente los discos necesarios o grandes VMs de vSphere (por ejemplo, solo los discos del SO o solo los discos de datos) directamente desde los snapshots de almacenamiento. Monte los discos al instante desde un snapshot a las VM seleccionadas para otros casos de uso, por ejemplo, para comparar el contenido en disco o realizar recuperaciones en masa a nivel de archivo usando herramientas de terceros.
- **Retención basada en puntos de restauración para snapshots de almacenamiento —** La retención de puntos de restauración en snapshots de almacenamiento ahora se procesa por VM. Anteriormente los snapshots de almacenamiento en sí mismo eran considerados como puntos de restauración, lo que ocasionaba varios problemas en casos extremos, como reintentos fallidos, migración de VM a otro volumen, etc.

Dell EMC VNX/VNXe/Unity/Unity XT

- **Versión de la herramienta de integración —** Se han actualizado las herramientas Dell EMC Navisphere y Unisphere CLI a la última versión para permitir la compatibilidad con TLS 1.2.

HPE 3PAR/Primera

- **Compatibilidad con 3PAR Remote Copy—** Ahora toda la funcionalidad de integración de snapshots de almacenamiento es compatible con la replicación 3PAR/Primera periódica asíncrona. Esto incluye gestionar la replicación de snapshots de almacenamiento, retención independiente para réplicas de snapshots y backup desde réplicas de snapshots en la segunda matriz para evitar el impacto de las actividades de backup en la matriz primaria.
- **Compatibilidad multiprotocolo de Nimble —** La funcionalidad de integración de snapshots de almacenamiento ahora es compatible con almacenamiento de Nimble con la posibilidad de tener activados los protocolos FC y iSCSI en la misma matriz.
- **Compatibilidad de versiones —** Se ha añadido compatibilidad para 3PAR OS 3.3.1 MU5 y se ha eliminado el soporte de las versiones de 3PAR OS por debajo de la versión 3.2.2 y WSAPI anteriores a la versión 1.5.

Lenovo

- **Compatibilidad con Lenovo DM —** Se ha añadido la integración de snapshots de almacenamiento de Lenovo ThinkSystem DM Series.

NetApp

- **Compatibilidad con ONTAP 9.8 —** Se ha añadido la compatibilidad con NetApp ONTAP 9.8 para la integración de snapshots de almacenamiento excepto para el procesamiento de VMs que residen en volúmenes FlexGroup. Nota: todavía puede usar el backup normal basado en el host o basado en agentes ara proteger dichas VMs.

Integraciones de almacenamiento secundario

ExaGrid

- **Soporte de autenticación de AD —** Se ha añadido compatibilidad para la autenticación basada en Microsoft Active Directory para registrar ExaGrid con Veeam.
- **Lógica de colocación de SOBR —** Por petición de ExaGrid, y a la luz de la deduplicación global que ofrecen, hemos desactivado la lógica especial de programación de la extensión de SOBR diseñada para deduplicar el almacenamiento y hacer que SOBR prefiera colocar el nuevo backup completo en la misma extensión que el backup completo anterior. Puede volver a la lógica de colocación anterior creando la entrada de registro *ExaGridEnableNewFullToSameExtent* (DWORD, 1) bajo la clave HKLM\SOFTWARE\Veeam\Veeam Backup and Replication en el servidor de backup.
- **Parámetros predeterminados de la interfaz de usuario —** Ahora recomendamos ajustar el nivel de compresión a Optimal en el asistente del trabajo de backup cuando ExaGrid está definido como el repositorio de destino, y habilitamos la opción "Decompress backup data blocks before storing" en el asistente del repositorio de backup de forma predeterminada al registrar un repositorio basado en ExaGrid. Este nuevo valor predeterminado permitirá a ExaGrid llevar a cabo la deduplicación de forma efectiva, con independencia de la carga de trabajo protegida.

Dell EMC Data Domain

- **Compatibilidad con Data Domain OS —** Se ha añadido compatibilidad para las versiones 7.1, 7.2 y 7.3 de Data Domain OS, mientras se ha retirado el soporte para todas las versiones de DD OS previas a la 6.1. Actualice su versión de Data Domain OS antes de actualizar a V11.
- **Versión de Data Domain Boost SDK —** DD Boost SDK se ha actualizado a la versión 7.0.

HPE StoreOnce

- **Trabajos de copia de backup como fuente —** Los trabajos Backup Copy ahora también pueden usarse como fuente para los trabajos Catalyst Copy. Anteriormente solo los trabajos de backup primarios eran admitidos como fuente.
- **Cinta para los backups Catalyst Copy —** Los trabajos Backup to Tape ahora son compatibles con los trabajos Catalyst Copy como fuente.
- **Rendimiento de la comprobación de estado —** El nivel de rendimiento de la comprobación de estado del backup en los trabajos Catalyst Copy se ha incrementado en varias veces a través del procesamiento en paralelo.
- **Interfaz de usuario de eliminación retrasada de la copia de backup —** Los trabajos Catalyst Copy habilitan la eliminación retrasada de las copias de backup desde el almacenamiento secundario, que resultan en una retención más duradera en los destinos de Catalyst Copy. El retraso de la eliminación ahora puede controlarse directamente en la interfaz de usuario, al contrario del ajuste del registro. Esta funcionalidad es compatible con almacenamiento HPE StoreOnce y HPE Cloud Volume Backup.
- **Compatibilidad con Cloud Volumes Backup —** La V11 añade compatibilidad con los trabajos de Catalyst Copy con HPE Cloud Volumes Backup.
- **Versión de Catalyst SDK —** HPE StoreOnce Catalyst SDK se ha actualizado a la versión 4.2.4 con la versión del protocolo V11.
- **Etiquetado de sesiones Catalyst API —** Los trabajos de backup de los recursos compartidos de archivos de Veeam ahora etiquetan las llamadas a la API de Catalyst con la etiqueta especial VeeamNAS. El soporte de HPE pretende usar esta información para diferenciar cargas de trabajo de Veeam en sus casos de soporte para conseguir una resolución más rápida.

Quantum DXi

- **Compatibilidad con Quantum FastClone —** V11 admite de manera oficial el clonado rápido en los repositorios de backup respaldados por los modelos Quantum DXi que soportan esta funcionalidad. Póngase en contacto con el equipo de soporte de Quantum para confirmar el estado del modelo de almacenamiento que está usando.
- **Rendimiento de restauración de VM completa mejorado —** Hemos añadido una lógica de restauración optimizada para la restauración de VMs completas, que ya se utiliza en otras integraciones de almacenamiento de deduplicación. El proxy de backup de Veeam ahora realiza lecturas secuenciales desde Quantum y escribe de forma aleatoria en los discos de destino, en lugar de restaurar los bloques en el orden en que se almacenan en el disco de destino.

Las integraciones de almacenamiento de deduplicación se incluyen en la licencia **Veeam Universal License**. Si se usa una licencia tradicional por socket, se necesita la edición **Enterprise** o superior.

Cinta

- **Copia de cinta —** Clone fácilmente las cintas seleccionadas con el fin de crear copias adicionales remotas, actualizar los datos almacenados para combatir el decaimiento de los medios magnéticos con el tiempo o migrar sus archivos a sistemas de generación LTO modernos con migraciones a las primeras y últimas generaciones soportadas. El servidor de backup actualizará el catálogo de backup con referencias a las cintas (destino) clonadas, mientras preserva también las referencias a las cintas (fuente) originales.
- **Verificación de cinta —** Compruebe sus cintas archivadas periódicamente para asegurar que los datos almacenados son todavía legibles y consistentes La verificación de las cintas magnéticas puede ser necesaria por motivos de cumplimiento normativo, y también le ayuda a uno a dormir mejor por la noche.

- **Restaurar todo el contenido en cinta —** Rescate fácilmente todos los datos de un conjunto de medios que incluya una cinta con errores mediante el volcado de todos los archivos que son todavía legibles a la ubicación especificada.
- **Modo de mantenimiento —** Ponga toda una biblioteca de cinta o unidades específicas en modo mantenimiento para comunicar a todos sus trabajos de cinta que temporalmente no las usen.
- **Límite de uso de la unidad por trabajo —** Ahora puede limitar el uso de la unidad de cinta a nivel de trabajos individuales para los trabajos de backup a cinta.
- **Forzar el borrado de cinta —** El proceso de borrado de cinta ahora ignorará los errores no críticos, como problemas de tamaño de bloque o de cabeceras, ya que son irrelevantes para una cinta que va a ser borrada.
- **Backup con reconocimiento del clúster para almacenamientos basados en NetApp ONTAP —** Cluster Aware Backup es una extensión del protocolo NDMP v4 que permite al servidor NDMP establecer una conexión de datos sobre un nodo propietario del volumen, optimizando el flujo de datos y mejorando el rendimiento de backup NDMP.
- **Fuentes de trabajo Backup to Tape —** Los trabajos de backup a cinta (Backup to tape) ahora pueden procesar copias de respaldo de backups de Nutanix AHV y Mac backups, así como backups nativos de la nube para AWS, Azure y Google, lo que le permite archivar backups de máquinas a cinta con fines de cumplimiento normativo.
- **Mejoras de rendimiento de los trabajos de archivo a cinta (File to Tape) —** Gracias a la mejora de la lógica de preprocesamiento de los trabajos de archivo a cinta, las operaciones de backup y restauración ahora se completan hasta 10 veces más rápido para conjuntos de datos con grandes números de archivos y carpetas en el ámbito de la protección.
- **Ámbito de protección de los trabajos de archivo a cinta —** Ahora puede especificar toda la fuente de datos (Windows Server o servidor de archivos SMB/NFS) como la fuente de los trabajos de archivo a cinta, que protegerán todos los recursos compartidos y exportaciones, incluidos los añadidos recientemente. Esta nueva funcionalidad ha hecho necesario el cambio del asistente de restauración File from Tape para respaldar la restauración de dichos backups, que como efecto colateral ahora le permite configurar restauraciones en masa desde múltiples recursos compartidos de archivo en una única pasada del asistente.
- **Informes mejorados —** Los trabajos de verificación de backup, restauración y cinta ahora generan un archivo CSV en la carpeta del log del trabajo, con todos los archivos que no se pudieron procesar.
- **Mejoras de la experiencia de usuario (UX) en la restauración desde cinta —** Las cintas necesarias ahora se muestran automáticamente para cada punto de restauración seleccionado en el asistente. Ya no necesita ver cada uno de los puntos de restauración, simplemente haga clic en Next y espere que aparezca el mensaje de introducir esas cintas.
- **Mejoras en la interfaz de usuario (IU) para la gestión de cinta —** Se ha añadido la vida útil de la cinta de limpieza en el cuadro de diálogo de propiedades de cinta y la biblioteca de cinta, y los números de serie de la unidad al cuadro de diálogo de propiedades del dispositivo. La sesión de rescan de la cinta ahora indica cuando se ha completado. La etiqueta de ubicación ahora puede configurarse en los servidores NDMP. Los menús de contexto en la pestaña Tape Infrastructure se ha actualizado para conseguir mayor claridad. El ancho de todas las columnas se ha ajustado para adaptarse al contenido de forma estándar.
- **Compatibilidad con las especificaciones LTO-9 —** Toda la funcionalidad de soporte de cinta nativa de la V11 se ha validado con éxito frente a muestras de diseño hardware de cinta LTO-9 proporcionadas amablemente por IBM. Si la cinta es el futuro, entonces V11 está preparado para ello.

Agentes de backup

Gestión de agentes

- **Backup desde snapshots de almacenamiento—** Los servidores Microsoft Windows Server con volúmenes alojados en matrices de almacenamiento compatibles ahora pueden copiarse usando trabajos de backup basados en agentes "gestionados por el servidor" desde snapshots de almacenamiento nativos. Este enfoque traslada la carga de proceso de los datos de backup desde el servidor protegido al proxy de backup dedicado. Por otra parte, el uso de snapshots de almacenamiento elimina la sobrecarga de E/S del sistema en ejecución fuera de los snapshots VSS Software para el intervalo de tiempo que dure el backup. Al abordar estos dos desafíos clásicos del backup basado en agentes, V11 ofrece backups con impacto nulo sin LAN, *idénticos a los backups de VM VMware e Hyper-V fuera del host*, a servidores físicos y clústers, que permite a los usuarios proteger incluso sus cargas de trabajo 24x7 más activas sin incumplir los SLA. Son compatibles todas las integraciones de almacenamiento incluidas y las basadas en la API Universal Storage, con conectividad iSCSI o FibreChannel, y no es necesario contar con un proveedor de VSS hardware específico de un fabricante.

- **Grupo de protección para agentes preinstalados —** Este tipo Protection Group (PG) proporciona una forma cómoda de instalar agentes usando soluciones de distribución de software de terceros cuando desplegarlos desde el servidor de backup no es posible debido a restricciones de la conexión de red y de seguridad. El asistente PG crea un paquete de instalación de agente personalizado que permite a un agente conectarse al servidor de backup automáticamente usando autenticación de tipo PKI (infraestructura de clave pública) con un certificado de PG. El servidor de backup de esta forma coloca un agente entrante en el protection group que creó su paquete de instalación y emite el nuevo certificado de autenticación personal. En ese momento puede usar el agente con normalidad en las directivas de backup "managed by agent" (gestionadas por agente). No es necesario que el servidor de backup sea capaz de conectarse a los agentes a través de la red, ya que los agentes mismos consultarán varias veces al día si se han producido cambios en la configuración de políticas.

- **Mejoras en la exportación como disco virtual —** Los discos de los backups basados en agente ahora se pueden exportar como discos fijos VHD/VHDX para permitir el montaje de estos en los servicios de Microsoft Azure (anteriormente los discos solo podían exportarse como discos dinámicos).

- **Notificación por email de hosts no protegidos —** Se ha añadido una notificación por correo electrónico opcional para hosts de los que no se ha hecho copia de backup al menos una vez dentro del número de días especificado en la política de backup "managed by agent" (gestionada por el agente).

- **Eliminar de la configuración —** Ahora puede eliminar las máquinas de los Protection Groups a través del menú de contexto en el host.

- **Medios de recuperación desde copias de backup —** Los medios de recuperación ahora pueden crearse también desde los backups creados por los trabajos de copia de backup (Backup Copy).

- **Veeam Agent *for Microsoft Windows* —** El asistente de trabajo de backup basado en agente ahora ofrece la posibilidad de configurar el ajuste "Backup all volumes except excluded" para el modo de backup a nivel de volumen, excluir del proceso la carpeta de OneDrive y usar el nuevo modo de backup del perfil de usuario.

Veeam Agents

- **Veeam Agent *for Microsoft Windows* v5:** La nueva funcionalidad incluye soporte para Microsoft Windows 10 version 20H2, uan compatibiidad más amplia con las versiones de Microsoft .NET Framework para evitar la necesidad de reinicio tras la instalación de .NET, opciones de retención GFS y diaria para servidores, backup de perfiles de usuario en el modo a nivel de archivo, detección mejorada de conexiones VPN, cumplimiento FIPS y mucho más.For the complete listFor the complete list Para consultar el listado completo de características nuevas, refiérase al documento Novedades.

- **Veeam Agent *for Linux* v5:** Entre las nuevas funcionalidades se incluye el soporte de nuevas versiones de sistemas operativos, backup de atributos extendidos en el modo a nivel de archivo, múltiples mejoras de los medios de recuperación, cumplimiento de FIPS y mucho más. Para consultar el listado completo de características nuevas, refiérase al documento Novedades.
- **Veeam Agent *for Mac*:** El nuevo agente proporciona backup gestionado para los datos del usuario para cualquier dispositivo macOS desde Veeam Backup & Replication ™, lo que le permite integrar perfectamente la protección de equipos y portátiles Mac en su estrategia general de protección de datos. Al contrario del software Time Machine de Apple, Veeam Agent *for Mac*le permite cumplir con la regla 3-2-1 a través de la creación de backups adicionales locales y remotos haciendo uso de las características y funcionalidades de Veeam que ya le son familiares.

  Basado en el probado motor de agente de Veeam Agent *for Linux* , el agente de Mac incluye las siguientes características:

  - Backup de datos de usuario y contenido de unidades USB externas
  - Integración con los perfiles de configuración de las soluciones MDM
  - Restauración sencilla a nivel de archivo en modo autoservicio para usuarios finales a través de una interfaz local

Plug-ins de aplicaciones empresariales:

General

- **Compatibilidad con Capacity Tier de SOBR —** Los backups y las copias de backup de todos los plug-ins de aplicaciones empresariales ahora pueden copiarse o trasladarse a almacenamiento de objetos con la funcionalidad Capacity Tier de SOBR. De igual forma que con los backups a nivel de imagen, restaurar desde los backups descargados al almacenamiento de objetos es un proceso totalmente transparente.
- **Mejoras de rendimiento —** Hemos hecho importantes mejoras de rendimiento en todos los frentes, en particular gracias al nuevo enfoque aplicado del manejo de los metadatos con los archivos de metadatos por backup, que mejora significativamente la escalabilidad general. Consulte la documentación de la actualización sobre cómo migrar sus backups ya existentes al nuevo formato de metadatos.
- **Metadatos autorrecuperables —** La comprobación periódica del estado del backup analiza todos los puntos de restauración cada seis horas y vuelve a crear archivos de metadatos que faltan, y cuya ausencia puede atribuirse a la interrupción del backup por un evento externo. Puede cambiar este periodo mediante la creación de la entrada de registro *DbPluginMissingMetaRegenerationAttemptIntervalMinutes* (DWORD) en el servidor de backup.
- **Cumplimiento de la norma FIPS —** Todos los plugins de aplicaciones empresariales ahora usan los módulos de cifrado conformes con FIPS.

Veeam Plug-in *for Oracle RMAN*

- **Compatibilidad con Oracle Data Guard —** Se ofrece compatibilidad completa para el backup de implementaciones de Oracle Data Guard.
- **Compatibilidad RAC mejorada —** Ahora se ofrece compatibilidad con las instalaciones de Oracle RAC con archivo /etc/oratab vacío.

Veeam Plug-in *for Oracle RMAN en AIX*

Este plugin o complemento nuevo ofrece la misma experiencia de funcionalidad, instalación y configuración que sus homólogos Solaris. Entre las versiones compatibles se incluyen IBM AIX 6.1, 7.1, 7.2 y Oracle 11, 12, 18, 19 (versión ppc64).

Veeam Plug-in for SAP HANA

- **Compatibilidad con SAP HANA 1.0 —** Además de la compatibilidad anterior con SAP HANA 2.0, esta versión ahora soporta SAP HANA Database 1.0 SPS 12 o posteriores (consulte el artículo KB2997 para conocer las instrucciones de instalación). El plugin está certificado oficialmente por SAP para las versiones 1.0 y 2.0 de HANA.

Veeam Plug-in for SAP on Oracle

Este nuevo plug-in certificado por SAP proporciona integraciones con SAP BR*Tools para permitir hacer backups de bases de datos Oracle directamente a los repositorios de Veeam de forma compatible con los modos de backup util_file y util_file_online. Tenga en cuenta que Veeam Plug-ins para Oracle RMAN y for SAP on Oracle pueden usarse juntos para ejecutar backups en el modo rman_util. Las versiones compatibles incluyen versiones de 64 bits de:

- OS: SLES 11,12 y 15; RHEL 6 y 7; Oracle Linux 6 y 7
- Oracle: 11.2 hasta 19.1
- BR*tools: 7.20 Patch 42 o posterior

Los plug-ins de aplicaciones empresariales se incluyen en la licencia **Veeam Universal License**. Si se usa una licencia tradicional por socket, se necesita la **edición Enterprise *Plus***.

Backup de NAS

General

- **Ámbito de protección root —** Ahora puede especificar toda la fuente de datos (Windows Server o servidor de archivos SMB/NFS) como fuente de los trabajos de backup de recursos compartidos de archivo, que protegerá todos los recursos compartidos y exportaciones, incluidos los añadidos recientemente. Esta nueva funcionalidad ha hecho necesario el cambio del asistente de restauración de recursos compartidos de archivos para respaldar la restauración de dichos backups, que como efecto colateral ahora le permite configurar restauraciones en masa desde múltiples recursos compartidos de archivo en una única pasada del asistente. Además, las carpetas de snapshots de almacenamiento serán excluidas del procesamiento automáticamente siempre que sean detectadas, con lo que ya no tiene que añadir de forma explícita estas carpetas a la lista de exclusiones del trabajo de backup.

  NOTA: Puede convertir los backups existentes al formato aceptado para su asignación a un nuevo trabajo de backup creado con el ámbito basado en root usando el cmdlet Convert-VBRNASBackupRootFormat.

- **Rendimiento mejorado —** El rendimiento del backup de recursos compartidos y trabajo de copia de backup ahora son dos veces más rápidos, gracias al uso de múltiples flujos de subida entre los data movers de origen y destino donde las que más se benefician son las transferencias sobre redes con una latencia alta.
- **Equilibrador de carga inteligente —** En presencia de múltiples proxies de backup, los trabajos de backup de recursos compartidos de archivos ahora detectarán y usarán automáticamente los proxies de backup menos ocupados (de igual forma que ya hacen los trabajos de backup de VM), lo que permite conseguir una carga más uniforme y hacer un uso completo de la capacidad de cómputo.
- **Alertas de archivos bloqueados —** Ahora puede controlar si quiere registrar problemas de procesamiento de archivos y atributos de archivos como una alerta en el resultado general del trabajo de backup de recursos compartidos de archivos. Además, la ruta al archivo de auditoría que enumera todos los archivos bloqueados se muestra ahora en el registro (log) del trabajo.

- **Retención basada en versión —** Para controlar mejor el consumo de espacio de almacenamiento en el repositorio de backup, ahora puede elegir entre aplicar la retención basada en versión a las versiones de los archivos solo en el repositorio de archivo (un comportamiento de la V10) o aplicar una retención transversal tanto en el backup como en el archivo.
- **Asignación automática de backup para las copias de backup —** Los procesos de copia de backup ahora intentarán detectar automáticamente la presencia del backup primero en la primera ejecución y continuará el backup existente con un incremento si está presente el primer backup o copia semilla.

Integraciones con almacenamiento primario

- **Enterprise NAS filer integration —** Las integraciones nativas de Dell EMC Isilon, Lenovo DM y NetApp FAS le permiten registrar todo el archivador como fuente de datos y llevar a cabo los backups de recursos compartidos de archivos sin tener que conseguir permisos de acceso para cada recurso compartido protegido. Además, el backup de dichas fuentes de datos se llevará a cabo desde los snapshots de almacenamiento nativos de forma estándar para evitar archivos bloqueados sin necesidad de configuraciones complejas y scripts para gestionar los snapshots.

  NOTA: Puede convertir los backups existentes al formato aceptado para su asignación a un nuevo trabajo de backup creado con el ámbito de archivador NAS usando el cmdlet Convert-VBRNASBackupStorageFormat.

- **Integración nativa del seguimiento de cambios en archivos —** Los trabajos de backup de recursos compartidos de la V11 puede integrarse con la API Changelist de Dell EMC Isilon para reducir la carga de almacenamiento y mejorar el rendimiento de los backups incrementales en escenarios en los que los recursos compartidos de archivos posean un gran número de subcarpetas con unas tasas de cambio muy bajas.

Integraciones con almacenamiento secundario

- **Blobs grandes —** Los backups de recursos compartidos y trabajos de copia de backup (Backup Copy) ahora cambiarán automáticamente a usar blobs de 1 GB cuando se usan como destino appliances de almacenamiento de deduplicación. Esto incremental la escalabilidad hasta en 20 veces para dispositivos de almacenamiento que soportan una cantidad limitada de archivos por appliance (por ejemplo HPE StoreOnce) y mejora el rendimiento del backup y la restauración unas cuantas veces para el almacenamiento de deduplicación.

  NOTA: Puede usar el cmdlet Convert-VBRNASBackupStorageFormat para actualizar sus trabajos existentes para usar blobs grandes.

- **Metadata extents —** Cuando se usan repositorios Scale-out Backup Repository™ que consistan exclusivamente de almacenamiento lento, como pueden ser los appliances de deduplicación, puede mejorar hasta cierto punto el rendimiento del backup y la restauración introduciendo una pequeña extensión para metadatos solamente con almacenamiento más rápido, que se usará únicamente para almacenar los metadatos del backup. Dado que se trata de una característica avanzada, solo puede configurarse con uede configurarse con PowerShell usando el cmdlet Set-VBRRepositoryExtent.

Interfaz de usuario

Consola de backup

- **No se necesita administrador local —** La consola de backup ya no requiere que los operadores utilicen una cuenta que pertenezca al grupo de administrador local en el sistema que ejecuta la consola. Esto ayuda a mejorar la seguridad al no tener que asignar privilegios administrativos a todos los operadores de la consola. Cuando se necesite instalar la actualización de la consola y en escenarios de restauración que realmente requieran privilegios de administrador local, se le ofrecerá la oportunidad de reiniciar la consola con una cuenta de administrador local.

- **Backup huérfanos —** Los backups sin un trabajo asociado son mucho más fáciles de supervisar ahora, gracias al nuevo nodo Orphaned (huérfano) en Backups. Anteriormente, este tipo de backups terminaban en el nodo Imported backups (backups importados) y era imposible de distinguirlos.
- **Nodos de trabajo basados en filtros —** Ahora puede añadir vistas de los trabajos personalizadas (una característica de la V10) como nodos persistentes al árbol de administración para conseguir un acceso más rápido a las vistas favoritas que utiliza con más frecuencia.
- **Información de inmutabilidad del backup —** Hemos añadido una columna que muestra el tiempo de caducidad de la inmutabilidad del backup del repositorio protegido (hardened) en el cuadro de diálogo de propiedades del backup.
- **Marcas de tiempo en el registro de acción —** Por petición popular, además de la columna de duración de la operación, ahora puede mostrar la columna timestamp (marca de tiempo) con la hora a la que se inició cada operación. Para hacer esto, haga clic con botón derecho en el encabezado action log (registro de acción).
- **Integración del centro de notificaciones de Windows —** Ahora usaremos el centro de notificaciones de Windows para mostrar notificaciones interactivas como que una base de datos de configuraciones de SQL Server se está acercando a su límite de tamaño máximo (nuevo en la V11), trabajos a cinta que están esperando a que se inserte un soporte y otros mensajes importantes que anteriormente se mostraban en un mensaje tipo globo en el área de notificación (bandeja del sistema).
- **Confusión del botón Finish resuelta —** El botón Finish (Terminar) del último paso de los asistentes de recuperación a nivel de archivo y nivel de elemento se han renombrado a Browse (Examinar) para comunicar mejor el hecho de que el proceso continuará con la selección de elementos. Anteriormente, algunos usuarios mostraban temor de hacer clic en este botón debido a que de forma equivocada asumían que comenzaría la restauración antes de seleccionar verdaderamente qué restaurar.
- **Consola de Swagger —** Ahora puede abrir la nueva documentación interactiva API RESTful del servidor de backup (con tecnología de Swagger) directamente desde el menú principal.
- **Funciones obsoletas —** La funcionalidad "Transform previous backup chains into rollbacks" se ha abandonado, con lo que la casilla de verificación correspondiente ya no se muestra en la interfaz de usuario para los nuevos trabajos creados. Si necesita ayuda para abandonar este modo de backup, comparta su caso en los foros de R&D de Veeam. Tenemos pensado eliminar esta funcionalidad por completo en nuestra versión principal en 2022.

Enterprise Manager

- **Localización de la interfaz de usuario web —** Hemos añadido el framework estándar de la industria GetText a Enterprise Manager —y gracias a nuestro equipo de ingenieros de sistemas, Veeam Backup Enterprise Manager v11 se entrega ahora con los siguientes idiomas incluidos: francés, alemán, italiano, japonés, español y chino simplificado.
- **Experiencia de inicio de sesión único (SSO) —** Hemos cambiado la IU de inicio de sesión para que ya no requiera la introducción del nombre de usuario para los inicios de sesión SSO. En su lugar, redirigimos inmediatamente los usuarios al proveedor de identidad configurado para la autenticación. Esto permite a los usuarios de una organización usar una autenticación sin credenciales (por ejemplo en entornos donde solo se usa smartcard) para iniciar sesión en Enterprise Manager y sus portales.
- **Compatibilidad con SAML para el portal de backup en modo autoservicio —** El portal ha despertado mucho interés fuera del ámbito de su audiencia objetiva original, particularmente dentro del grupo de los proveedores de servicios. Para apoyar esta tendencia, hemos añadido la integración con SAML, para permitir a los proveedores de servicios proporcionar a sus tenants acceso al portal mediante la asignación de cuotas a usuarios externos y grupos. En caso de usar cuentas SAML, el único modo de delegación soportado es el basado en las etiquetas de vSphere.
- **Mejoras de la IU —** Para la recuperación de elementos de Microsoft Exchange, ahora podremos mostrar el nombre del buzón de correo junto al nombre de usuario para evitar confusiones con personas con nombres similares. También hemos añadido la funcionalidad de búsqueda de objetos al definir el ámbito o alcance del rol Restore Operator (operador de restauración).

Licenciamiento

General

- **El mejor cambio es que no haya cambios, por fin —** V11 usa el mismo formato de archivo de licencia introducido en la V10. Dicho tipo de archivos de licencia ya no están vinculados a una versión particular de software, lo que le permite usar su archivo de licencia de la V10 para la V11, siempre que su contrato de mantenimiento siga activo.

- **Actualización automática de la licencia en la instalación —** Al llevar a cabo la actualización desde V9, el asistente de instalación le ofrecerá la oportunidad de descargar el archivo de licencia de la V11 automáticamente. Esto requiere subir su licencia actualmente instalada a los servidores de Veeam. Si su backup de servidor no cuenta con conexión a Internet o si prefiere no subir su licencia actual, puede descargar si lo prefiere su archivo de licencia desde el portal de clientes.

- **Actualización automática de licencia en el producto—** Al instalar un archivo de licencia, se le ofrecerá la oportunidad de descargar automáticamente extensiones de licencia cuando renueve o amplíe su contrato. Esta funcionalidad opcional requiere que el servidor de backup envíe el ID de licencia, el ID de instalación y el cómputo de consumo de cargas de trabajo a los servidores de Veeam de forma periódica. Si prefiere no compartir esta información con Veeam, no habilite esta funcionalidad y en su lugar descargue sus archivos de licencia actualizados desde el portal de clientes e instálelos manualmente.

- **Renovación de licencia simplificada —** Ahora puede iniciar el proceso de renovación de licencia directamente desde el cuadro de diálogo de información de licencia. El botón renovación redirige a los usuarios al sitio web de Veeam y el formulario de solicitud de renovación de licencia con parte de la información requerida ya insertada basándose en la licencia instalada actualmente.

Veeam Universal License (VUL)

- **Protección del doble de datos NAS —** Tras revisar los descuentos medios que nuestros equipos de ventas han proporcionado en oportunidades de protección de NAS basada en la licencia VUL, hemos decidido doblar la cantidad de datos NAS cubiertos por una licencia de 250 GB a 500 GB. Este cambio también significa que ahora puede proteger los primeros 500 GB de datos desde cualquier fuente de archivos sin coste alguno (frente a los 250 GB en la V10a). Para poder aprovechar esta nueva capacidad de backup NAS debe actualizar a la V11.

- **Eliminación de la edición Starter —** Esta edición se descatalogó en otoño de 2020, con lo que V11 no aceptará este tipo de licencias. Descargue un archivo de licencia de reemplazo para Veeam Backup Essentials™ desde el portal del cliente — es una actualización gratuita para el resto del periodo del contrato.

Licencias por sockets

- **Eliminación de ediciones de producto —** Al igual que con VUL, las licencias por socket se ofrecen ahora a nuevos clientes en una edición única con todas las características, anteriormente conocida como Enterprise *Plus*. Los clientes existen que ya posean una licencia por socket pueden seguir usándola, renovar y ampliar cualquiera que sea la edición que posean. Si está interesado en cualquier funcionalidad no disponible en su edición, póngase en contacto con un representante comercial de Veeam para conseguir ofertas especiales para la actualización de su edición de licencia por socket o migrar a la licencia VUL.

Community Edition

- **Ahora con más características —** La versión V11 *Community Edition* incluye todas las nuevas características y mejoras de la V11 excepto aquellas etiquetadas con los requisitos de licenciamiento especiales. También se beneficia del cambio en la capacidad del backup del NAS, permitiendo ahora la protección de más de 5 TB de datos de NAS con la licencia gratuita, donde los primeros 500 GB de los datos del recurso compartido de archivos no contabilizan como consumo para la licencia.

  La compatibilidad de *Community Edition* mediante la actualización a Veeam Backup Essentials ya es posible. La suscripción cuesta menos que una cena en un restaurante elegante, y le da acceso a TODAS las características y el soporte al cliente 24x7. Este tipo de conversiones nos ayudan a seguir ofreciendo protección de datos de clase empresarial gratis a aquellos que realmente no se lo pueden permitir.

Más información
veeam.com/es

Descargar versión de prueba gratuita
vee.am/backupes