

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código:SIG-TI-CKE-MN03		

CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **“uso interno”**.

El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO.....	3
2. ALCANCE	3
3. DEFINICIONES	3
4. CONTENIDO	4
5. FLUJO DEL PROCEDIMIENTO.....	50
6. SOPORTE Y LICENCIAMIENTO	51
7. ROLES Y RESPONSABILIDADES.	52
8. CONTROL DE CAMBIOS	53
9. FLUJO DE APROBACIÓN.....	54

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

1. OBJETIVO

El objetivo de este documento es proporcionar una guía detallada sobre el proceso de recuperación de datos utilizando las herramientas de respaldo Veeam Backup y Data Protector. Se busca describir los pasos necesarios para llevar a cabo una recuperación efectiva, así como revisar las características y funcionalidades de ambas herramientas. Con evidencias directas de las herramientas actuales.

2. ALCANCE

Este documento inicia con la necesidad de documentar el proceso estructurado que se lleva a cabo con la herramienta de Veeam Backup y Dataprotector, centrándose en la ejecución de restauraciones, implementación de planes de recuperación mediante la restauración de datos. Se abordará la identificación y validación de los puntos de restauración disponibles, garantizando que sean adecuados y funcionales para una recuperación efectiva.

3. DEFINICIONES

Backup: es una copia de la información que por seguridad se realiza y que se utiliza en caso de materializarse un incidente que genere pérdida de datos.

Estos son útiles para dos casos:

1. Recuperarse de una catástrofe informática
2. Recuperar una pequeña cantidad de archivos que puedan haberse eliminado accidentalmente o corrompido.

Administrador Backup: Persona responsable de la configuración, programación y correcta ejecución de los respaldos.

Proveedor de soporte: entidad que tiene personal especializado en el conocimiento de las soluciones de respaldo, al cual se escalan fallas identificadas en las herramientas de respaldo.

RTO: Es el tiempo máximo aceptable que una aplicación o servicio puede estar inactivo después de un incidente antes de que cause un impacto inaceptable en el negocio. es el tiempo que se tarda en restaurar la funcionalidad del sistema o servicio tras una interrupción.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

RPO: Es el punto en el que se debe recuperar la información después de una interrupción. Indica la cantidad máxima de datos que se puede perder debido a un incidente, expresado en términos de tiempo. Es la cantidad de datos que se podría perder y que aún se considera aceptable para la organización

4. CONTENIDO

Proceso de Veeam Backup - Respaldo y restauración.

1. Respaldos de máquinas virtuales en Vmware.

Veeam Backup & Replication no instala software de agente dentro del sistema operativo invitado de la máquina virtual para recuperar los datos de la máquina virtual. Para realizar copias de seguridad de las máquinas virtuales, aprovecha las capacidades de instantáneas de VMware vSphere. Cuando realiza una copia de seguridad de una máquina virtual, Veeam Backup & Replication solicita a VMware vSphere que cree una instantánea de la máquina virtual. Puede pensar en la instantánea de la máquina virtual como una copia de un momento determinado de una máquina virtual que incluye discos virtuales, estado del sistema, configuración, etc. Veeam Backup & Replication utiliza esta copia de un momento determinado como fuente de datos para la copia de seguridad.

Veeam Backup & Replication copia los datos de las máquinas virtuales desde el almacén de datos de origen a nivel de bloque. Recupera los datos de las máquinas virtuales, los comprime y los deduplica, y los almacena en archivos de backup en el repositorio de backup en formato exclusivo de Veeam.

En Veeam Backup & Replication, la copia de seguridad es un proceso impulsado por trabajos. Para realizar copias de seguridad, debe configurar trabajos de copia de seguridad. Un trabajo de copia de seguridad es una unidad de configuración de la actividad de copia de seguridad. El trabajo de copia de seguridad define cuándo, qué, cómo y dónde se debe realizar la copia de seguridad. Un trabajo de copia de seguridad se puede utilizar para procesar una o varias máquinas virtuales. Puede indicarle a Veeam Backup & Replication que ejecute trabajos automáticamente según un cronograma o que los inicie manualmente.

La primera sesión de trabajo de backup siempre produce un backup completo de la imagen de la máquina virtual. Las sesiones de trabajo de backup posteriores son incrementales: Veeam Backup & Replication copia solo aquellos bloques de datos que han cambiado desde la última sesión de trabajo de backup. Para realizar un seguimiento de los bloques de datos modificados, Veeam Backup & Replication utiliza diferentes enfoques

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

2. Cómo funciona la copia de seguridad.

Veeam Backup & Replication realiza copias de seguridad de máquinas virtuales de la siguiente manera:

Cuando se inicia una nueva sesión de trabajo de backup, Veeam Backup & Replication inicia el proceso de Veeam Backup Manager en el servidor de backup. Veeam Backup Manager lee la configuración del trabajo desde la base de datos de configuración y crea una lista de tareas de VM para procesar. Por cada disco de VM agregado al trabajo, Veeam Backup & Replication crea una nueva tarea.

Veeam Backup Manager se conecta al Veeam Backup Service. El Veeam Backup Service incluye un componente de programación de recursos que administra todas las tareas y los recursos de la infraestructura de backup. El programador de recursos verifica qué recursos de la infraestructura de backup están disponibles y asigna servidores proxy y repositorios de backup para procesar las tareas de trabajo.

Veeam Backup Manager establece una conexión con Veeam Data Movers en el repositorio de respaldo de destino y el proxy de respaldo y establece una serie de reglas para la transferencia de datos, como reglas de limitación del tráfico de red, etc.

Los Veeam Data Movers en el proxy de respaldo y el repositorio de respaldo establecen una conexión entre sí para la transferencia de datos.

Veeam Backup Manager consulta información sobre las máquinas virtuales y los hosts de virtualización desde Veeam Bróker Service.

Si el procesamiento de imágenes consciente de la aplicación está habilitado para el trabajo, Veeam Backup & Replication se conecta a los sistemas operativos invitados de las máquinas virtuales, implementa componentes de tiempo de ejecución no persistentes o, si es necesario, componentes de agente persistentes en los sistemas operativos invitados de las máquinas virtuales y realiza tareas de procesamiento en el invitado.

Veeam Backup & Replication solicita a vCenter Server o al host ESXi que cree una instantánea de la máquina virtual. Los discos de la máquina virtual se colocan en estado de solo lectura y cada disco virtual recibe un archivo delta. Todos los cambios que el usuario realiza en la máquina virtual durante la copia de seguridad se escriben en archivos delta.

El Veeam Data Mover de origen lee los datos de la máquina virtual desde el disco de la máquina virtual de solo lectura y transfiere los datos al repositorio de backup en uno de los modos de transporte. Durante las sesiones de trabajo incrementales, el Veeam Data Mover de origen utiliza CBT para recuperar solo aquellos bloques de datos que han cambiado desde la sesión de trabajo anterior. Si CBT no está disponible, el Veeam Data Mover de origen interactúa con el Veeam Data Mover de destino en el repositorio de backup para obtener metadatos de backup y utiliza estos metadatos para detectar bloques que han cambiado desde la sesión de trabajo anterior.

Al transportar datos de la máquina virtual, el Veeam Data Mover de origen realiza un procesamiento adicional. Filtra bloques de datos cero, bloques de archivos de intercambio y bloques de archivos de SO invitado de la máquina virtual excluidos.

El Veeam Data Mover de origen comprime los datos de la máquina virtual y lo transporta al Veeam Data Mover de destino.

Una vez que el proxy de respaldo termina de leer los datos de la máquina virtual, Veeam Backup & Replication solicita al servidor vCenter o al host ESXi que confirme la instantánea de la máquina virtual.

3. Diagrama de arquitectura de respaldo Veeam Backup.

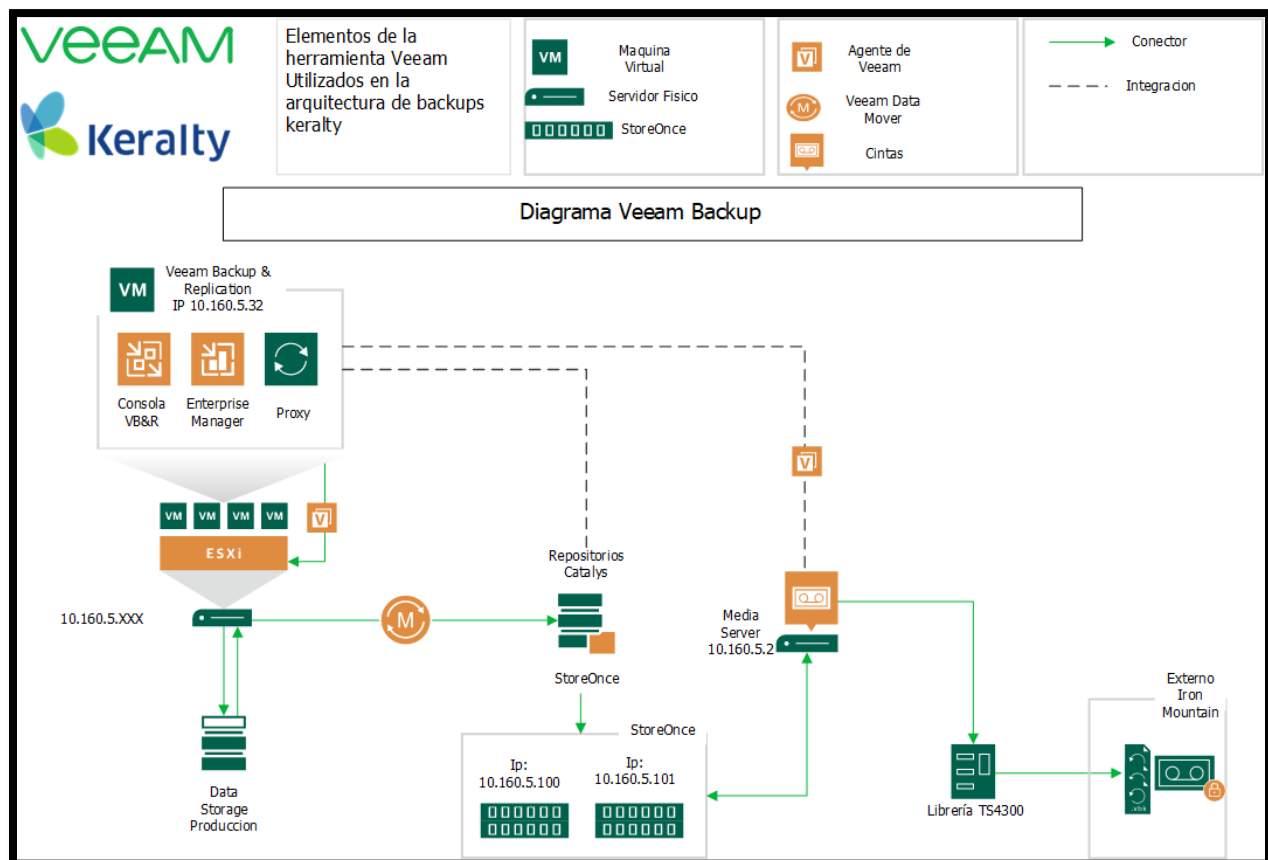


Imagen 1: Arquitectura Respaldo Veeam

4. Procedimiento de restauración

Acceso a la herramienta de respaldo.

Servidor: `srvvrepvm1.keralty.com`

Icono de la Consola.

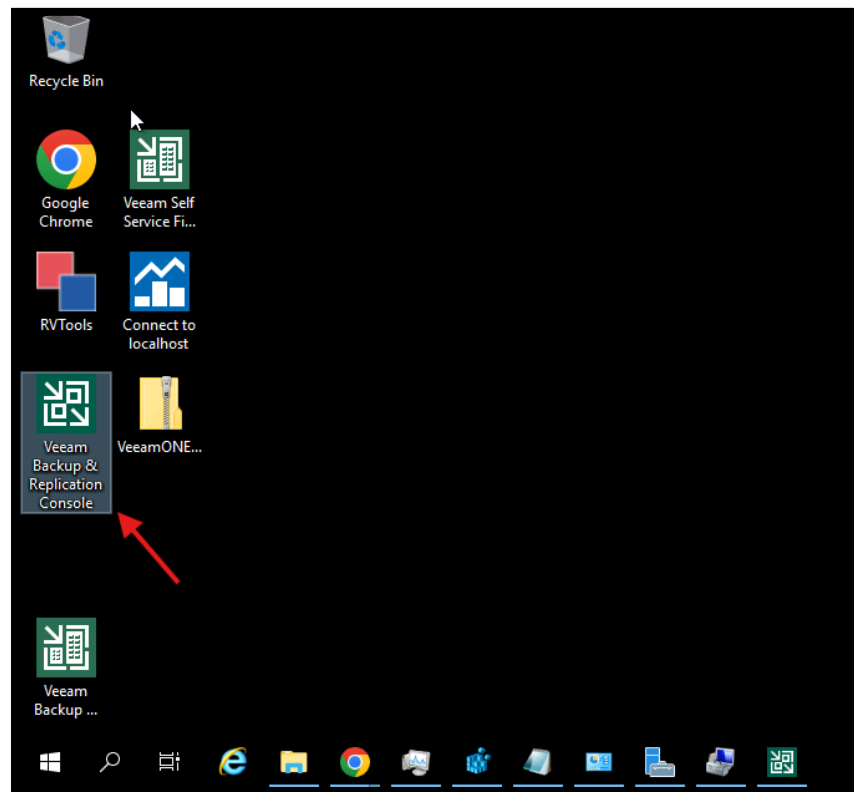


Imagen 2: Acceso consola Veeam.

Cuando abre la consola de Veeam Backup & Replication por primera vez o después de instalar un parche acumulativo en el servidor de backup, debe ejecutar la consola con una cuenta con permisos de administrador local en la máquina donde está instalada la consola. En otros casos, puede ejecutarla con una cuenta que sea miembro del grupo Usuarios en la máquina donde está instalada la consola. Sin embargo, es posible que necesite permisos adicionales para recuperar archivos del sistema operativo invitado de las máquinas virtuales de Microsoft Windows.

Las cuentas que son miembros del grupo de usuarios protegidos de Active Directory no se pueden usar para acceder al servidor de backup de forma remota a través de la consola de Veeam Backup & Replication

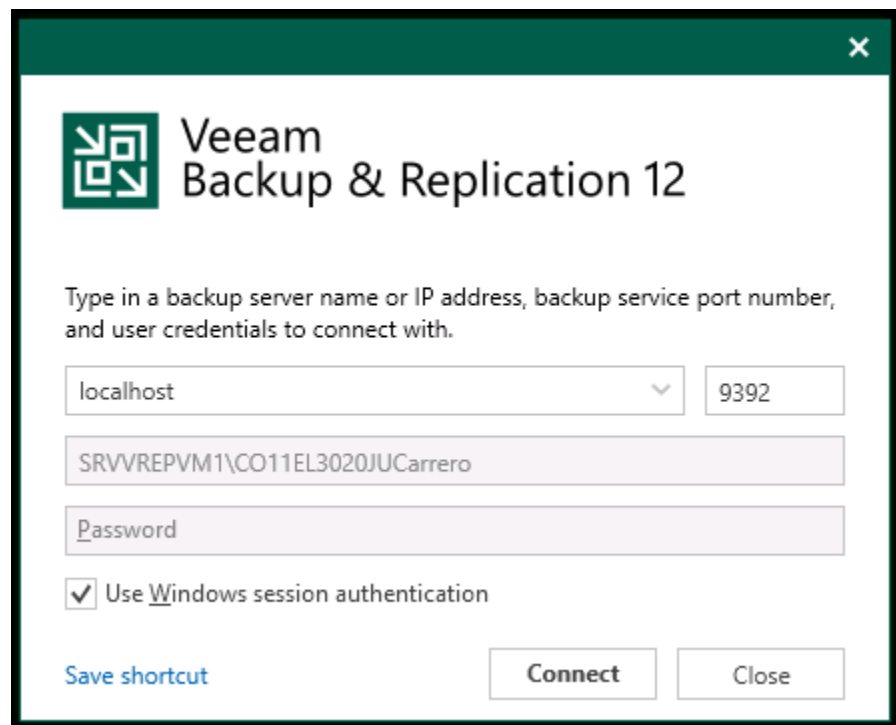


Imagen 3: Autenticación consola Veeam.

Tipo de restauración.

Para el proceso de restauración de maquina se selecciona “VMware vSphere”.

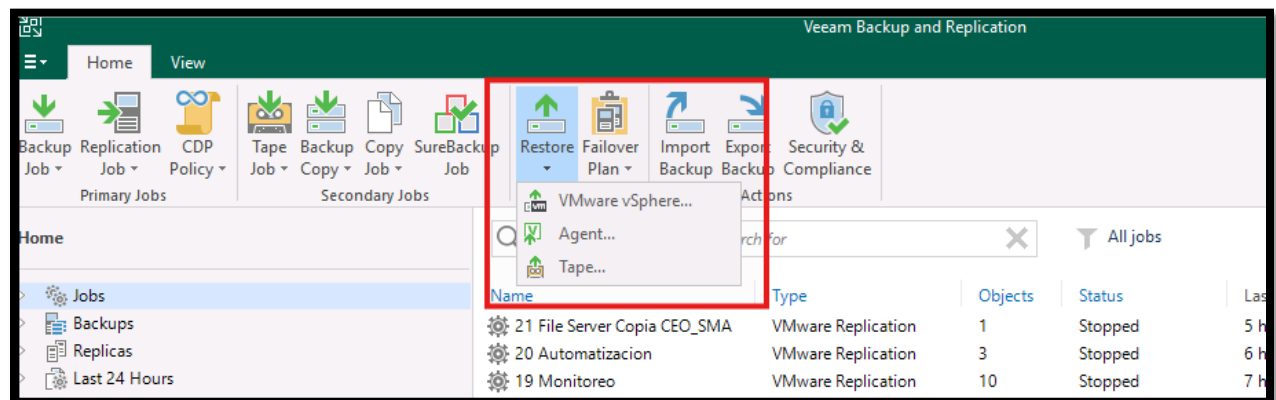


Imagen 4: Consola Veeam opción restore.

Elección de restauración.

Se selecciona la opción de restaurar desde archivo de backup.

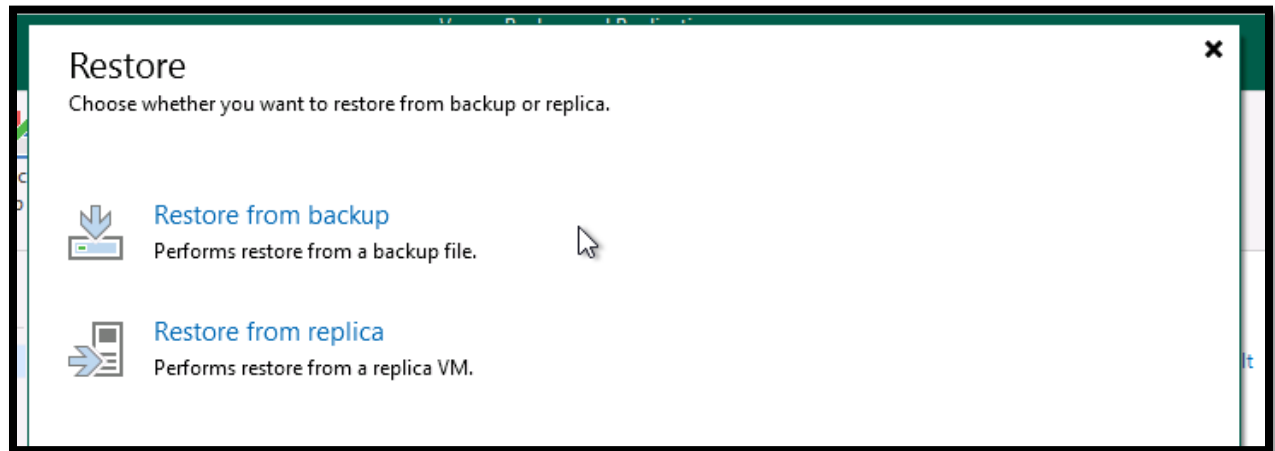


Imagen 5: Opción restore

Opciones de restauración desde la selección de archivo de respaldo.

Se selecciona maquina completa.

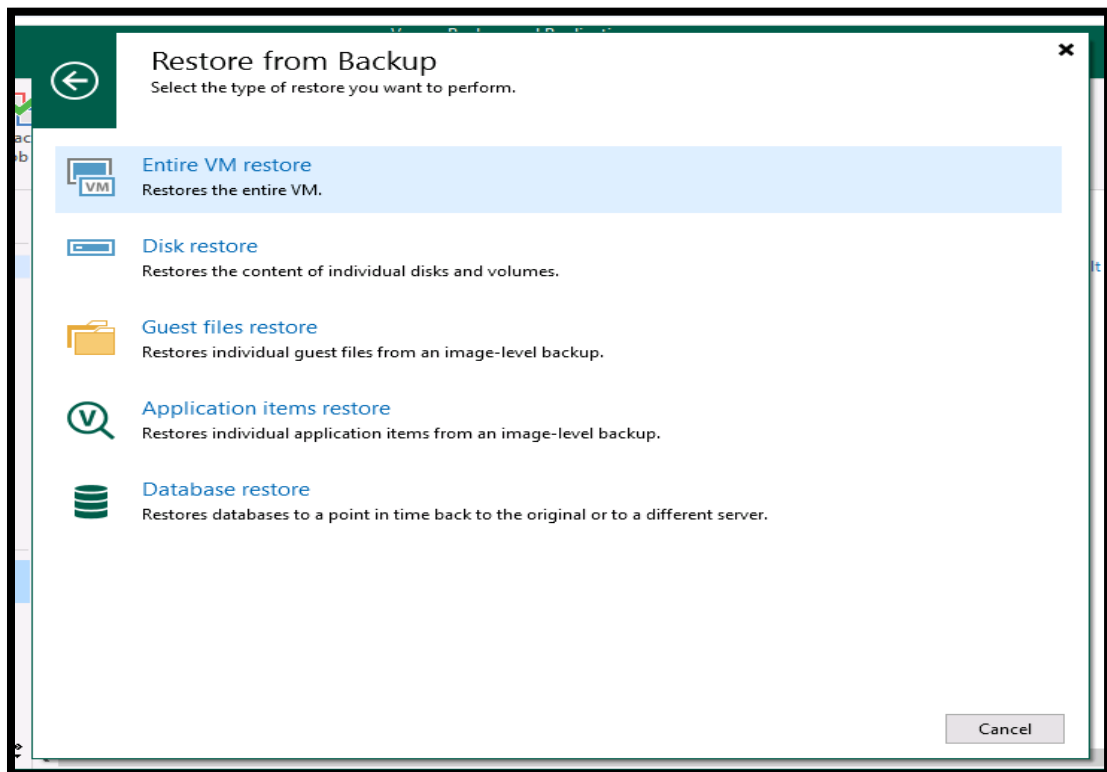


Imagen 6: Opción tipo restore.

Se selecciona restauración desde backup.

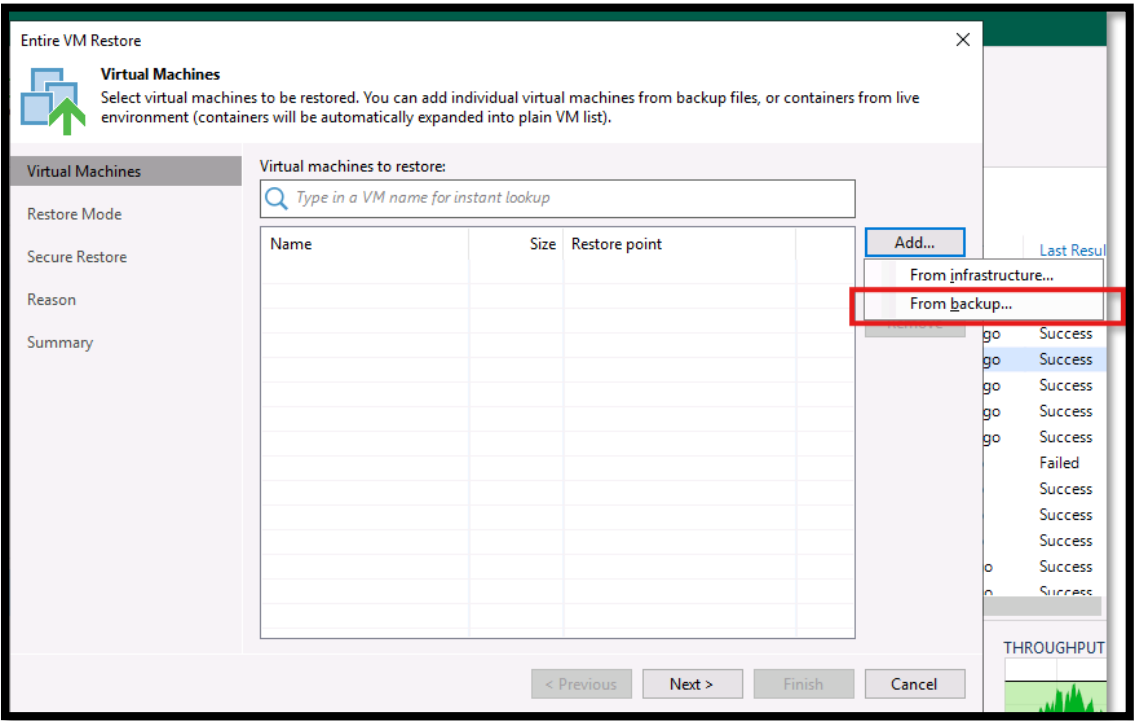


Imagen 7: Selección medio

Se selecciona máquina a recuperar.

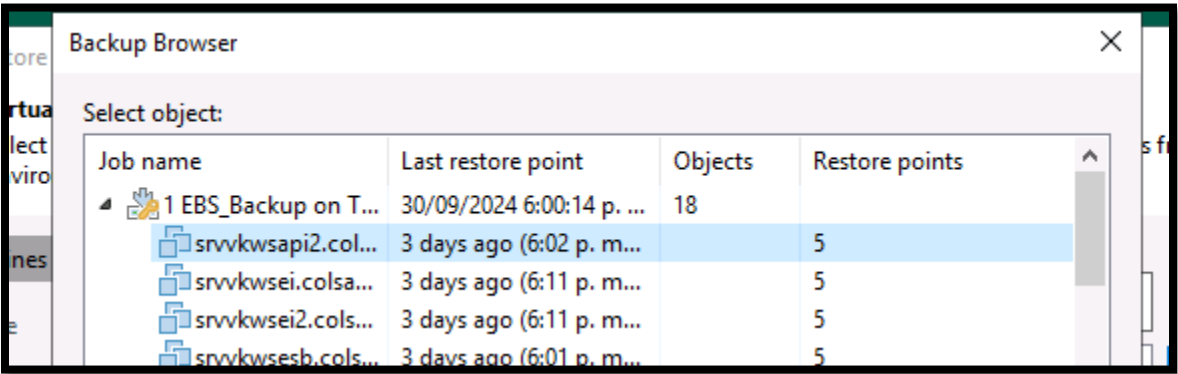


Imagen 8: Selección máquina virtual del trabajo

Se selecciona punto de restauración.

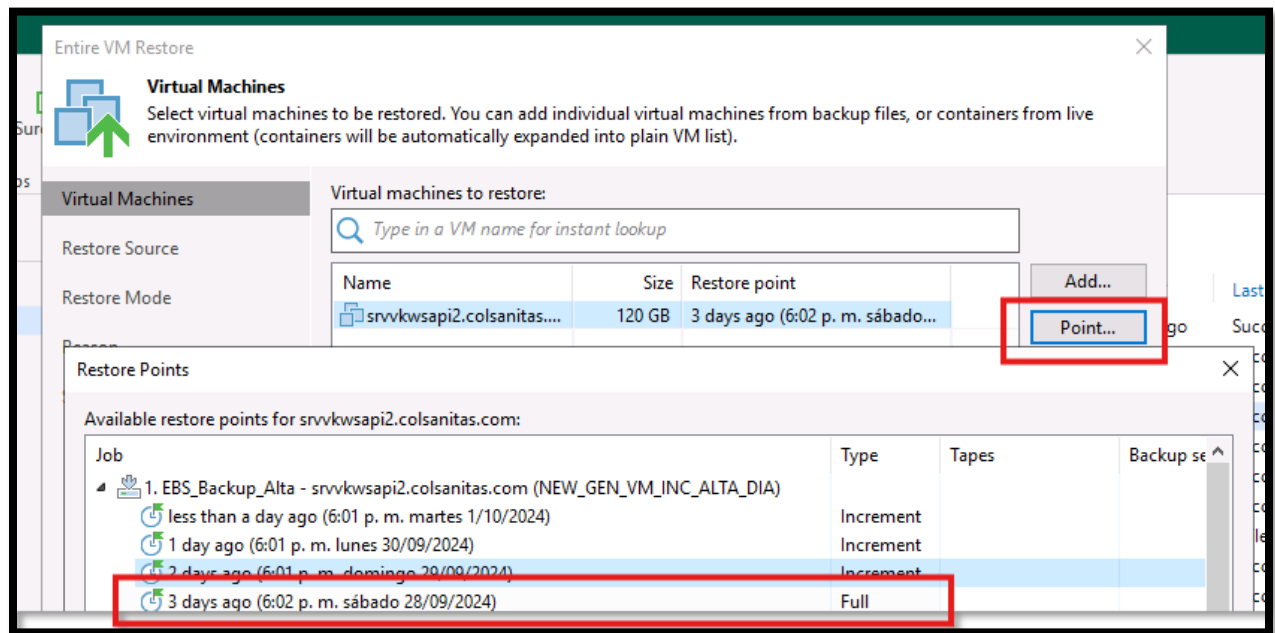


Imagen 9: Selección punto restauración.

Cuando se evidencia la maquina virtual y el punto deseado en el asistente de restauración se continua.

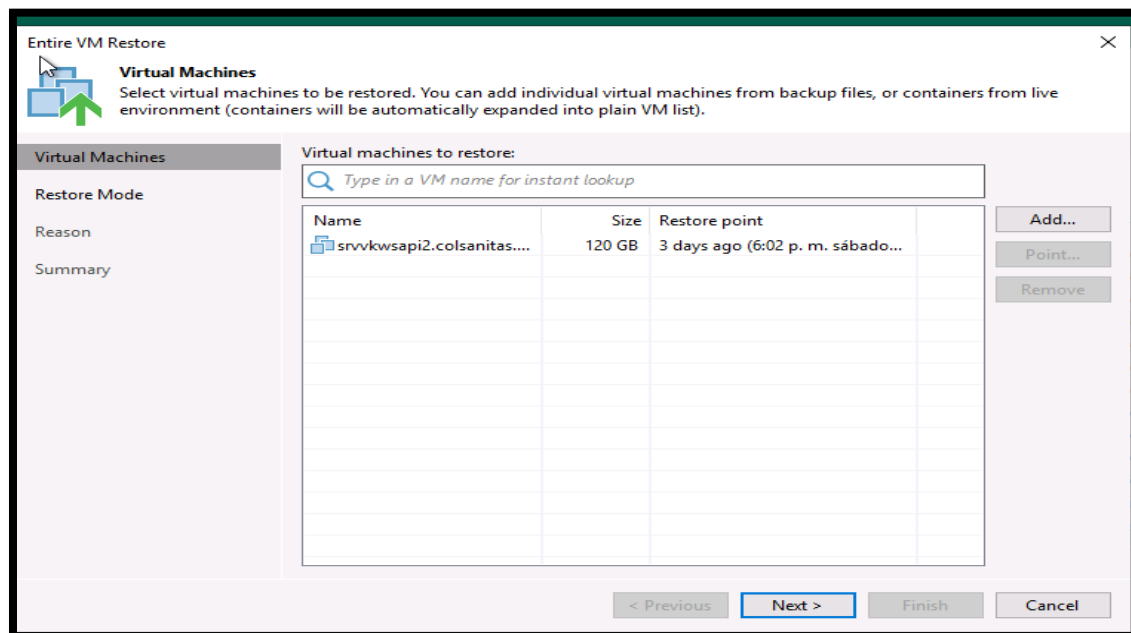


Imagen 10: datos restaurar.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

Modo de restauración.

del asistente, elija el modo de restauración y el proxy de respaldo necesarios para transferir los datos de la máquina virtual:

Elija un modo de restauración:

Seleccione Restaurar a la ubicación original para restaurar las máquinas virtuales con su configuración inicial y a su ubicación original. Si selecciona esta opción, pasará inmediatamente al paso Motivo del asistente.

Durante la restauración a la ubicación original, Veeam Backup & Replication restaura solo aquellos discos que están incluidos en el archivo de backup. Esto significa que, una vez finalizada la restauración, no es necesario actualizar los trabajos existentes que procesan las máquinas virtuales originales.

Seleccione Restaurar en una nueva ubicación o con diferentes configuraciones para restaurar las máquinas virtuales en una ubicación diferente o con diferentes configuraciones (como la ubicación de la máquina virtual, la configuración de red, el formato de los discos virtuales restaurados, etc.). Si se selecciona esta opción, el asistente de restauración completa de máquinas virtuales incluirá pasos adicionales para personalizar la configuración de las máquinas virtuales.

Durante la restauración a una nueva ubicación, Veeam Backup & Replication crea nuevas máquinas virtuales. Si desea procesar las máquinas virtuales restauradas, debe editar los trabajos existentes o crear nuevos trabajos para procesar las máquinas virtuales restauradas. Si restaura máquinas virtuales con el mismo nombre y en la misma carpeta que las máquinas virtuales originales, Veeam Backup & Replication elimina las máquinas virtuales originales. En este caso, debe editar los trabajos existentes para excluir las máquinas virtuales originales de ellos.

Seleccione Restauración por etapas para ejecutar un script ejecutable para las máquinas virtuales antes de restaurarlas al entorno de producción. Si se selecciona esta opción, el asistente de restauración completa de máquinas virtuales incluirá un paso adicional para personalizar la configuración de restauración por etapas.

Durante la restauración por etapas a la ubicación original, es decir, cuando deja la configuración original en los siguientes pasos del asistente, Veeam Backup & Replication elimina las máquinas virtuales originales. Sin embargo, Veeam Backup & Replication actualiza automáticamente los trabajos existentes para procesar las máquinas virtuales restauradas y excluir las máquinas virtuales originales.

Durante la restauración por etapas en una nueva ubicación, Veeam Backup & Replication crea nuevas máquinas virtuales. Si desea procesar las máquinas virtuales restauradas, debe editar los trabajos existentes o crear trabajos nuevos.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

[Para restaurar la máquina virtual a la ubicación original] Seleccione la casilla de verificación **Reversión rápida** para realizar una restauración incremental de la máquina virtual. Veeam Backup & Replication consultará a CBT para obtener los bloques de datos necesarios para revertir la máquina virtual a un punto anterior en el tiempo y restaurará solo estos bloques de datos desde la copia de seguridad. La restauración rápida reduce significativamente el tiempo de restauración y tiene poco impacto en el entorno de producción.

Se recomienda que habilite esta opción si restaura una máquina virtual después de un problema que ocurrió a nivel del sistema operativo invitado de la máquina virtual: por ejemplo, se produjo un error de aplicación o un usuario eliminó accidentalmente un archivo en el sistema operativo invitado de la máquina virtual. No habilite esta opción si el problema ocurrió a nivel de hardware de la máquina virtual, a nivel de almacenamiento o debido a una pérdida de energía.

Haga clic en el enlace **Seleccionar proxy** para usar a fin de seleccionar los servidores proxy de respaldo a través de los cuales se deben transportar los datos de la máquina virtual al almacén de datos de origen. Puede asignar servidores proxy de respaldo de manera explícita o indicarle a Veeam Backup & Replication que seleccione servidores proxy de respaldo de manera automática.

Si elige **Selección automática**, Veeam Backup & Replication detectará los servidores proxy de respaldo que estén conectados al almacén de datos de origen y asignará automáticamente recursos de proxy óptimos para procesar los datos de la máquina virtual.

Durante el proceso de restauración, las máquinas virtuales se procesan simultáneamente. Veeam Backup & Replication comprueba los servidores proxy de backup disponibles. Si hay más de un servidor proxy de backup disponible, Veeam Backup & Replication analiza los modos de transporte que los servidores proxy de backup pueden usar para escribir datos en el destino, la carga de trabajo actual en estos servidores proxy de backup y selecciona los recursos más adecuados para el procesamiento de las máquinas virtuales.

Si elige **Usar solo los servidores proxy de respaldo seleccionados**, puede seleccionar explícitamente los servidores proxy de respaldo que se utilizarán para la restauración. Se recomienda que seleccione al menos dos servidores proxy para garantizar que las máquinas virtuales se recuperen si uno de los servidores proxy de respaldo falla o pierde su conectividad con el almacén de datos de origen durante la restauración.

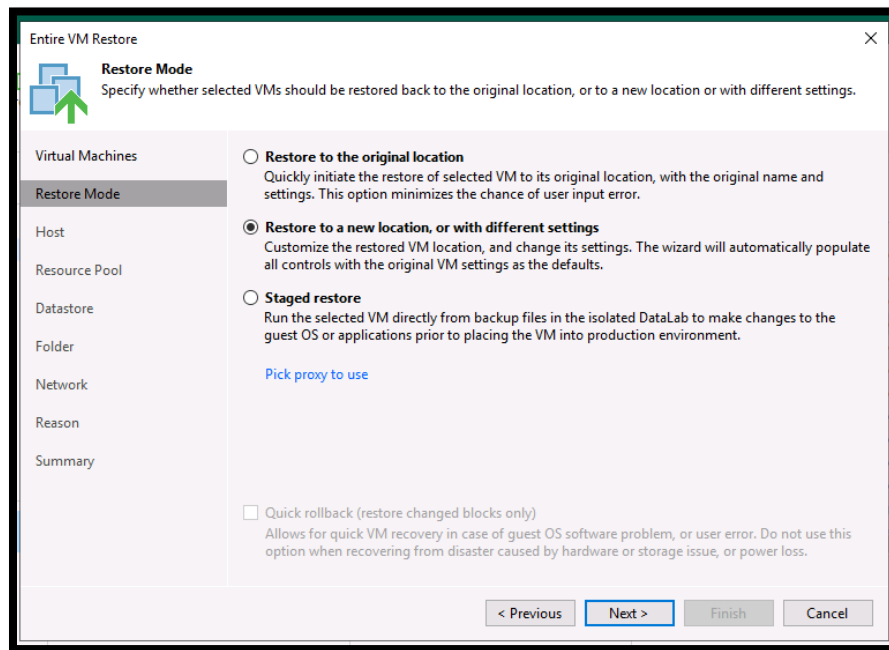


Imagen 11: Modo restore.

El paso de Host del asistente está disponible si ha elegido cambiar la ubicación y la configuración de la máquina virtual restaurada.

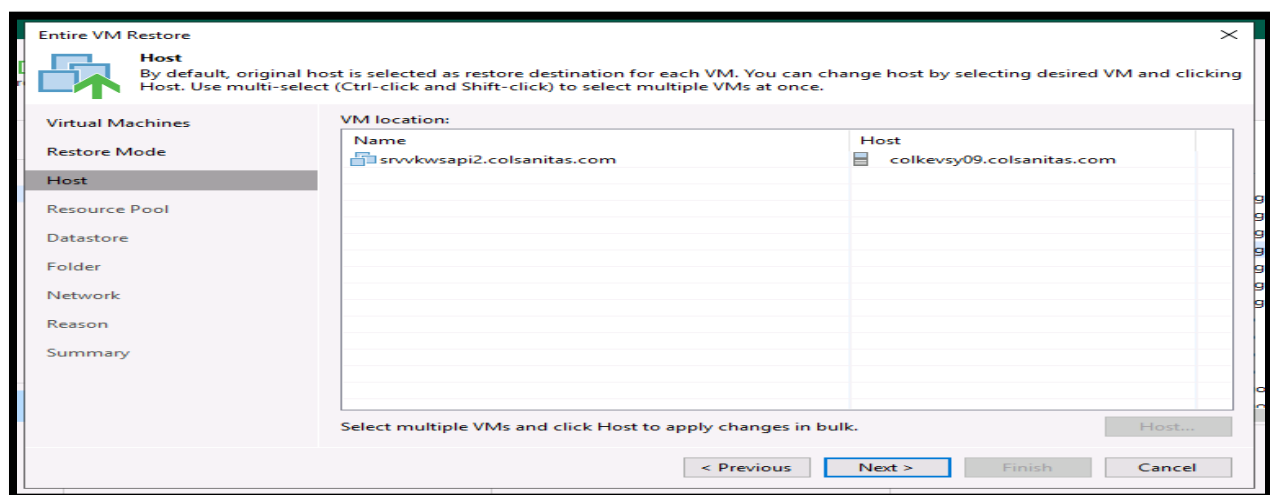


Imagen 12: Ubicación máquina virtual.

En este paso le permite cambiar el pool de recursos.

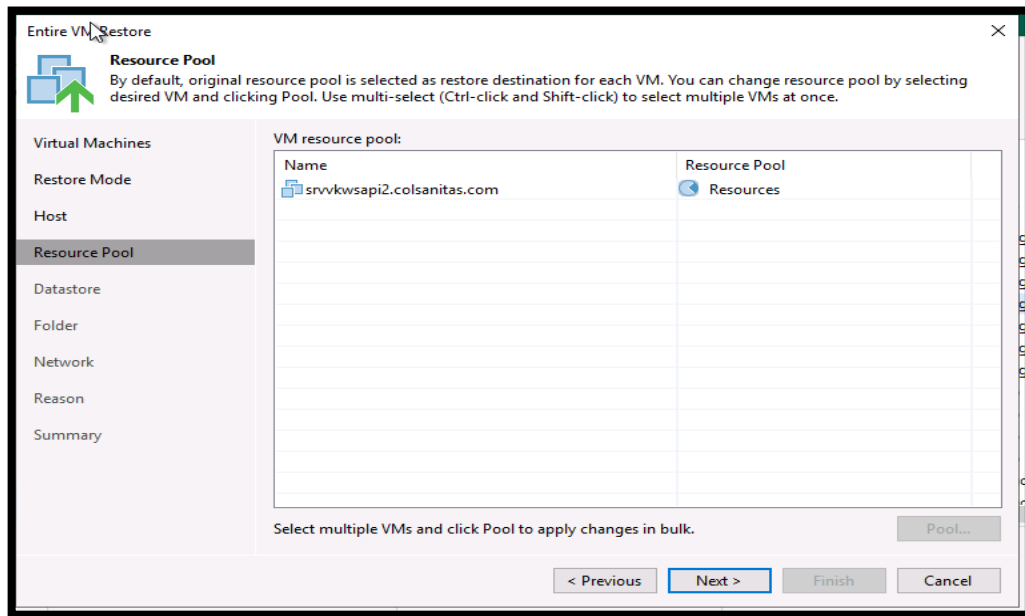


Imagen 13: Grupo recursos.

En este paso le permite escoger el datastore que mejor se acomode a la restauración.

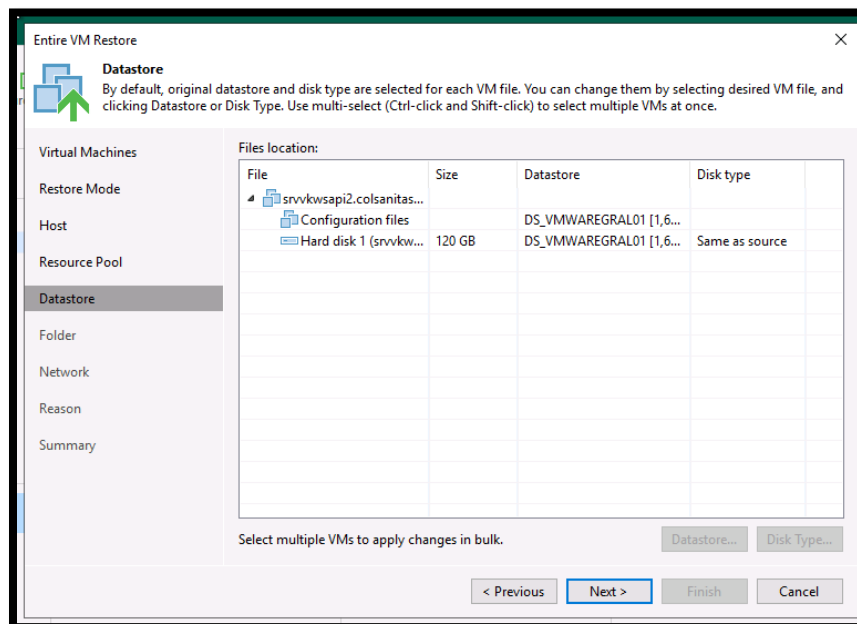


Imagen 14: Ubicación datastore.

Seleccione la ubicación de la maquina restaurada, esta opción le permite cambiar el nombre en

caso de que no quiera afectar la maquina origina

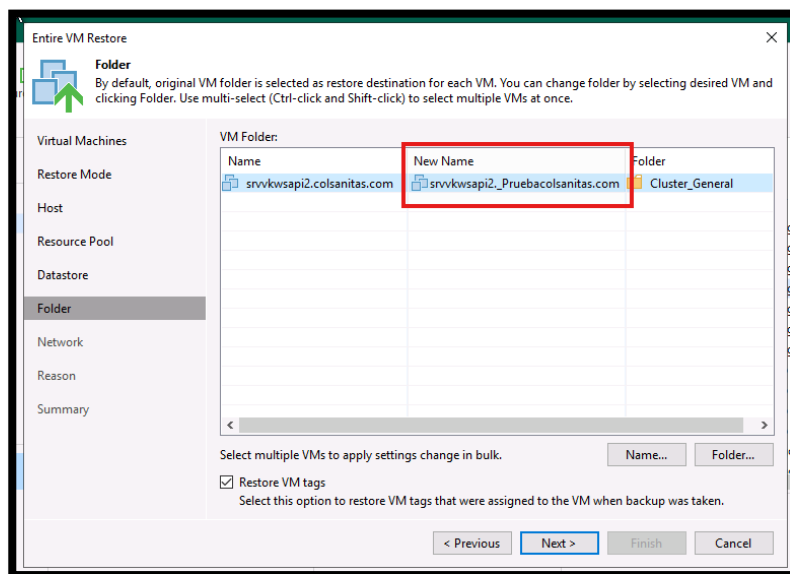


Imagen 15: Cambio nombre máquina virtual.

En este paso le permite seleccionar la red a desplegarse en la maquina virtual.

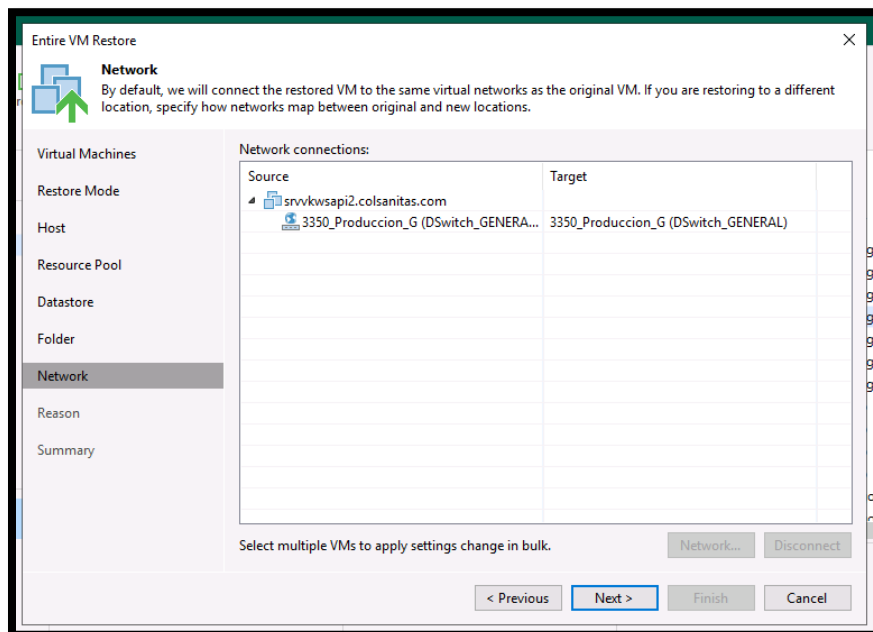
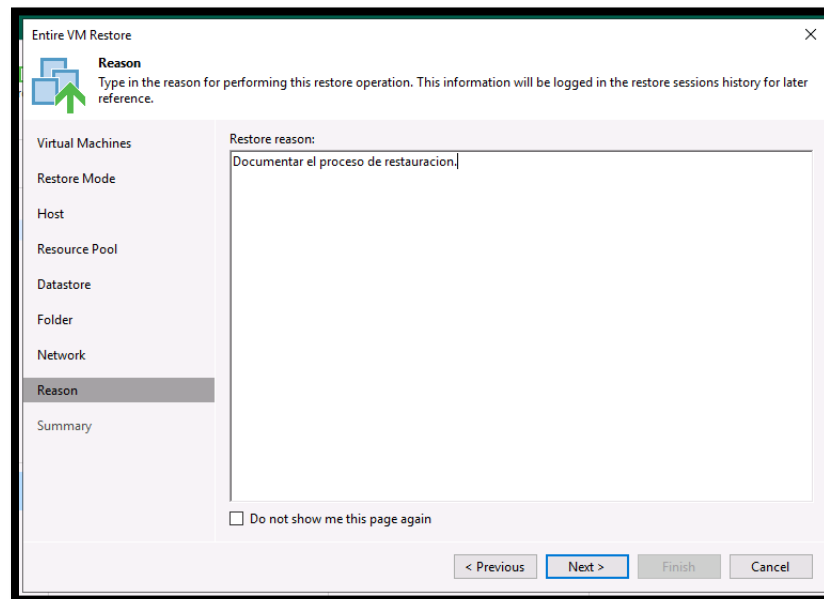


Imagen 16: Selección red.

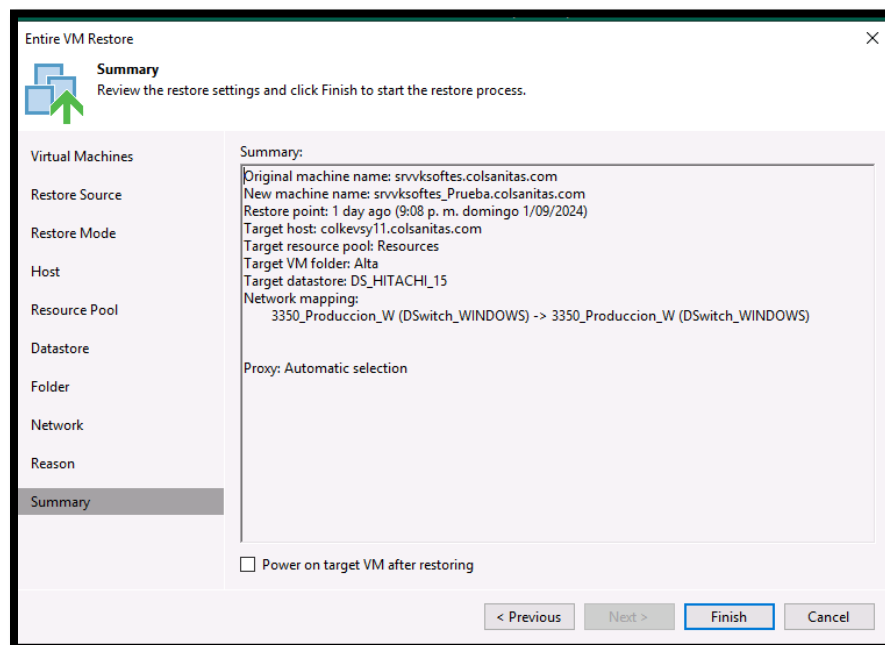
Opcional, indicar la razón del proceso en cuestión.



The screenshot shows the 'Entire VM Restore' window with the 'Reason' tab selected. The left sidebar lists various configuration options: Virtual Machines, Restore Mode, Host, Resource Pool, Datastore, Folder, Network, Reason (selected), and Summary. The main area is titled 'Reason' and contains a text box for 'Restore reason:' with the text 'Documentar el proceso de restauracion.' entered. Below the text box is a checkbox labeled 'Do not show me this page again' which is unchecked. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

Imagen 16: Reason restore.

Podemos evidencia un resumen antes de ejecutar el proceso.



The screenshot shows the 'Entire VM Restore' window with the 'Summary' tab selected. The left sidebar is the same as in the previous image, but 'Summary' is now selected. The main area is titled 'Summary' and contains a text box with the following details: 'Original machine name: srvksoftes.colsanitas.com', 'New machine name: srvksoftes_Prueba.colsanitas.com', 'Restore point: 1 day ago (9:08 p. m. domingo 1/09/2024)', 'Target host: colkevsy11.colsanitas.com', 'Target resource pool: Resources', 'Target VM folder: Alta', 'Target datastore: DS_HITACHI_15', 'Network mapping: 3350_Produccion_W (DSwitch_WINDOWS) -> 3350_Produccion_W (DSwitch_WINDOWS)', and 'Proxy: Automatic selection'. Below the text box is a checkbox labeled 'Power on target VM after restoring' which is unchecked. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

Imagen 17: Resumen configuración restore.

Adicional podemos evidenciar el avance de la restauración.

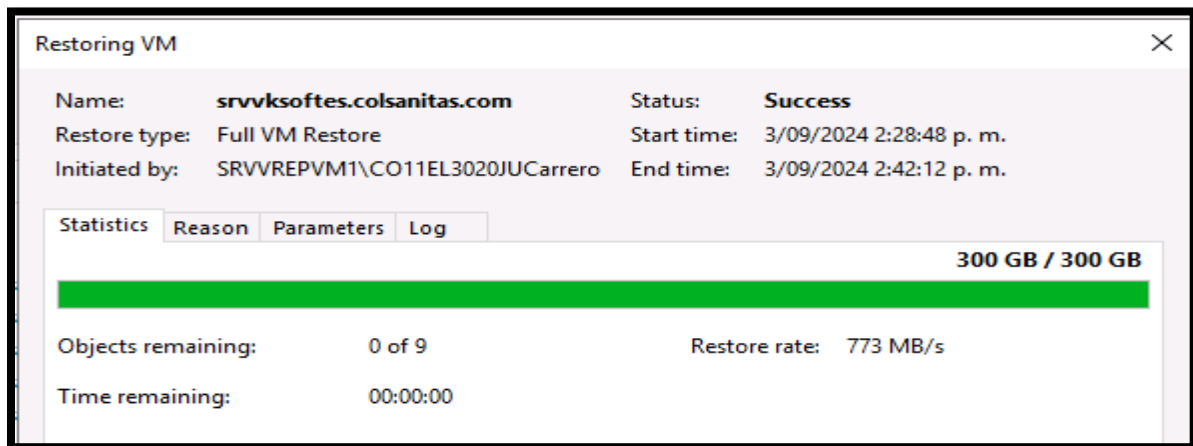


Imagen 18: Estadística restore.

Evidencia de una restauración.

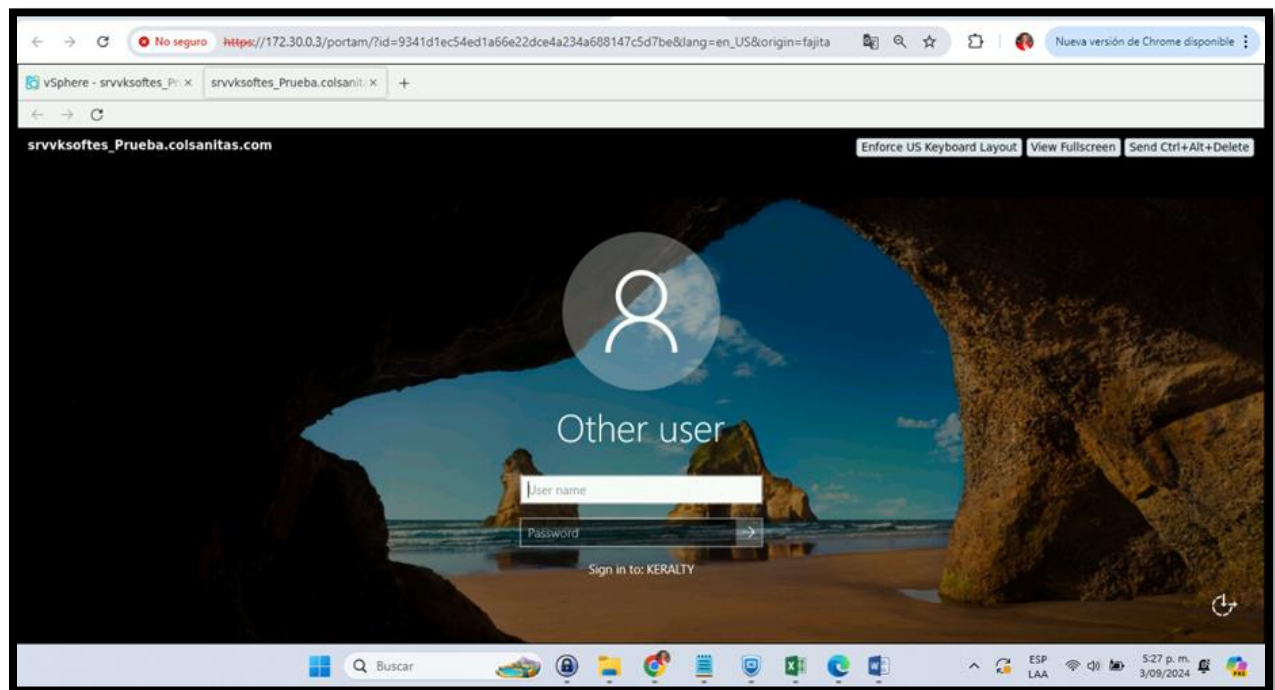


Imagen 19: Evidencia restore pantalla VMware.

Proceso de Veeam Recovery Orchestrator

Veeam Recovery Orchestrator (Orchestrator) amplía la funcionalidad de Veeam Data Platform al orquestar procesos de recuperación, con planes de recuperación de un solo clic para

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

aplicaciones críticas y funciones avanzadas para documentación y pruebas.

Orchestrator aprovecha las capacidades de recuperación de Veeam Backup & Replication para crear flujos de trabajo de recuperación ante desastres, automatizar los procesos de recuperación y eliminar los pasos manuales propensos a errores. Orchestrator también proporciona capacidades de generación de informes que permiten a las empresas documentar sus planes de recuperación ante desastres para cumplir con los requisitos de cumplimiento. Con Orchestrator, puede hacer lo siguiente.

Orqueste la recuperación: cree flujos de trabajo para orquestar operaciones de recuperación tanto para máquinas virtuales como físicas en entornos de nube VMware vSphere y Microsoft Azure.

Automatice controles y pruebas: programe controles y pruebas para automatizar la verificación de los planes de recuperación, con funciones como laboratorios de pruebas aislados y controles de preparación integrales.

Cumpla con los requisitos de cumplimiento: vea los logros de RPO y RTO en el panel y genere informes actualizados automáticamente para controles, pruebas y ejecuciones del plan de recuperación, lo que garantiza que se cumplan los requisitos de cumplimiento y auditoría.

Servidor Veeam Orchestrator

El servidor de Orchestrator es el núcleo de configuración, administración y gestión de la arquitectura de Orchestrator. Aquí es donde se crean, auditan, prueban y ejecutan los planes de recuperación. Internamente, el servidor de Orchestrator está compuesto por los siguientes componentes:

Servicio de servidor Veeam Orchestrator: es responsable de gestionar los planes de recuperación y administrar los roles y permisos de los usuarios.

Veeam Orchestrator Web UI: Es una interfaz de usuario basada en web que permite a los usuarios interactuar con el servicio de servidor Veeam Orchestrator y realizar diversas acciones de configuración y administración.

Veeam Backup & Replication Server: Se instala con el servidor Orchestrator para suministrar bibliotecas de Veeam PowerShell y admitir determinados escenarios de recuperación ante desastres. Se lo denomina servidor "integrado". El servidor funciona como un servidor Veeam Backup & Replication completamente funcional.

SQL Server: Se utiliza para alojar datos de configuración. Se puede instalar una instancia de Microsoft SQL Server Express de forma local. Sin embargo, para obtener el mejor rendimiento y escalabilidad, se recomienda la edición Microsoft SQL Server Enterprise, que puede ser un servidor remoto.

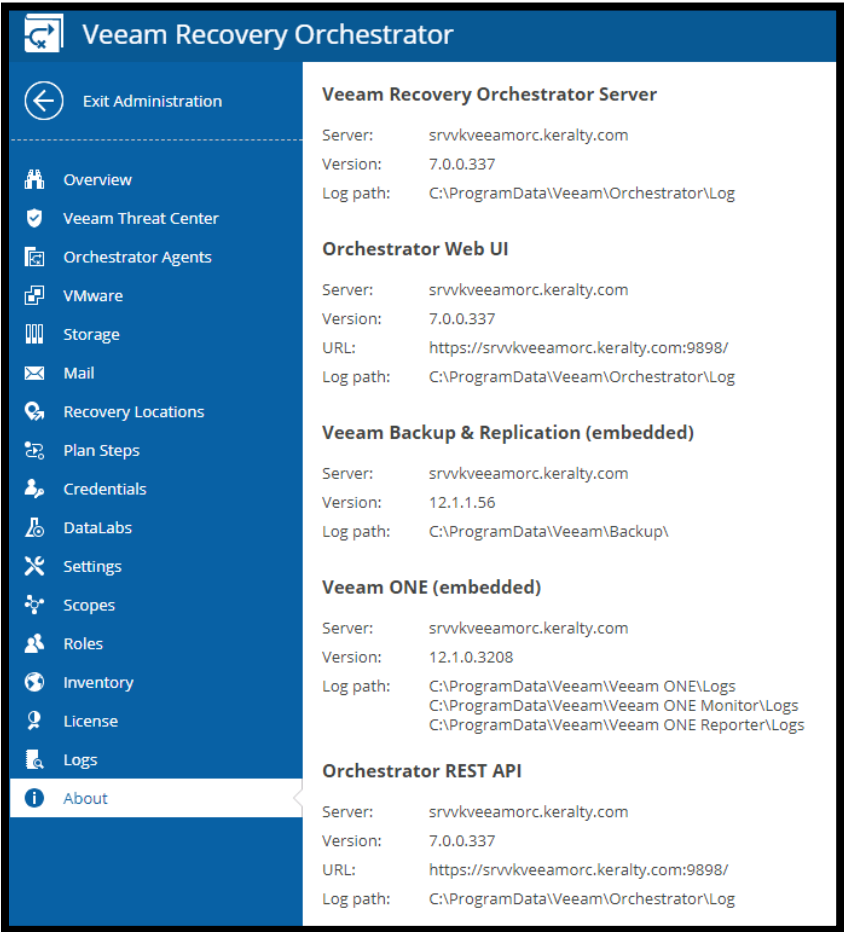


Imagen 20: Detalle Veeam Recovery Orchestrator

Servidores de replicación y backup de Veeam.

Implemente un agente Orchestrator en cada uno de sus servidores de Veeam Backup & Replication para orquestar la recuperación de las máquinas protegidas.




Status	Veeam Server ↑	Server Type	Server Version	Agent Version
✓ Healthy	 10.160.5.32	Veeam Backup Enterprise Manager	12.1.2.172	7.0.0.337
✓ Healthy	 SRVVKVEEAMORC	Veeam Backup & Replication server (Embedded)	12.1.1.56	7.0.0.337
✓ Healthy	 srvvrepvm1.keralty.com	Veeam Backup & Replication server (Managed by EM)	12.1.2.172	7.0.0.337

Imagen 21: Servidores configurados Orchestrator.

Se despliega agente de orchestrator en tres tipos de servidores.

10.160.5.32: Veeam Backup Enterprise Manager- servicio instalado en el servidor de VB&R

srvvkveeamorc: Servidor designado para desplegar el servicio de Veeam Recovery Orchestrator

srvvrepvm1.keralty.com: Servidor con el servicio principal de Veeam backup & replication.

Orquestación de la restauración en VMware vSphere

Este escenario de implementación ilustra la recuperación en un entorno VMware vSphere desde copias de seguridad de máquinas virtuales vSphere y agentes de Veeam creadas por Veeam Backup & Replication.

En este escenario, las cargas de trabajo físicas están protegidas por Veeam Agent for Windows o Veeam Agent for Linux, y las cargas de trabajo de las máquinas virtuales de vSphere están protegidas por Veeam Backup & Replication. Todas estas cargas de trabajo se pueden recuperar en el entorno VMware vSphere como máquinas virtuales. Orchestrator puede utilizar repositorios de copia de seguridad tanto primarios como de copia, y aprovechar tanto Veeam Secure Restore como Veeam Instant VM Recovery mientras recupera copias de seguridad de agentes y máquinas virtuales como nuevas máquinas virtuales de vSphere

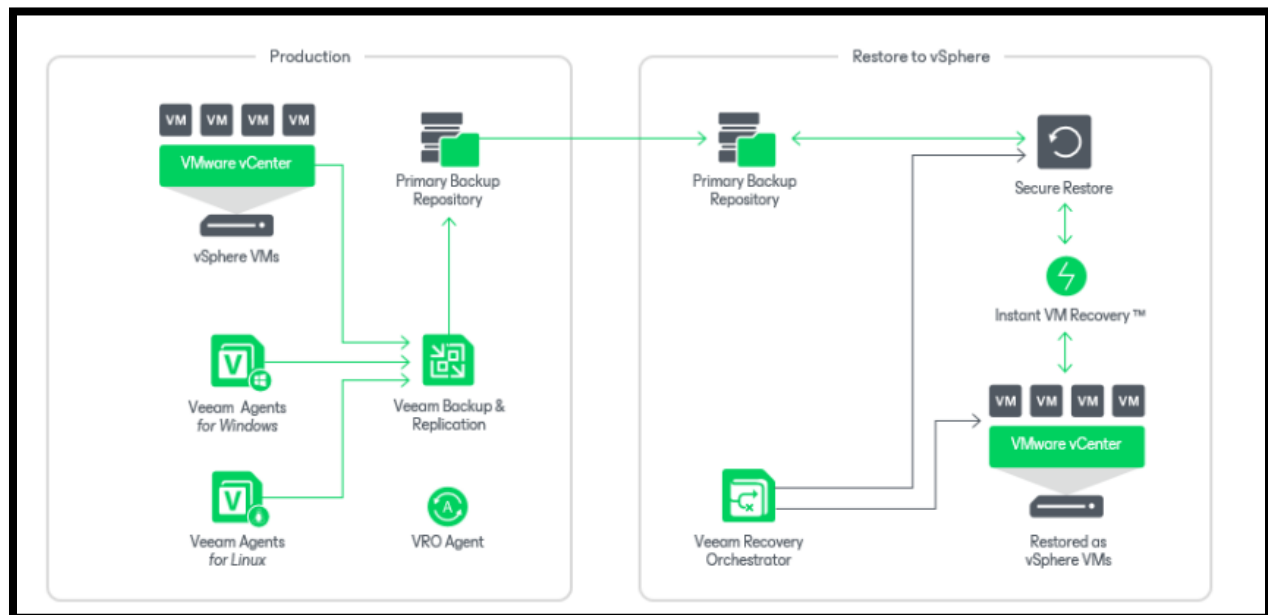


Imagen 34: Arquitectura Veeam Recovery Orchestrator.

Ubicaciones de recuperación.

Las ubicaciones de recuperación de VMware se utilizan para definir recursos de cómputo y almacenamiento en un entorno de vSphere necesarios al ejecutar planes de restauración.

Antes de ejecutar un plan de restauración o realizar una operación de conmutación por recuperación, puede elegir si desea recuperar las máquinas en la ubicación original o en una nueva.

Si desea restaurar las máquinas virtuales a su ubicación original, no necesita configurar ningún recurso. Sin embargo, la ubicación original de la máquina virtual no se aplica a las copias de seguridad del agente de Veeam, solo a las copias de seguridad de máquinas virtuales de vSphere.

Orchestrator ya incluye una ubicación de recuperación incorporada denominada Ubicación de la máquina virtual original. Si selecciona esta ubicación, Orchestrator detectará automáticamente la ubicación original de las máquinas virtuales procesadas y las restaurará a esa ubicación.

Puede personalizar el nivel de capacidad del almacén de datos, establecer la preferencia de copia de seguridad, permitir la recuperación de máquinas virtuales en diferentes ubicaciones y habilitar la recuperación instantánea de máquinas virtuales para la ubicación. Para obtener más información, consulte Configuración de la ubicación de recuperación original.

Si desea restaurar máquinas en una ubicación diferente, primero debe categorizar los recursos de vCenter Server en ubicaciones de recuperación de VMware.




Location ↑	Type	Agents	VMs	Plan	Instant VM R...	Storage Syste...	Description
Original VM Location	 VMware	N/A	✓ Enabled	-	Enabled	N/A	Original locati...
vCenter Contingencia	 VMware	✗ Disabled	✓ Enabled	25 Plans ▾	Enabled	N/A	
vCenter GCP	 VMware	✗ Disabled	✓ Enabled	-	Enabled	N/A	

Imagen 23: Ubicación recuperación.

Actualmente se tienen presentadas en el Veeam recovery orchestrator 3 ubicaciones de recuperación

syvcenterosi.colsanitas.com VMware Ubicación Original.

10.160.5.21 VMware Ubicación de contingencia

10.24.0.2 VMware GCP

Grupos de inventario

Los grupos de inventario son conjuntos de máquinas virtuales que son administradas por el servidor Veeam ONE integrado instalado en el servidor Orchestrator.

Para crear planes de recuperación, utilizará uno o más grupos de inventario que contienen objetos para recuperar. La mayoría de los grupos de inventario se crean automáticamente, en función de los elementos detectados, como trabajos de Veeam Backup & Replication y grupos de protección, almacenes de datos de vSphere o etiquetas de máquinas virtuales de vSphere. A menos que se agregue un grupo de inventario a la lista de elementos de inventario para al menos un ámbito con el rol de usuario de autor del plan o administrador asignado, no estará disponible para su uso en el ámbito. Para obtener más información,















<input type="checkbox"/> Group ↑	Scope
Selected: 0 of 208	
<input type="checkbox"/>  0 Veeam Backup:10.160.5.32	Default Scope
<input type="checkbox"/>  0 Veeam Backup:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  1 EBS:10.160.5.32	Default Scope
<input type="checkbox"/>  1 EBS:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  1. EBS_Backup_Alta:10.160.5.32	Default Scope
<input type="checkbox"/>  1. EBS_Backup_Alta:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  2 Transversales:10.160.5.32	Default Scope
<input type="checkbox"/>  2 Transversales:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  2. Transversales_Backup_Alta:10.160.5.32	Default Scope
<input type="checkbox"/>  2. Transversales_Backup_Alta:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  3 Avicena:10.160.5.32	Default Scope
<input type="checkbox"/>  3 Avicena:srvvrepvm1.keralty.com	Default Scope
<input type="checkbox"/>  3. Avicena_Backup_Alta:10.160.5.32	Default Scope
<input type="checkbox"/>  3. Avicena_Backup_Alta:srvvrepvm1.keralty.com	Default Scope

Imagen 24: Grupo aplicaciones 1.

Planes de recuperación.

Orchestrator utiliza la funcionalidad de recuperación de datos y conmutación por error que ofrece Veeam Backup & Replication para automatizar las acciones de recuperación. Además, Orchestrator proporciona una orquestación de recuperación de máquinas virtuales de vSphere basada en instantáneas de almacenamiento replicadas creadas en sistemas de almacenamiento HPE. Para estos fines.

Si desea recuperar máquinas de las copias de seguridad del agente vSphere y Veeam en un entorno VMware vSphere, puede crear un plan de restauración.

Después de crear y configurar un plan de restauración, ejecutar una comprobación de preparación exitosa y una prueba, el plan se puede considerar listo para la restauración. Puede invocar varias acciones para el plan, según el estado actual del mismo.

Availability	Plan	↑ State	Scope	Latest Test	Latest Check	Recovery Location
⏸ Disabled	0 Veeam Backup - Replica	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:59:00 AM	N/A
⏸ Disabled	1 EBS Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 8:48:24 AM	vm vCenter Contingencia
⏸ Disabled	2 Transversales Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 8:55:06 AM	vm vCenter Contingencia
⏸ Disabled	3 Avicena Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/21/2024 3:30:46 PM	vm vCenter Contingencia
⏸ Disabled	4 Validador APP Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 9:46:51 AM	vm vCenter Contingencia
⏸ Disabled	5 Portal MP Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 8:57:03 AM	vm vCenter Contingencia
⏸ Disabled	6 Portal EPS Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 9:13:52 AM	vm vCenter Contingencia
⏸ Disabled	7 Xoma ODO OPT Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:12:40 AM	vm vCenter Contingencia
⏸ Disabled	8 Portal Prestadores Backup ...	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 9:44:47 AM	vm vCenter Contingencia
⏸ Disabled	10 Conector OSI Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:24:22 AM	vm vCenter Contingencia
⏸ Disabled	11 Konector Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:26:29 AM	vm vCenter Contingencia

Imagen 25: Grupo aplicaciones 2.

Availability	Plan	↑ State	Scope	Latest Test	Latest Check	Recovery Location
⏸ Disabled	13 Avicena RD Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:36:54 AM	vm vCenter Contingencia
⏸ Disabled	14 Avicena Peru Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 9:11:16 AM	vm vCenter Contingencia
⏸ Disabled	15 Otros Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 9:50:04 AM	vm vCenter Contingencia
⏸ Disabled	16 Monitoreo Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 8:51:16 AM	vm vCenter Contingencia
⏸ Disabled	17 Automatizacion Backup A...	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 10:02:50 AM	vm vCenter Contingencia
⏸ Disabled	18 Backup Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 10:14:25 AM	vm vCenter Contingencia
⏸ Disabled	19 Openshift Backup Media	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 9:08:44 AM	vm vCenter Contingencia
⏸ Disabled	20 Portal Osisanitas Backup ...	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:29:22 AM	vm vCenter Contingencia
⏸ Disabled	21 SQL Server Backup Alta	🔍 Needs Verified Check or test recommended	Default Scope	Never	Failed 8/23/2024 10:31:20 AM	vm vCenter Contingencia
⏸ Disabled	22 Avicena Backup Media	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:20:27 AM	vm vCenter Contingencia
⏸ Disabled	23 Monitoreo Backup Baja	🔍 Needs Verified Check or test recommended	Default Scope	Never	Passed 8/23/2024 10:32:29 AM	vm vCenter Contingencia

Imagen 26: Grupo aplicaciones 3.

Estados y modos del plan

Los planes de restauración pueden adquirir los siguientes estados predeterminados después de su creación. Los mismos estados se muestran después de restablecer un plan y después de completar una prueba o una verificación




Plan Estatal	Icono	Descripción
NECESITA VERIFICARSE		El plan nunca ha sido probado, nunca ha pasado una verificación de preparación o ha sido modificado desde la última prueba o verificación de preparación de DataLab.
NO VERIFICADO		El plan no ha podido ser probado o no ha pasado una verificación de preparación.
VERIFICADO		El plan ha sido probado con éxito o ha pasado una verificación de preparación.

Imagen 27: Estados y modos del plan.

Para restaurar las máquinas.

Plan de restauración a una ubicación de recuperación Orchestrator utiliza el siguiente algoritmo:

1. La solución analiza todos los hosts agregados a la ubicación como recursos informáticos para detectar el primer host disponible. Este es el host donde se registrará la primera máquina procesada.

Orchestrator aplica la asignación especificada en la tabla de asignación de red para la ubicación para establecer la configuración de red requerida de la máquina virtual recuperada.

Orchestrator comprueba si la configuración de red del host detectado coincide con la configuración de red requerida. Si estas configuraciones no coinciden, Orchestrator vuelve al paso 1.

2. En la lista de almacenes de datos conectados al host como recursos de almacenamiento, Orchestrator busca el primer almacén de datos que esté disponible y tenga suficiente capacidad. Este es el almacén de datos donde se almacenarán los archivos de la máquina. Para calcular la capacidad del almacén de datos y asegurarse de que tenga suficiente espacio para acomodar la máquina virtual recuperada, Orchestrator utiliza el umbral que usted especifica al crear o configurar la ubicación.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

3. Al calcular la cantidad de espacio libre disponible en un almacén de datos, Orchestrator supone que el archivo de intercambio de la máquina procesada también se restaurará en este almacén de datos. Orchestrator también tiene en cuenta que todos los archivos de disco de la máquina se restaurarán en el mismo almacén de datos que almacena el archivo. VMX, independientemente de si la máquina de origen almacena sus archivos de disco en varios almacenes de datos. Esto puede influir en la estimación de capacidad resultante y en la forma en que Orchestrator busca almacenes de datos para restaurar máquinas.

4. Cuando Orchestrator comienza a procesar la siguiente máquina, la solución busca en todos los hosts agregados a la ubicación como recursos computacionales para detectar el próximo host disponible:

Si Orchestrator detecta dicho host, este será el host donde se registrará la máquina.

Si no hay más hosts disponibles, Orchestrator utiliza el host detectado en el paso 1 para registrar la máquina.

Luego, Orchestrator pasa por los pasos 2 y 3 para detectar la red de destino y el almacén de datos de la máquina.

5. Orchestrator repite el paso 4 para todas las demás máquinas incluidas en el plan hasta que se restauren todas las máquinas. El orden en el que se procesan las máquinas depende de las opciones de recuperación de máquinas virtuales definidas al configurar el plan.

Si los almacenes de datos agregados a la ubicación de recuperación como recursos de almacenamiento superan el umbral de capacidad antes de que se restauren todas las máquinas, la falla de este paso para una máquina de un grupo crítico detiene el plan. Para solucionar el problema, configure la ubicación para agregar más almacenes de datos e intente ejecutar el plan detenido nuevamente.

Cómo selecciona Orchestrator los archivos de copia de seguridad.

Generalmente, al realizar una restauración a una ubicación de recuperación, Orchestrator examina la lista de todos los puntos de restauración creados para una máquina para elegir un punto de restauración que cumpla con el requisito de fecha especificado en el asistente del plan de ejecución. El archivo de copia de seguridad que contiene el punto de restauración elegido se utiliza para recuperar la máquina.

Sin embargo, cuando utiliza las funciones de copia de seguridad que ofrece Veeam Backup & Replication, tiene varias instancias de los mismos datos de copia de seguridad en diferentes ubicaciones. Esta situación puede influir en la forma en que Orchestrator elige los archivos de copia de seguridad para recuperar las máquinas.

En caso de que Orchestrator detecte 2 archivos de respaldo que contengan el punto de restauración elegido (un archivo creado por un trabajo de respaldo y el otro archivo creado por un trabajo de copia de respaldo), utiliza uno de estos archivos según la configuración de

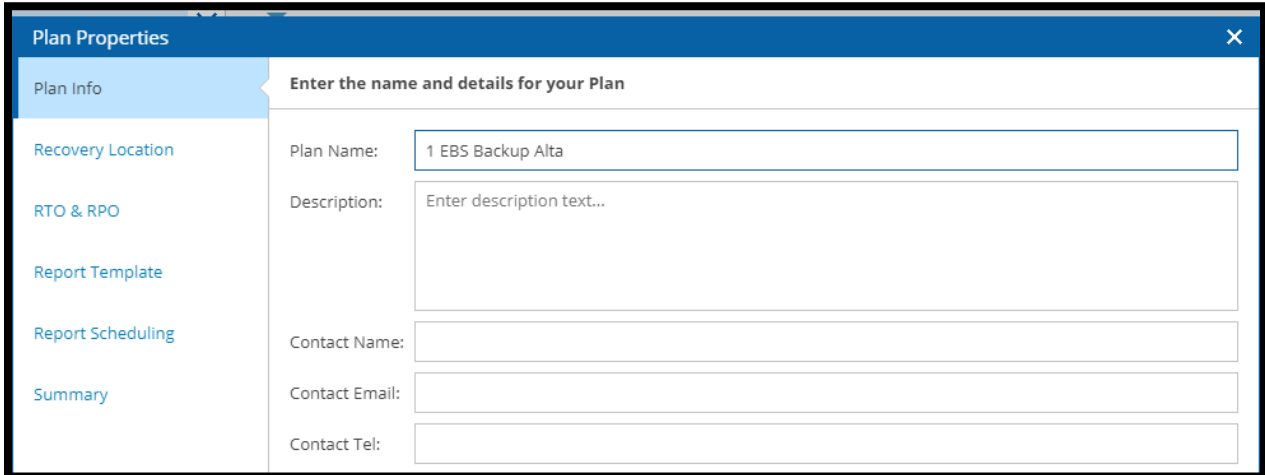
preferencia de copia de respaldo configurada para la ubicación de recuperación:

Con la preferencia de copia de seguridad deshabilitada, Orchestrator utiliza el archivo de copia de seguridad producido por el trabajo de copia de seguridad.

Con la preferencia de copia de seguridad habilitada, Orchestrator utiliza el archivo de copia de seguridad producido por el trabajo.

Estructura de un plan de recuperación.

Nombre del plan

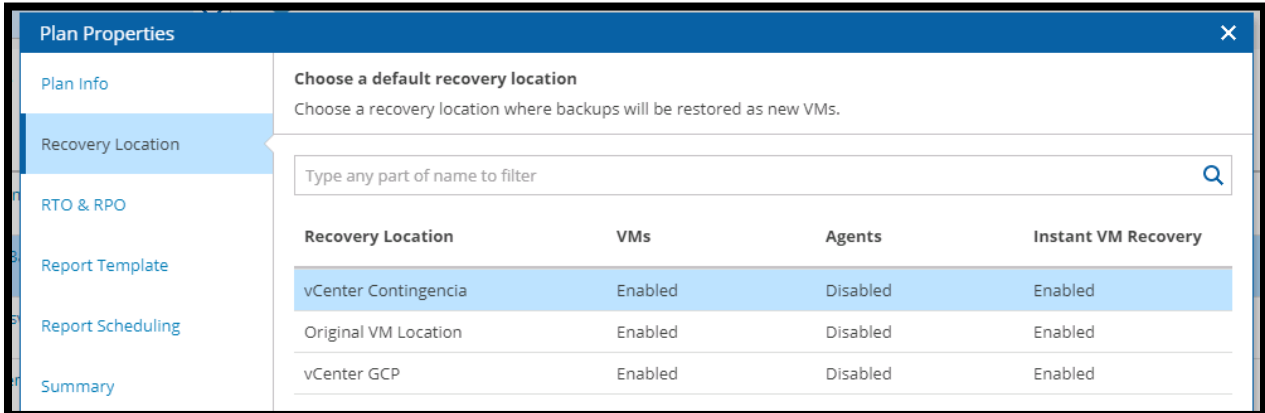


The screenshot shows a 'Plan Properties' dialog box with a sidebar on the left containing the following links: Plan Info (selected), Recovery Location, RTO & RPO, Report Template, Report Scheduling, and Summary. The main area is titled 'Enter the name and details for your Plan' and contains the following fields:

- Plan Name:** 1 EBS Backup Alta
- Description:** Enter description text...
- Contact Name:** (empty field)
- Contact Email:** (empty field)
- Contact Tel:** (empty field)

Imagen 28: Estructura plan recuperación.

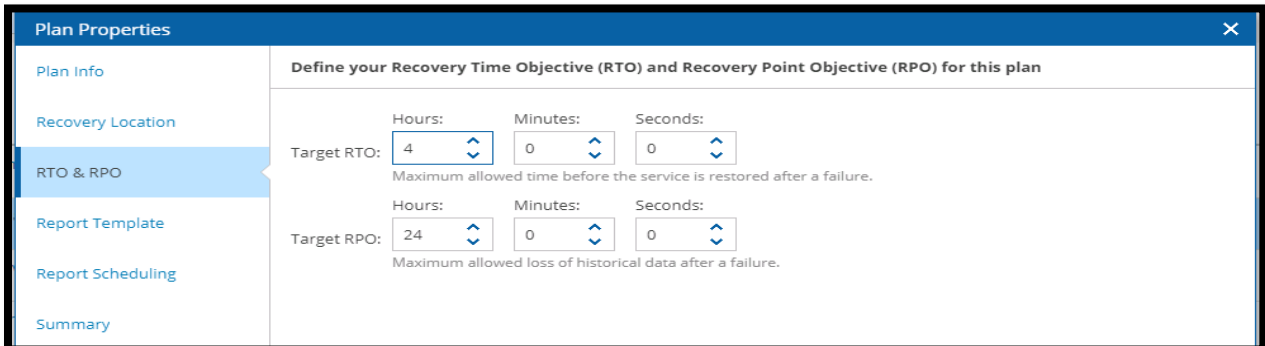
Ubicación de recuperación



Recovery Location	VMs	Agents	Instant VM Recovery
vCenter Contingencia	Enabled	Disabled	Enabled
Original VM Location	Enabled	Disabled	Enabled
vCenter GCP	Enabled	Disabled	Enabled

Imagen 29: Ubicación recuperación.

Configuración de RTO y RPO



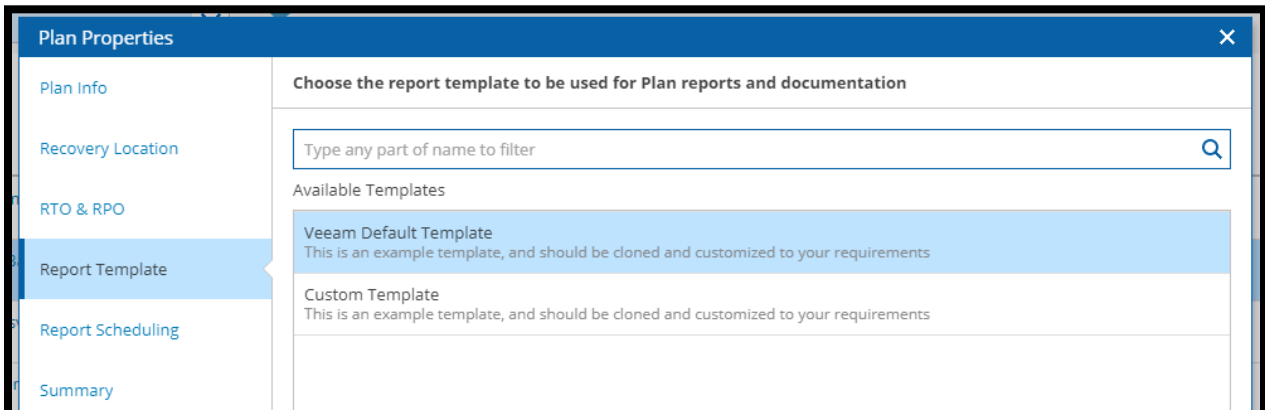
Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan

Target RTO: Hours: 4, Minutes: 0, Seconds: 0
Maximum allowed time before the service is restored after a failure.

Target RPO: Hours: 24, Minutes: 0, Seconds: 0
Maximum allowed loss of historical data after a failure.

Imagen 30: Configuración RTO y RPO.

Plantilla de Reportes



Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

- Veeam Default Template
This is an example template, and should be cloned and customized to your requirements
- Custom Template
This is an example template, and should be cloned and customized to your requirements

Imagen 31: Plantilla reportes.

Resumen de la configuración

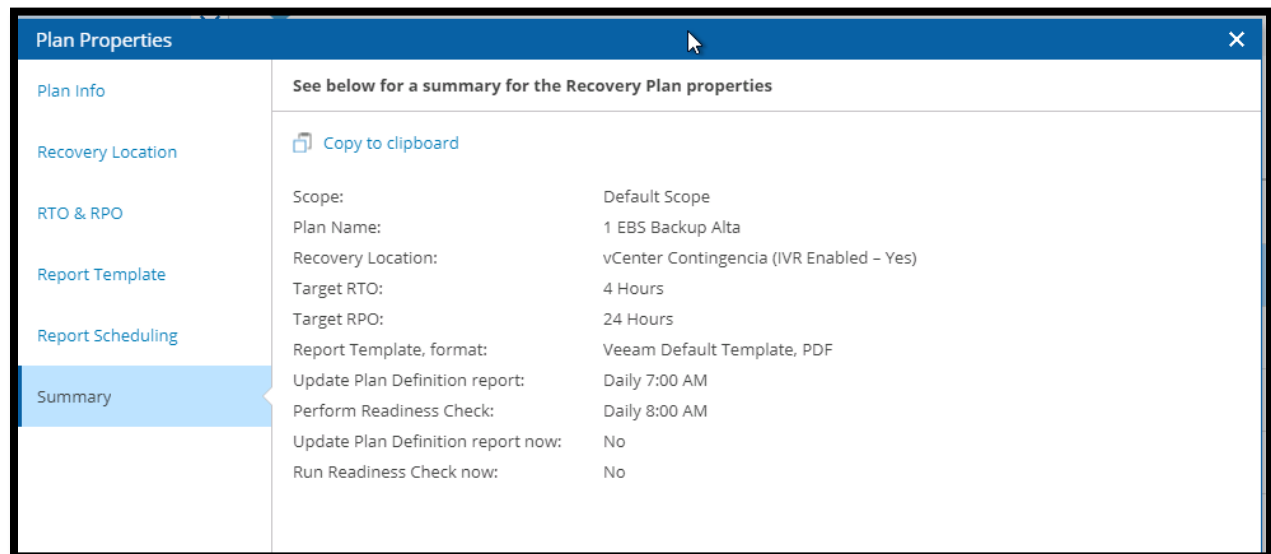


Imagen 32: Resumen configuración.

Pasos de ejecución del plan

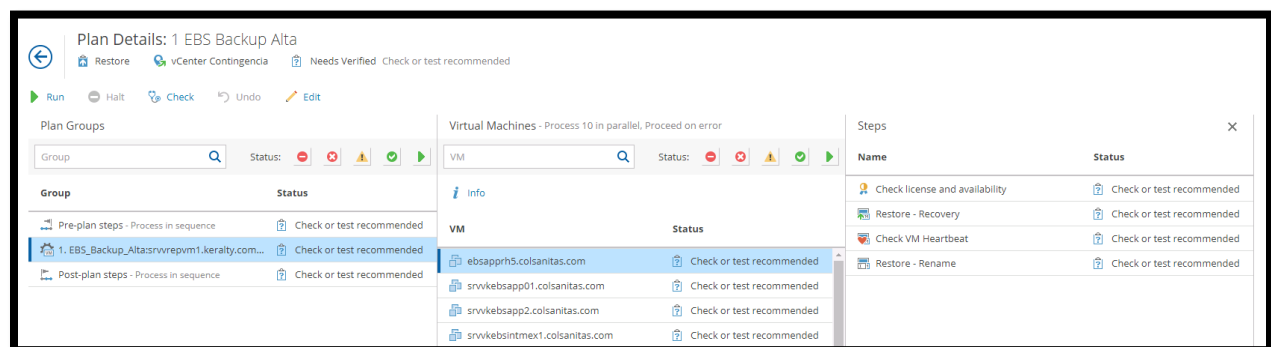


Imagen 33: Pasos ejecución plan.

Proceso de Chequeo

La opción de chequeo está diseñada para garantizar que las copias de seguridad son recuperables y que los datos están íntegros y accesibles. Esto es crucial para evitar sorpresas durante un proceso de recuperación real.

Beneficios de la Opción de Chequeo

Aumento de la Confianza: Proporciona confianza en que los datos están respaldados correctamente y pueden ser recuperados cuando sea necesario.

Proactividad: Permite detectar problemas antes de que se conviertan en situaciones críticas, facilitando la resolución anticipada.

Eficiencia en la Recuperación: Asegura que, en caso de necesitar una restauración, el proceso se realice sin contratiempos, ya que los datos han sido validados.

Plan Groups		Virtual Machines - Process 10 in parallel, Proceed on error		Steps	
Group	Status	VM	Status	Name	Status
Pre-plan steps - Process in sequence	Completed			Check license and availability	Completed
Post-plan steps - Process in sequence	Completed			Restore - Recovery	Completed
5.Portail MP_Backup_Altasrvvrepvm1.keralty.com - Proce...	Completed	srvmkas5n01.colsanitas.com	Completed	Check VM Heartbeat	Completed
		srvmkfsasegura.colsanitas.com	Completed	Restore - Migrate	Completed
		srvmkifdpx1.colsanitas.com	Completed	Restore - Rename	Completed
		srvmkifdpx2.colsanitas.com	Completed		

Imagen 34: Chequeo plan.

Proceso de respaldo y restauración con Dataprotector.

Data Protector es una solución de copia de seguridad que ofrece protección de datos confiable y alta accesibilidad para los datos de su empresa en rápido crecimiento. Data Protector ofrece una funcionalidad integral de copia de seguridad y restauración diseñada específicamente para entornos distribuidos y de toda la empresa. Data Protector se puede utilizar en entornos que van desde un solo sistema hasta miles de sistemas en varios sitios.

Actualmente la herramienta de respaldo de dataprotector asegura la información de Filesystem SQL y Oracle.

Estos respaldos son asegurados en discos de los Storeonce y cintas. Bajo un esquema de Transacción, Incrementales y copias completas.

Versión actual. 10.91.

Servidor: srvmcmtriara2.keralty.com (10.160.5.31)

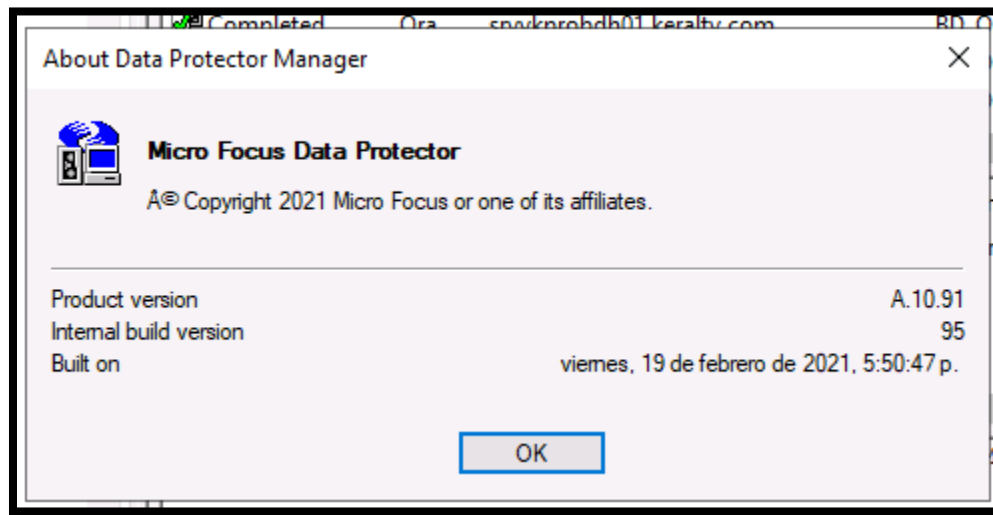


Imagen 35: Versión Data Protector.

Componentes

Administrador de celdas

El administrador de celdas es el sistema principal que controla la celda Data Protector desde un punto central, donde se instala el software principal de Data Protector con el IDB. El administrador de celdas ejecuta los administradores de sesiones que controlan las sesiones de copia de seguridad y restauración y escriben información de las sesiones en el IDB. El IDB realiza un seguimiento de los archivos respaldados, así como de la configuración de la celda Data Protector.

Servidor de instalación

El servidor de instalación es el equipo en el que se almacena el repositorio de software de Data Protector. Se necesita al menos un servidor de instalación para UNIX y otro para el entorno Windows para poder realizar instalaciones remotas a través de la red y distribuir los componentes de software a los sistemas cliente de la celda.

Sistemas de clientes

Después de instalar el software Data Protector en el sistema Cell Manager, puede instalar los componentes de Data Protector en todos los sistemas de la celda. Estos sistemas se convierten en clientes de Data Protector. La función de un cliente depende del software Data Protector que haya instalado en este sistema.

Sistemas que se deben respaldar

Los sistemas cliente de los que desea realizar una copia de seguridad deben tener instalado el agente de disco Data Protector (DA, también llamado agente de copia de seguridad). El agente de disco lee o escribe datos de un disco en el sistema y envía o recibe datos de un agente de medios. El agente de disco también está instalado en el administrador de celdas, lo que le permite realizar copias de seguridad de los datos en el administrador de celdas, la configuración de Data Protector y la IDB.

Sistemas con dispositivos de respaldo

Los sistemas cliente con dispositivos de copia de seguridad conectados deben tener instalado un agente de medios (MA) de Data Protector. Un agente de medios lee o escribe datos de los medios del dispositivo y envía o recibe datos del agente de discos. Un dispositivo de copia de seguridad se puede conectar a cualquier sistema y no solo al administrador de celdas. Los sistemas cliente con dispositivos de copia de seguridad también se denominan servidores de unidades. Un sistema cliente con varios dispositivos de copia de seguridad se denomina servidor de múltiples unidades.

Diagrama de la arquitectura de respaldo con dataprotector.

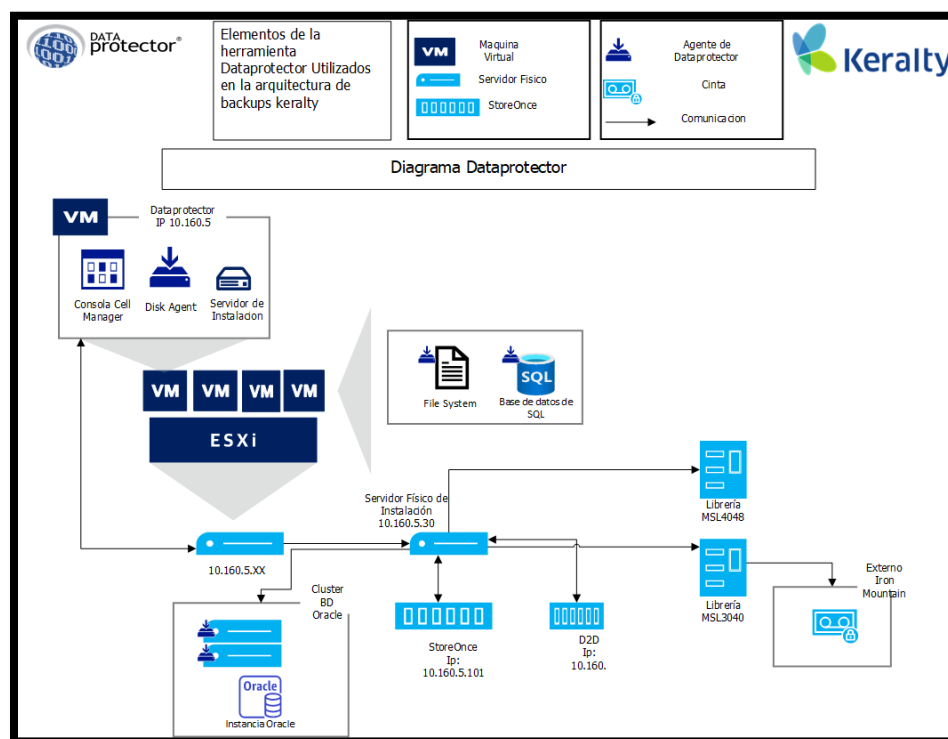


Imagen 36: Arquitectura Data Protector.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

Cuando se inicia una sesión de copia de seguridad

El proceso Backup Sesión Manager (BSM) se inicia en el sistema Cell Manager y controla la sesión de copia de seguridad. Este proceso lee la especificación de copia de seguridad para obtener información sobre qué se debe respaldar y qué opciones, medios y dispositivos se deben usar para la copia de seguridad.

El BSM abre el IDB y escribe en el IDB información sobre la sesión de respaldo, como mensajes generados, detalles sobre los datos respaldados y los dispositivos y medios que se usaron para la sesión.

El BSM inicia los agentes de medios (MA) en los sistemas con dispositivos configurados para realizar copias de seguridad. Se inicia un nuevo agente de medios para cada unidad utilizada en paralelo. La cantidad de agentes de medios que se pueden iniciar en la celda está limitada por la configuración de la celda y la cantidad de licencias que haya adquirido.

En una sesión de respaldo con duplicación de objetos, el BSM también inicia los agentes de medios que se utilizarán para la duplicación.

El BSM inicia los agentes de disco (DA) para cada disco que se va a respaldar en paralelo. La cantidad real de agentes de disco que se inician depende de la concurrencia de agentes de disco configurados en la especificación de respaldo. Esta es la cantidad de agentes de disco que se pueden iniciar para enviar datos en paralelo a un agente de medios, lo que permite que un dispositivo realice transmisiones.

Los agentes de disco leen datos de los discos y los envían a los agentes de medios que escriben datos en los medios.

En una sesión de copia de seguridad con duplicación de objetos, los agentes de medios utilizados para escribir objetos duplicados se conectan en cadena. Cada agente de medios escribe los datos recibidos en el medio y los reenvía al siguiente agente de medios en la cadena.

El BSM supervisa el progreso de la sesión e inicia nuevos Agentes de disco y nuevos Agentes de medios según sea necesario.

Cuando se completa la sesión de respaldo, el BSM cierra la sesión.

Proceso de restauración de un respaldo de Filesystem

De forma predeterminada, el objeto de copia de seguridad se restaura en la misma ruta desde la que se realizó la copia de seguridad. Los siguientes pasos muestran cómo realizar una restauración simple:

En la Lista de contexto, haga clic en Restaurar.

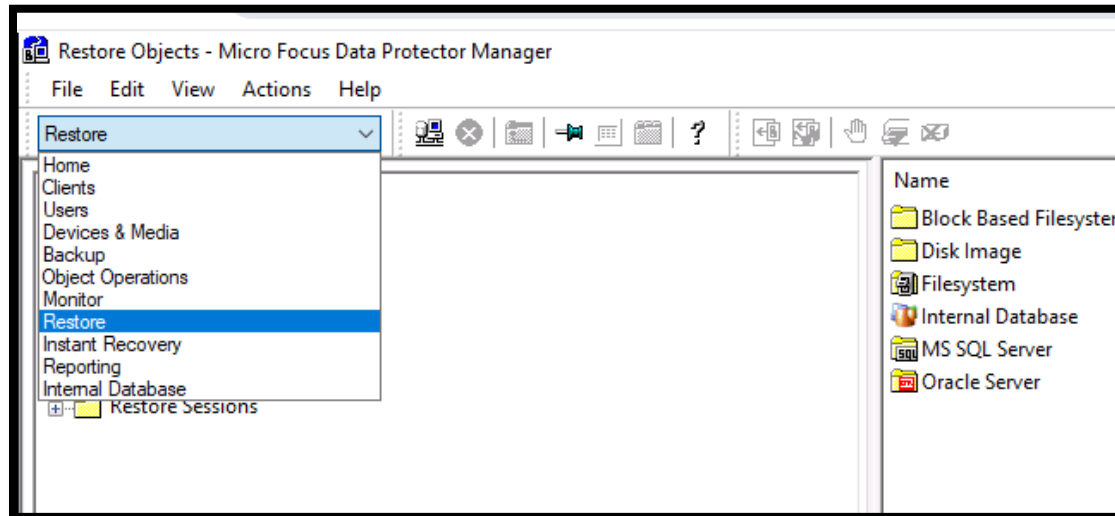


Imagen 37: Menú opción restore file system.

Seleccionar el servidor de cual quiere ejecutar la restauración.

La vista Restaurar aparece en el Área de resultados.

Busque y seleccione las casillas de verificación junto a los directorios/archivos que desea restaurar.

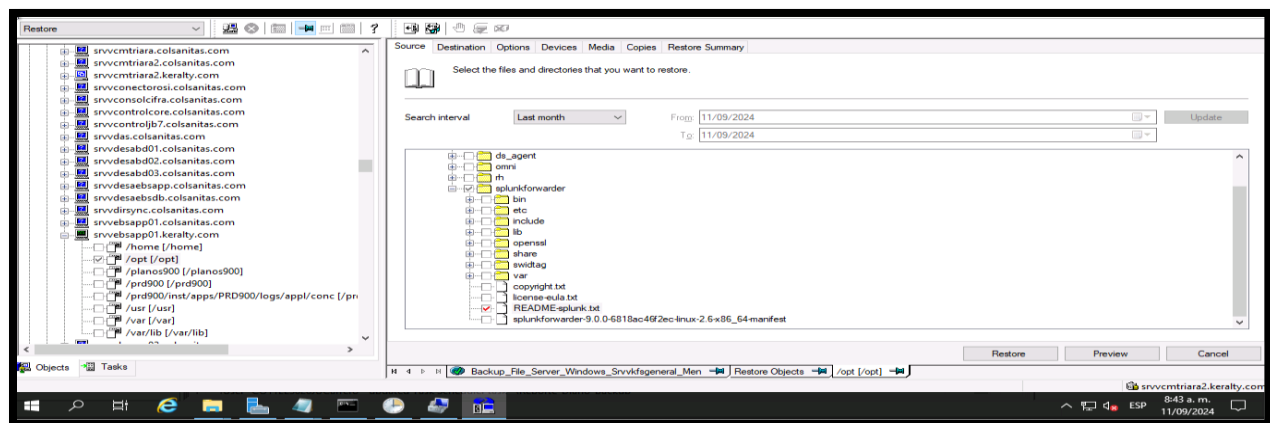


Imagen 38: Selección ruta restore.

Seleccione la pestaña Destino para elegir dónde desea restaurar. Si no selecciona nada, los directorios o archivos seleccionados se restaurarán a la ruta original.

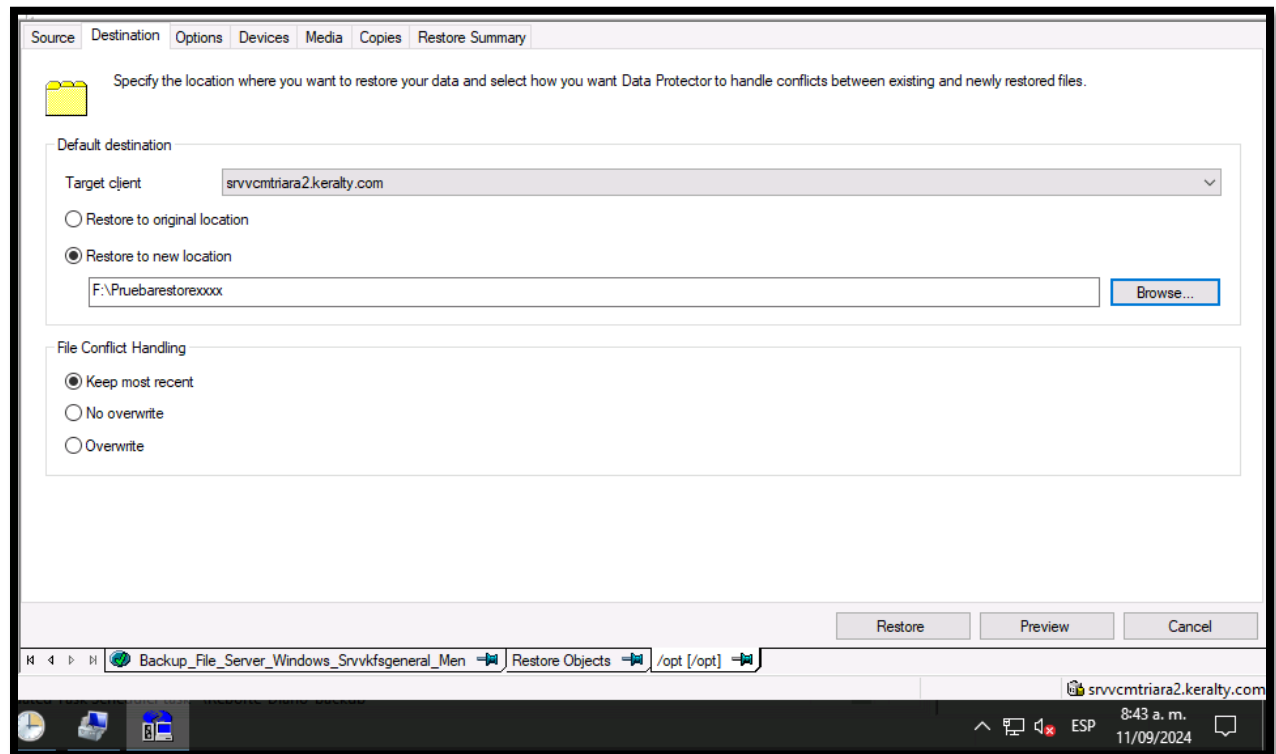


Imagen 39: Destino restore.

Valide el dispositivo que le permitirá la restauración.

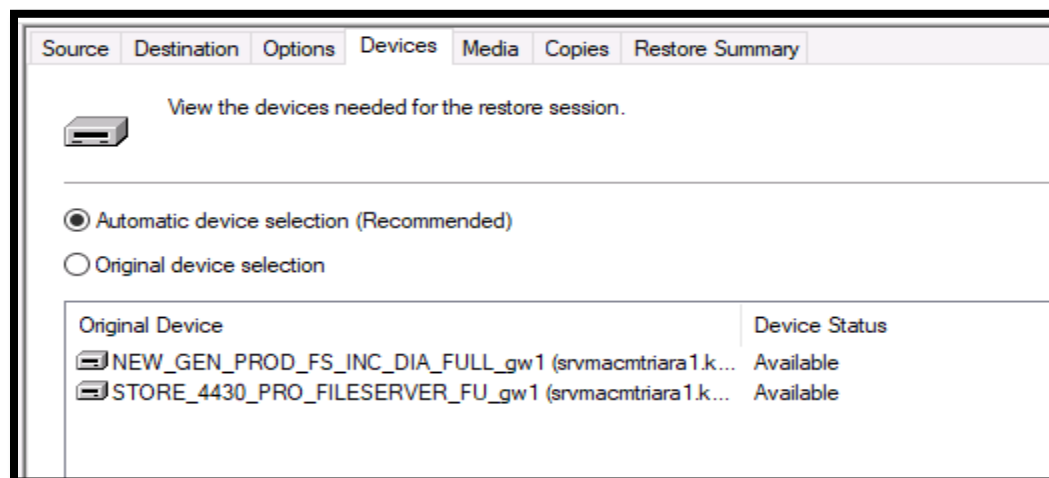


Imagen 40: Medios restore.

Si el respaldo está en cinta puede verificar el medio en el cual se ubico el respaldo.

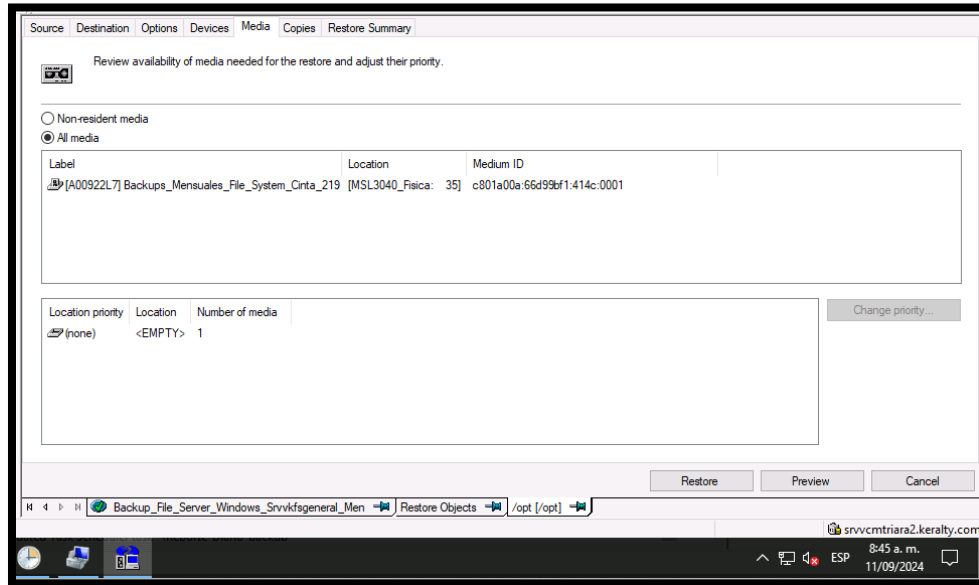


Imagen 41: Medios restore.

Haga clic en el botón Iniciar restauración. Aparecerá el asistente de restauración. Siga los valores predeterminados propuestos en el asistente (haga clic en Siguiente y Finalizar).

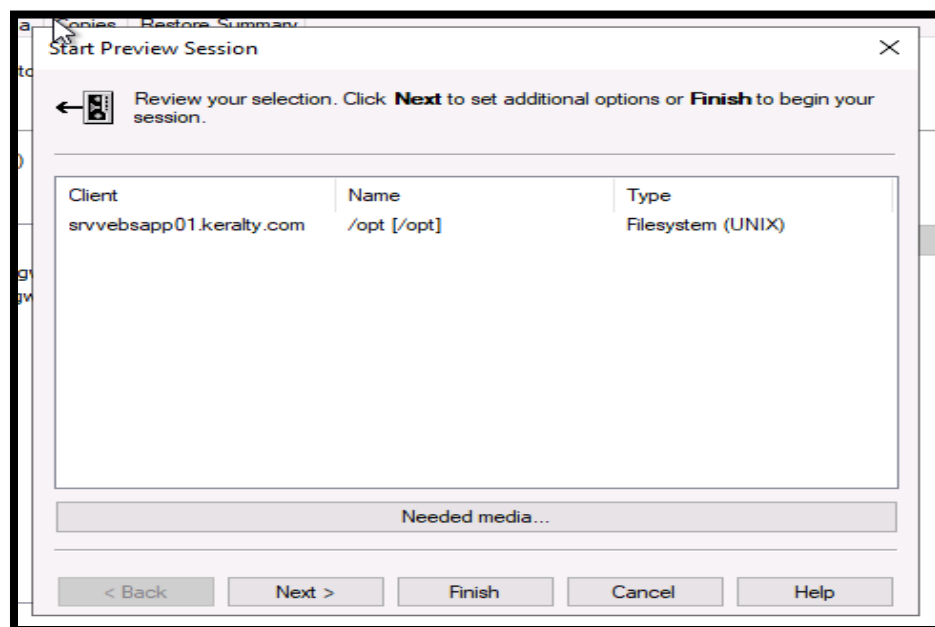


Imagen 42: Previo ejecución.

Se abre la ventana Iniciar sesión de restauración, que muestra el progreso de la restauración de los objetos seleccionados.

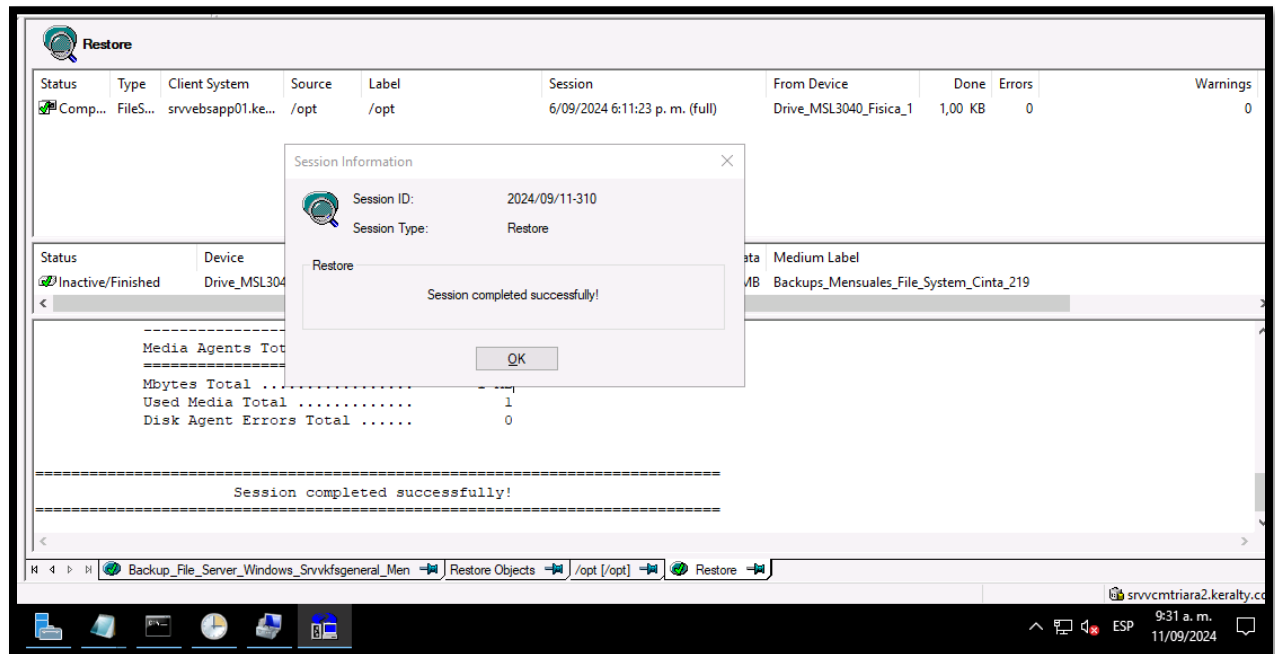
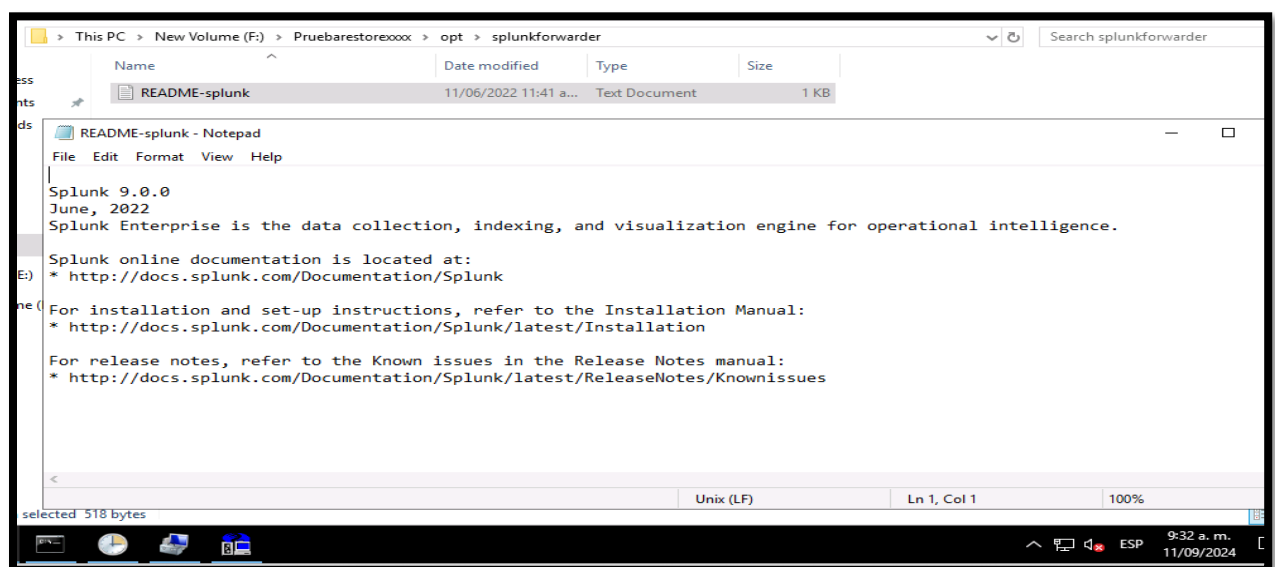


Imagen 43: finalización restore.

Evidencia de la restauración.



Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

Imagen 44: Validación restore.

Proceso de restauración de una base de datos SQL.

Data Protector ofrece distintos tipos de restauración según sus necesidades. Puede seleccionar la restauración en un momento determinado, la restauración completa de la base de datos, así como la restauración de los datos de SQL Server en una nueva ubicación, en un SQL Server diferente o en una instancia de SQL Server diferente.

Puede restaurar bases de datos de SQL Server mediante la GUI o CLI de Data Protector.

Para recuperar la base de datos maestra, inicie el proceso de recuperación ante desastres de SQL Server.

Verificar que las bases de datos a restaurar no estén en uso.

En una configuración de grupo de disponibilidad, es obligatorio restaurar a un cliente y una instancia diferentes. El usuario debe seleccionar las opciones de restauración con los valores adecuados para los campos "Restaurar a otro cliente" y "Restaurar a otra instancia". Asegúrese de no seleccionar un agente de escucha de grupo de disponibilidad para el cliente de destino (ya que no es compatible) y de que la instancia de SQL Server seleccionada exista en el cliente de destino. Asegúrese también de que la base de datos que seleccionó para la restauración no pertenezca a ningún grupo de disponibilidad.

La restauración a otra instancia no funciona si la base de datos original que se va a restaurar todavía existe en la instancia principal. Si la restauración a otra instancia debe realizarse correctamente, asegúrese de que la base de datos original ya se haya eliminado o deba eliminarse.

Proceda de la siguiente manera utilizando el Data Protector Manager:

En la Lista de contexto, haga clic en Restaurar.

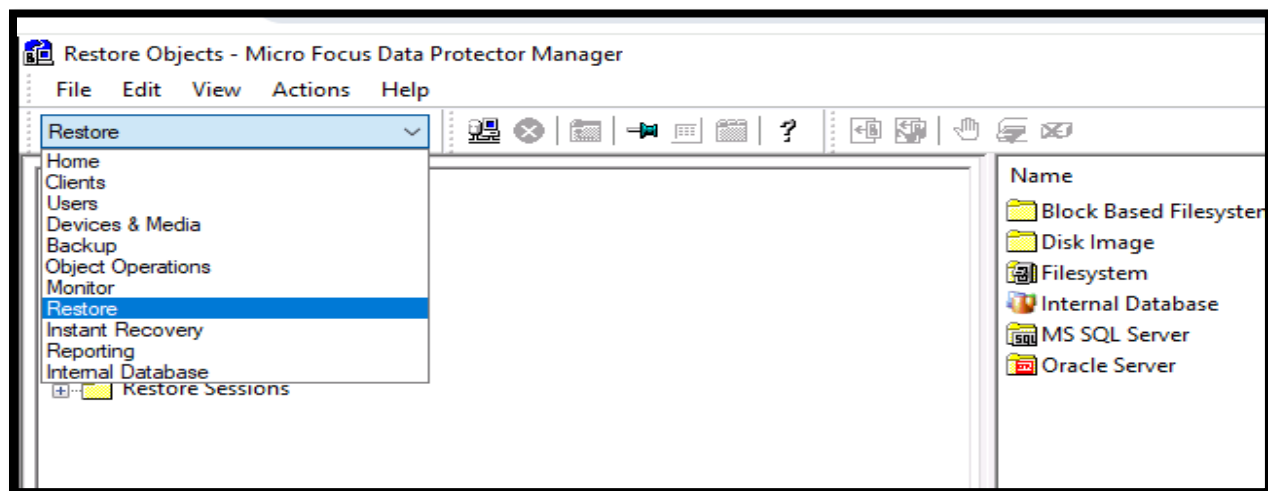


Imagen 45: Menú opción restore SQL Server

En el Panel de alcance, expanda Restaurar objetos, MS SQL Server y, a continuación, seleccione el servidor Microsoft SQL Server desde el que desea realizar la restauración. En el Área de resultados, se muestra una lista de los objetos respaldados.

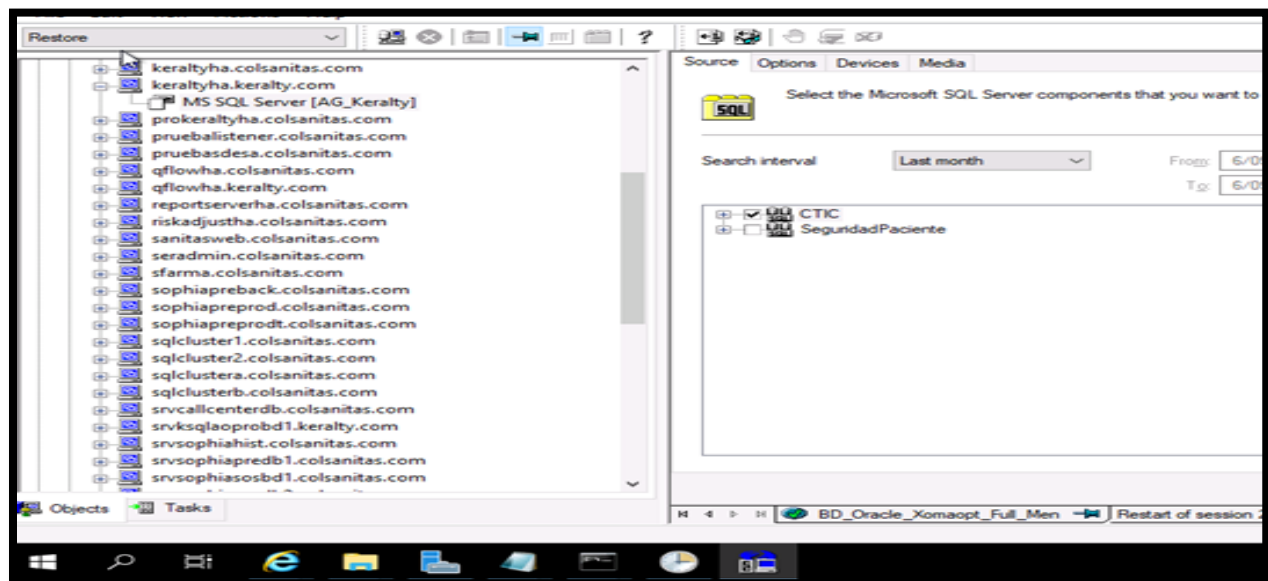


Imagen 46: Selección ruta restore SQL Server

Para seleccionar opciones específicas del objeto de respaldo, haga clic con el botón derecho en el objeto y seleccione

En la pestaña Versión, seleccione la versión de copia de seguridad (fecha de copia de seguridad) que desea utilizar para restaurar o seleccione la opción Restaurar al estado más reciente posible. Esta última opción siempre restaura la cadena de copias de seguridad como si estuviera

seleccionada la opción Restauración completa de la base de datos. Incluye las copias de seguridad completas, diferenciales y del registro de transacciones.

Opcionalmente, en la pestaña Avanzado, seleccione la opción Restaurar base de datos con nuevo nombre y especifique nuevas ubicaciones de restauración.

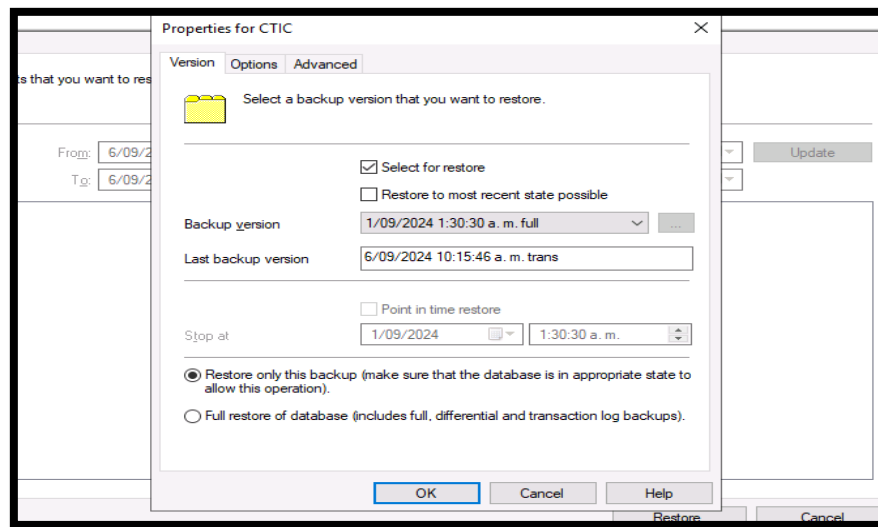


Imagen 47: Selección versión restore SQL Server.

Nota: No es necesario crear una base de datos vacía antes de restaurar, porque la base de datos y sus archivos son generados automáticamente por SQL Server.

Importante:

Antes de poder restaurar un archivo de datos, se debe realizar una copia de seguridad del registro de transacciones activas de la base de datos. En caso de que el registro se haya dañado, no se podrán restaurar archivos de datos específicos y solo se podrá restaurar la base de datos completa.

Seleccione otras opciones de restauración según corresponda. Tenga en cuenta que algunas opciones no están disponibles para restaurar archivos de datos.

En la página de propiedades Opciones, especifique nuevas ubicaciones para las bases de datos, si desea restaurar sus datos en un cliente o instancia diferente.

Importante: Al hacer clic en Opciones, se explora la celda en busca de instancias de SQL Server en ejecución que puedan convertirse en instancias de destino para la restauración. Si no se encuentran instancias, se deshabilita la opción Restaurar a otra instancia y se muestra el mensaje No hay instancias en este sistema cliente.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código:SIG-TI-CKE-MN03		

Asegúrese de que la instancia de SQL Server especificada exista en el cliente de destino. De lo contrario, la restauración fallará.

Seleccione una de las siguientes acciones de restauración:

Restaurar datos. Seleccione esta opción para restaurar toda la base de datos. Esta opción está seleccionada de manera predeterminada.

Restaurar y mostrar solo la lista de archivos. Seleccione esta opción si no conoce los nombres de los archivos originales. En este caso, se muestran los archivos respaldados en una sesión en particular.

Restaurar y mostrar solo encabezados. Seleccione esta opción si necesita detalles específicos sobre la copia de seguridad. Se muestra la información del encabezado de SQL Server.

Seleccione Habilitar copia de seguridad de registros de cola para realizar una sesión de copia de seguridad de registros de cola, justo antes de que comience la sesión de restauración, utilizando la especificación de copia de seguridad seleccionada en la lista desplegable. Esto captura los registros de la cola que aún no se han respaldado. Antes de seleccionar esta opción, asegúrese de lo siguiente:

La opción Poner la base de datos en modo de usuario único - cerrar la sesión de todos los usuarios está seleccionada para todas las bases de datos involucradas.

La opción Restaurar datos está seleccionada.

Para restaurar en un cliente de SQL Server diferente, seleccione Restaurar en otro cliente y el cliente de destino en la lista desplegable.

Para restaurar en una instancia de SQL Server diferente, seleccione Restaurar en otra instancia.

Si no hay instancias en la lista desplegable, ingrese el nombre de la instancia usted mismo.

Asegúrese de que la instancia de SQL Server especificada exista en el cliente de destino. De lo contrario, la restauración fallará.

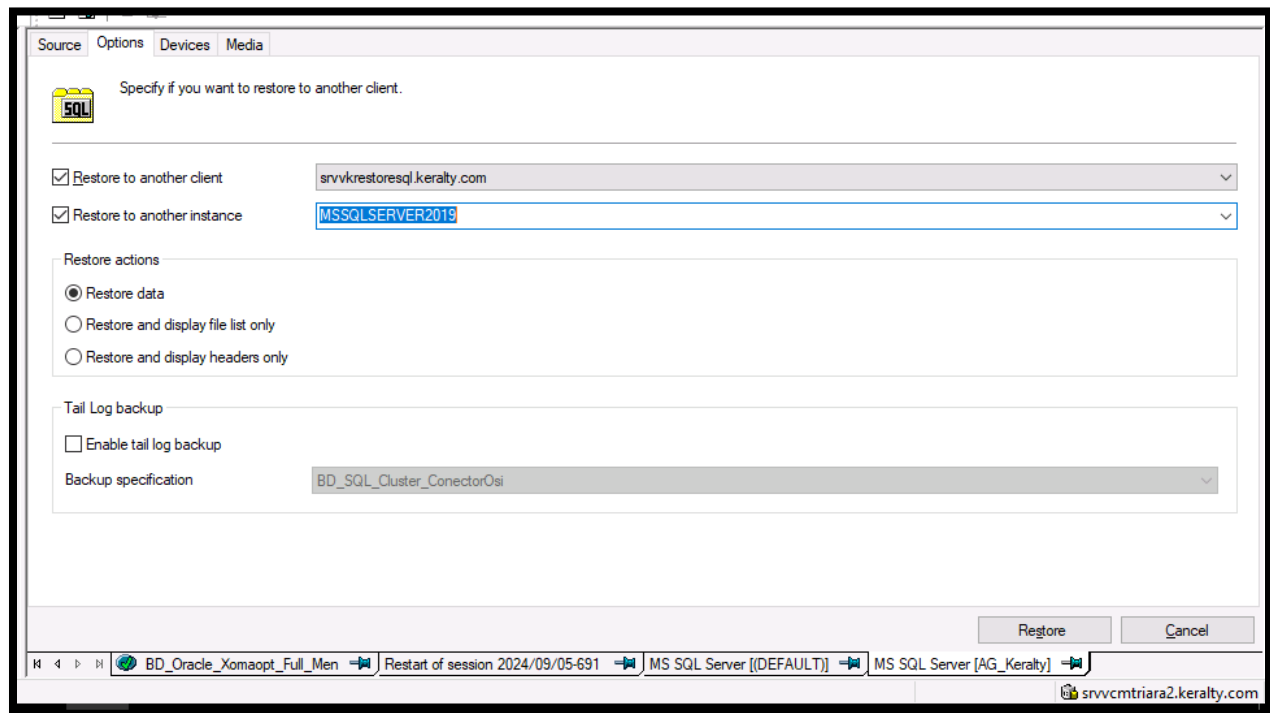


Imagen 48: Opción restore SQL Server.

En la página Dispositivos, seleccione los dispositivos que se utilizarán para la restauración.
 Si el respaldo esta en cinta puede validarla en la pestaña “Media”

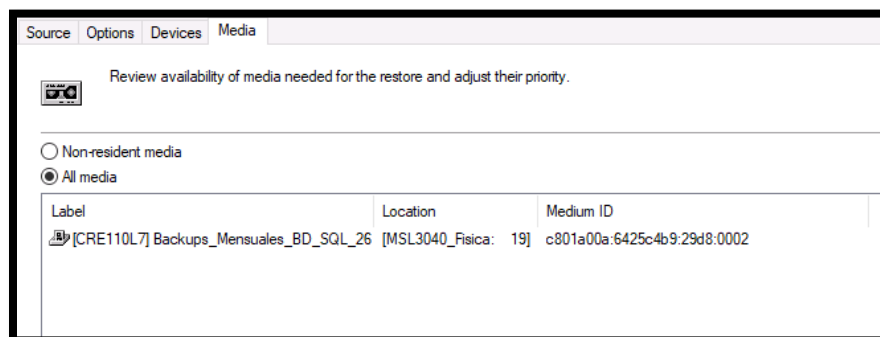


Imagen 49: Medios restore SQL Server.

Haga clic en Restaurar MS SQL Server y luego en Siguiente para seleccionar Nivel de informe
 Carga de red.
 Haga clic en Finalizar para iniciar la restauración.

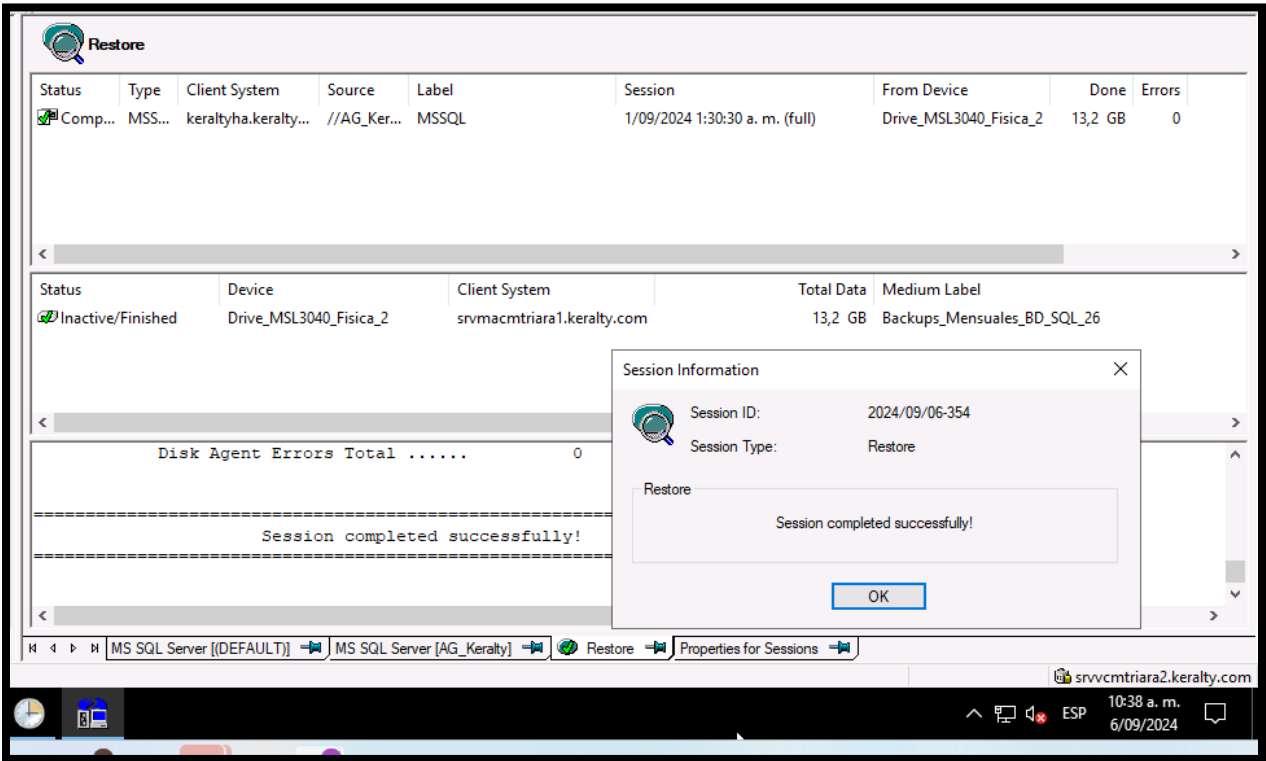


Imagen 50: finalización restore SQL Server.

Evidencia acceso Base de Datos.

Results		Messages						
	restore_date	destination_database_name	user_name	backup_set_id	restore_type	replace	recovery	restart
1	2024-09-06 10:30:41.300	CTIC_Prueba	CO11VG20BACKUP	1038	D	1	0	0
2	2024-06-14 09:58:00.103	CTIC_Prueba	CO11VG20BACKUP	1035	D	1	0	0
3	2024-04-12 16:28:24.690	CTIC_prueba	CO11VG20BACKUP	1033	D	1	0	0

Imagen 51: Evidencia restore SQL Server 1.

La base de datos abre correctamente.

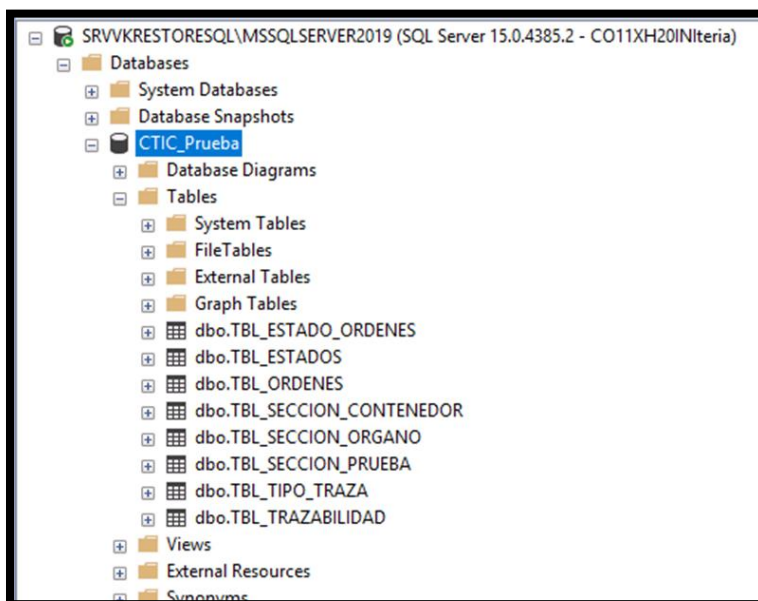


Imagen 52: Evidencia restore SQL Server 2.

Base de datos disponible

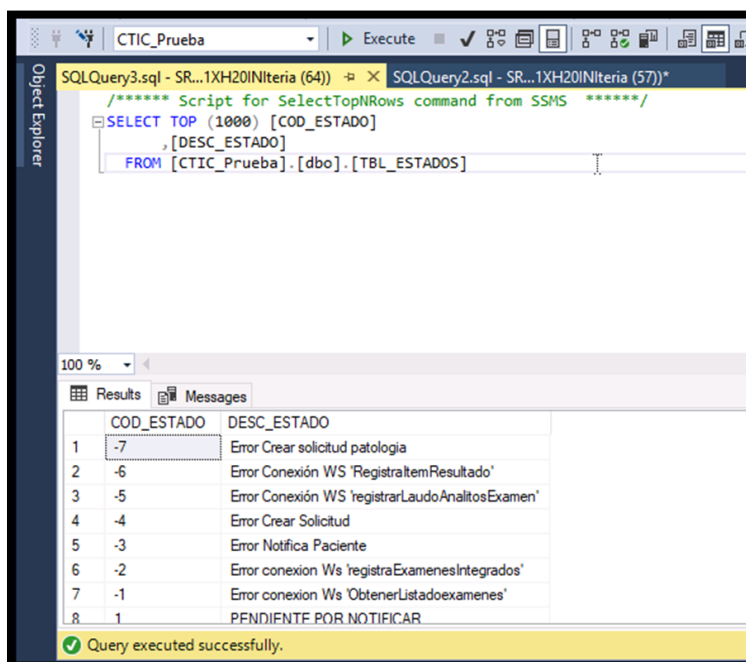


Imagen 53: Evidencia restore SQL Server 3.

Restaurar Oracle mediante RMAN.

Data Protector actúa como un software de administración de medios para el sistema Oracle, por lo que RMAN se puede utilizar para una restauración.

Desde la administración de la herramienta se procede con la entrega del log de la sesión de respaldo.

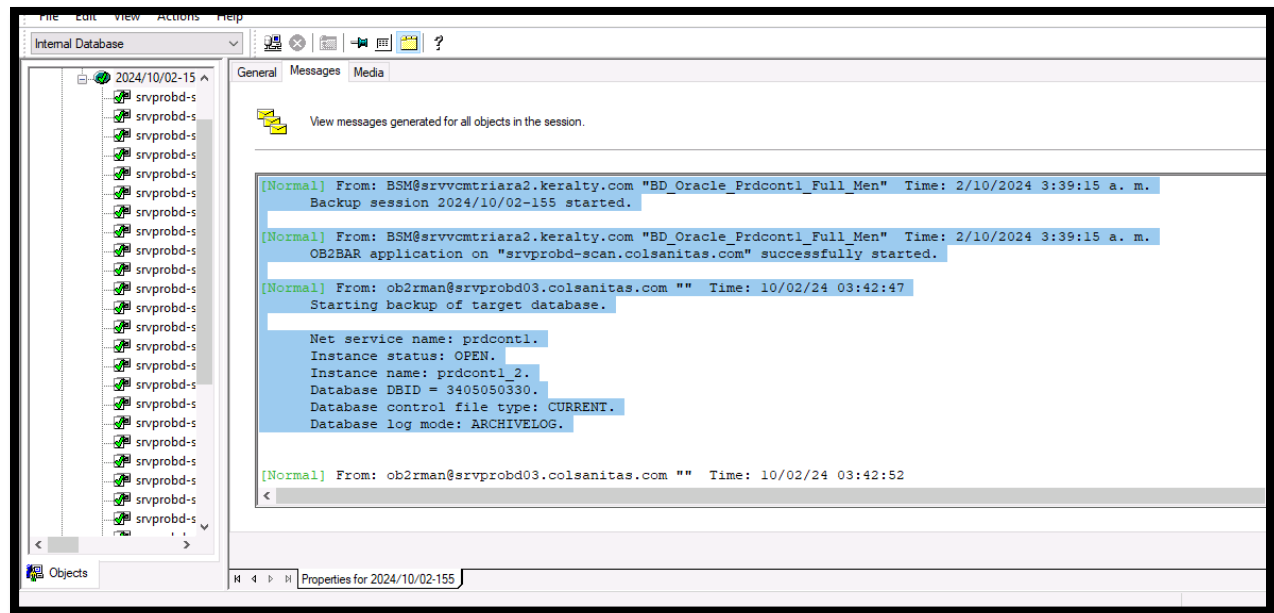


Imagen 54: log Backup base de datos Oracle.

El especialista de base de datos con la información del archivo procede a ejecutar la restauración desde la consola Oracle.

En la herramienta de dataprotector se evidencia el estado de la sesión.

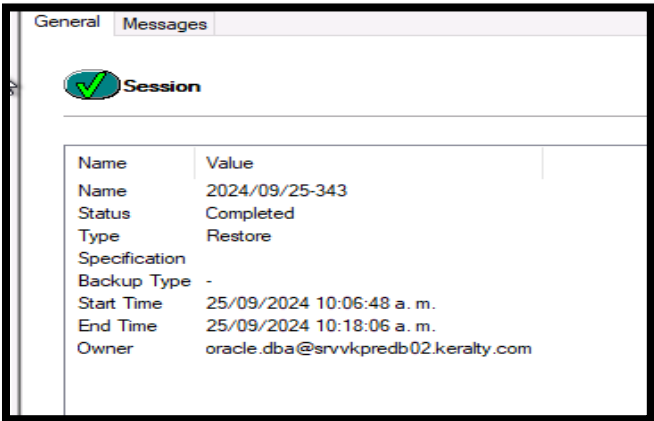


Imagen 55: Sesión restore Oracle.

De igual manera podemos ver el resultado del proceso ejecutado.



Imagen 56: log restore base de datos Oracle 1.

El medio dispositivo utilizado. De igual manera que en las sesiones anteriores puede ser de disco o de cinta.

```

Unloading medium to slot \\COFC-CZ3002Q801\PROD_ORA_ARC_FULL_DIA\c801a00a_66d55157_2200_f606 from device STORE_PROD_OI\A

[Normal] From: RMA@srvprobd04.colsanitas.com "STORE_PROD_ORA_ARC_FULL_DIA_gw6 [GW 17236:0:4119985568364368017]" Time: 25/09/2024 10:20:28 a. m.
COMPLETED Media Agent "STORE_PROD_ORA_ARC_FULL_DIA_gw6 [GW 17236:0:4119985568364368017]"

[Normal] From: RMA@srvprobd04.colsanitas.com "Drive_MSL3040_Fisica_3" Time: 25/09/2024 10:20:28 a. m.
Ejecting medium '6'.

[Normal] From: RMA@srvprobd04.colsanitas.com "Drive_MSL3040_Fisica_3" Time: 25/09/2024 10:20:28 a. m.
=> UMA@srvmacmtriara1.keralty.com@Changer1:0:0:7:1
Unloading medium to slot 6 from device /dev/nst4

[Normal] From: RMA@srvprobd04.colsanitas.com "Drive_MSL3040_Fisica_3" Time: 25/09/2024 10:20:56 a. m.
COMPLETED Media Agent "Drive_MSL3040_Fisica_3"

[Normal] From: RSM@srvvcmtriara2.keralty.com "" Time: 25/09/2024 10:18:06 a. m.

Restore Statistics:

```

Imagen 57: log restore base de datos Oracle 2.

El especialista de base de datos envía el log generado desde Oracle como evidencia de la restauración.

```

RMAN> run {
allocate auxiliary channel 'dev_0' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_1' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_2' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_3' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_4' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_5' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_6' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';
allocate auxiliary channel 'dev_7' type 'sbt_tape' parms 'SBT_LIBRARY=/opt/omni/lib/libob2oracle8_64bit.so';

send device type 'sbt_tape' 'OB2BARHOSTNAME=svrprobd-scan.colsanitas.com';
send channel 'dev_0' 'OB2BARTYPE=Oracle8';
send channel 'dev_0' '07> 8> 9> 10> 11> 12> 13> B2APPNAME=prdcont3';
send channel 'dev_0' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_1' 'OB2BARTYPE=Oracle8';
send channel 'dev_1' 'OB2APPNAME=prdcont3';
send channel 'dev_1' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_2' 'OB2BARTYPE=Oracle8';
send channel 'dev_2' 'OB2APPNAME=prdcont3';
send channel 'dev_2' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_3' 'OB2BARTYPE=Oracle8';
send channel 'dev_3' 'OB2APPNAME=prdcont3';
send channel 'dev_3' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_4' 'OB2BARTYPE=Oracle8';
send channel 'dev_4' 'OB2APPNAME=prdcont3';
send channel 'dev_4' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_5' 'OB2BARTYPE=Oracle8';
send channel 'dev_5' 'OB2APPNAME=prdcont3';
send channel 'dev_5' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_6' 'OB2BARTYPE=Oracle8';
send channel 'dev_6' 'OB2APPNAME=prdcont3';
send channel 'dev_6' 'OB2BARLIST=BD_Oracle_Prdcont3_Full_Men';
send channel 'dev_7' 'OB2BARTYPE=Oracle8';
send channel 'dev_7' 'OB2APPNAME=prdcont3';
}

```

Imagen 58: Evidencia acceso a la base de datos restore 1.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

En este punto se valida que los datos de la base de datos corresponde con la sesion y el log enviado para restaurar.

De esta manera se puede garantizar que la informacion es correcta y corresponde con lo entregado.

```

Keenabling controlfile options for auxiliary database
Executing: alter database force logging

contents of Memory Script:
{
  sql clone 'alter system set "_system_trig_enabled"=FALSE';
  Alter clone database open resetlogs;
  sql clone 'alter system reset "_system_trig_enabled"';
}
executing Memory Script

sql statement: alter system set "_system_trig_enabled"=FALSE

database opened

PL/SQL package SYS.DBMS_BACKUP_RESTORE version 19.23.00.00 in AUXILIARY database is not current
PL/SQL package SYS.DBMS_RCVMAN version 19.23.00.00 in AUXILIARY database is not current
sql statement: alter system reset "_system_trig_enabled"
Executing: drop pluggable database "CAPMB" including datafiles
Executing: drop pluggable database "BDCAPA" including datafiles

contents of Memory Script:
{
  sql clone "alter pluggable database all open";
}
executing Memory Script

sql statement: alter pluggable database all open
Dropping offline and skipped tablespaces
Executing: alter database default tablespace system
Executing: drop tablespace "USERS" including contents cascade constraints
Finished Duplicate Db at 25-SEP-24

RMAN>

```

Imagen 59: Evidencia acceso a la base de datos restore 2.

NOTA: actualmente no se cuenta con un sitio alternativo de recuperación, este se encuentra en proceso de ser adquirido y el trámite se encuentra en copras.

En caso de algún incidente una vez aprobado por la Gerencia, se puede recuperas los respaldos en el mismo sitio de origen, siempre y cuando este no presente una afectación física o alguna otra novedad propia del incidente.

¡Error! Marcador no definido.

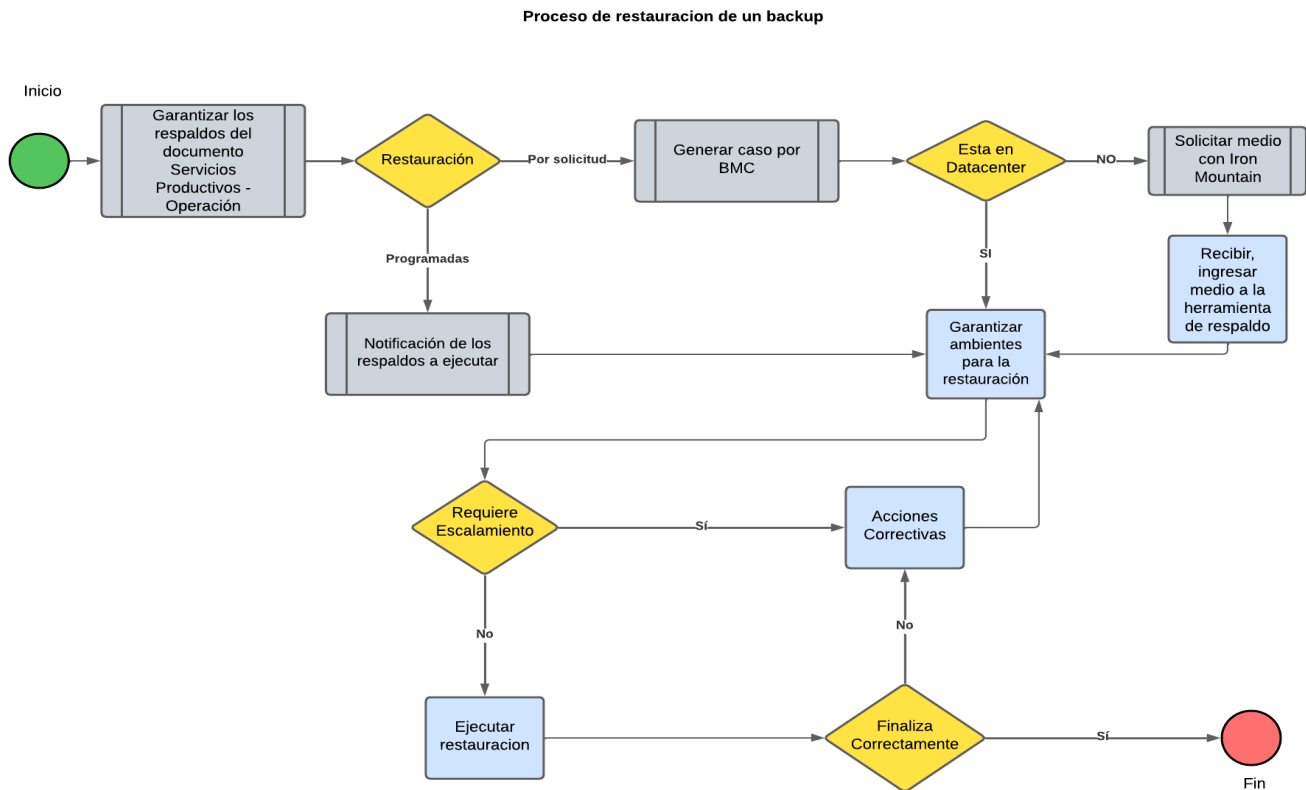


Imagen 60: Flujo de proceso de restauración

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

5. SOPORTE Y LICENCIAMIENTO

Data Protector

Fabricante: Opentext

Licencia: Tradicional permanente, soporte renovación anual.

Disponibilidad: soporte 24/7

Línea de Atención: teléfono: +57 1 601 9158115

Portal: https://portal.microfocus.com/s/?language=en_US

Tiempos de Respuesta

- **Soporte Crítico (Severity 1):**
 - **Descripción:** Sistema inoperativo o crítico.
 - **Tiempo de Respuesta:** 1 hora.
- **Soporte Alto (Severity 2):**
 - **Descripción:** Problema severo que afecta la funcionalidad, pero no impide el uso.
 - **Tiempo de Respuesta:** 4 horas.
- **Soporte Moderado (Severity 3):**
 - **Descripción:** Problema que no afecta gravemente el funcionamiento.
 - **Tiempo de Respuesta:** 1 día hábil.
- **Soporte Bajo (Severity 4):**
 - **Descripción:** Preguntas generales o problemas menores.
 - **Tiempo de Respuesta:** 2 días hábiles.

Veeam

Fabricante: Veeam Software

Licencia: Premium Enterprise plus, renovación licencia anual.

Disponibilidad: Soporte 24/7

Línea de Atención: Teléfono: +57 1 601 3810636

Portal: <https://www.veeam.com/es/support.html>

Tiempos de Respuesta

- **Soporte Crítico (Gravedad 1):**
 - **Descripción:** Falta de disponibilidad de un componente software crítico,
 - **Tiempo de Respuesta:** 1 hora.
- **Soporte Alto (Gravedad 2):**
 - **Descripción:** El problema afecta a las operaciones de producción
 - **Tiempo de Respuesta:** 3 horas.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

- **Soporte Moderado (Gravedad 3):**
 - **Descripción:** El problema tiene un impacto leve, la mayoría de funciones siguen siendo utilizables.
 - **Tiempo de Respuesta:** 6 horas.
- **Soporte Bajo (Gravedad 4):**
 - **Descripción:** El problema produce un impacto mínimo o es una consulta.
 - **Tiempo de Respuesta:** 8 horas.

6. ROLES Y RESPONSABILIDADES.

Administrador de sistemas Keralty: Nayil Alberto Salinas Alvis

Responsabilidad: Liderar la gestión de las plataformas de respaldo de Keralty.

Operadores Terasys

Responsabilidades: Monitoreo de los respaldos, escalamiento de novedades y diligenciamiento de la trazabilidad de los respaldos

Administrador de backups Terasys: Juan Sebastian Carrero Rodriguez

Responsabilidades: Garantiza la ejecución de los respaldos, la documentación de los procesos, edición resolución de novedades, escalamiento con fabricante. Pruebas de restauración.

Administrador de sistemas Keralty Elizabeth Mosquera

Responsabilidades: Pruebas de funcionamiento de las restauraciones, entrega de evidencia.

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código:SIG-TI-CKE-MN03		

7. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
04/10/2024	Creación del documento	1.0

Tabla 1 Tabla de control de versiones

Versión: 1.0	MANUAL RECUPERACIÓN POR BACKUPS	
Fecha: 23-12-2024		
Código: SIG-TI-CKE-MN03		

8. FLUJO DE APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: Nayil Alberto Salinas Alvis Nombre: Sebastián Carrero Fecha: 04/10/2024	Nombre: Luisa Castaño Área/Proceso: Dirección de Operaciones de TI y comunicaciones Fecha: 23/12/2024	Nombre: Luisa Castaño Área/Proceso: Dirección de Operaciones de TI y comunicaciones Fecha: 23/12/2024

Tabla 2 Tabla de aprobación de documento

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.