Copia de seguridad y restauración de Active Directory con Acronis Backup & Recovery 11

Documentación técnica

Se aplica a las siguientes ediciones:

- ☑ Advanced Server
- ☑ Virtual Edition
- ☑ Advanced Server SBS Edition
- ☐ Advanced Workstation
- ☐ Server for Linux
- ☑ Server for Windows
- ☐ Workstation

Contenido

1 Introducción

Microsoft Active Directory es un componente central de la plataforma Windows y puede encontrarse en un entorno de Windows de cualquier tamaño. Active Directory contiene la información fundamental para que las empresas puedan funcionar.

Esta documentación técnica proporciona información que permite a los administradores de sistemas implementar sus propias soluciones de recuperación para Active Directory utilizando el software Acronis Backup & Recovery 11.

2 Información general de copia de seguridad y recuperación

Los servicios de Microsoft Active Directory (AD) utilizan una base de datos ubicada en el sistema de archivos de un controlador de dominio. Si hay más de un controlador de dominio disponible, la información almacenada en la base de datos se replica constantemente entre los múltiples controladores de dominio.

Un componente de Windows llamado servicio de instantáneas de volumen (VSS) se utiliza para crear una copia consistente de la base de datos de AD.

Las situaciones de recuperación de Active Directory pueden incluir la recuperación de un controlador de dominio bloqueado, la recuperación de una base de datos de AD corrupta y la recuperación de objetos de AD eliminados o modificados accidentalmente. Las operaciones y herramientas necesarias también pueden variar según el tipo de información que deba restaurarse y la disponibilidad de otros controladores de dominio.

3 Copia de seguridad de Active Directory

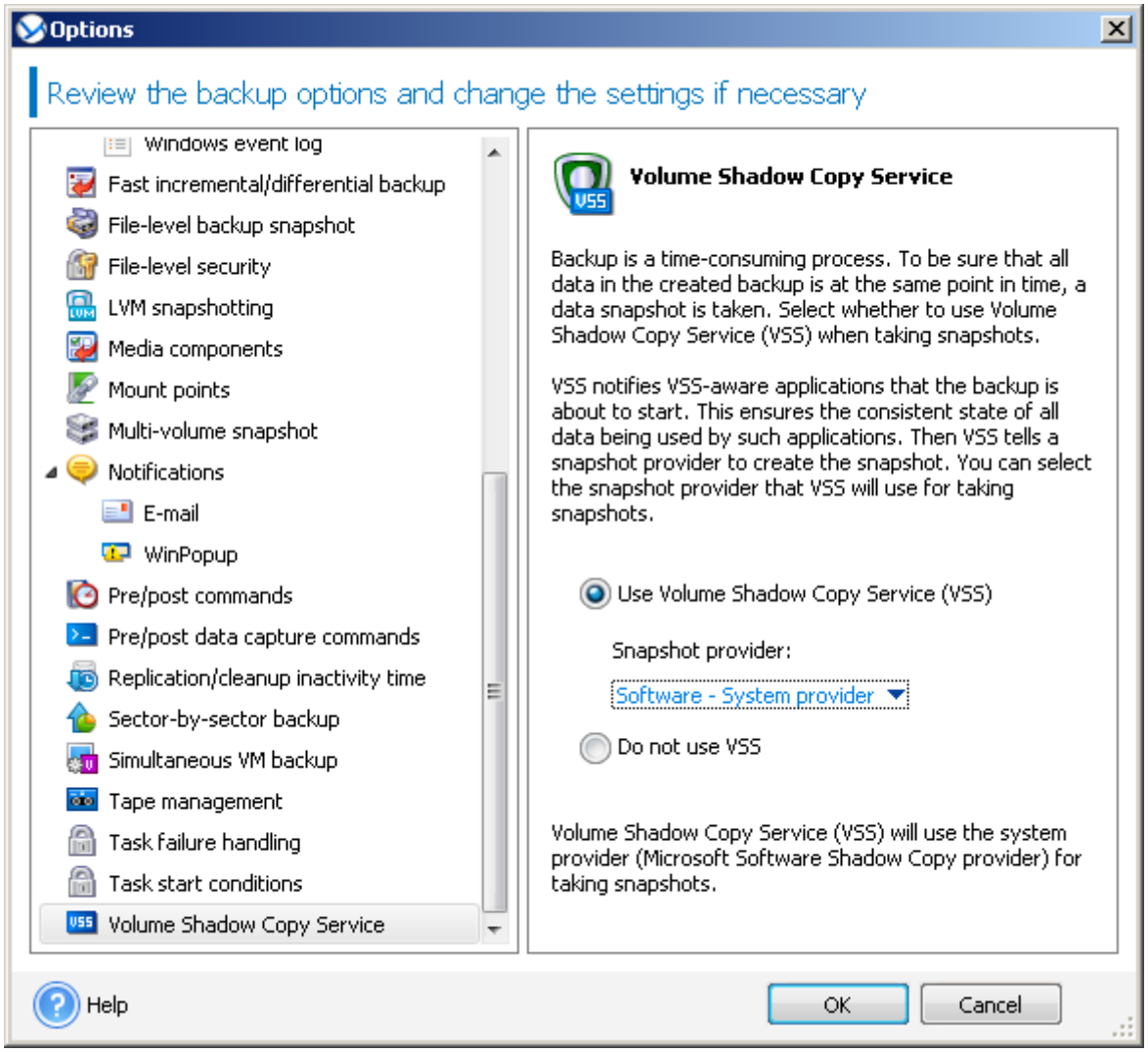
En Windows (incluyendo Windows 2003 y Windows 2008), la base de datos de Active Directory generalmente se ubica en la carpeta **%systemroot%\NTDS** (como C:\Windows\NTDS) de un controlador de dominio. A pesar de que esta ubicación se utiliza de manera predeterminada, es configurable. La utilidad de la línea de comandos **Ntdsutil** puede ayudarle a encontrar la ubicación actual. Tenga en cuenta que la base de datos y los registros de transacciones pueden almacenarse en diferentes volúmenes; por lo tanto, tenga en cuenta que ambos se incluyen en la copia de seguridad.

Le recomendamos que realice la copia de seguridad del volumen del sistema del controlador de dominio, del volumen de arranque y de los volúmenes donde está ubicada la base de datos y los registros de transacciones de AD. La copia de seguridad resultante incluirá toda la información necesaria para recuperar el controlador de dominio completamente y restaurar Active Directory.

Debido a que el servicio de Active Directory casi siempre se está ejecutando, deberá utilizarse el servicio de instantáneas de volumen (VSS) para garantizar la consistencia de los archivos en la copia de seguridad. Sin VSS, los archivos se encontrarían en un estado llamado "coherente con el bloqueo", es decir, después de la restauración, el sistema estaría en el mismo estado que si se hubiera desconectado la alimentación en el momento en el que comenzaba la copia de seguridad.

A pesar de que dichas copias de seguridad son lo suficientemente adecuadas para las aplicaciones, es posible que las bases de datos (incluyendo la base de datos de Active Directory) no puedan iniciarse desde un estado coherente con el bloqueo y es posible que necesiten una recuperación manual.

Para evitarlo, asegúrese de que la opción **Utilizar el servicio de instantáneas de volumen (VSS)** esté seleccionada en las opciones de copia de seguridad al crear una copia de seguridad de un controlador de dominio. En **Proveedor de la instantánea**, seleccione **Software - Proveedor del sistema**. Acronis Backup & Recovery 11 utilizará el proveedor de instantáneas de software de Microsoft. Esto garantiza que la base de datos de Active Directory se incluya en la copia de seguridad en un estado coherente



La siguiente pregunta es con qué frecuencia necesita realizar la copia de seguridad del controlador de dominio. Microsoft recomienda realizar al menos dos copias de seguridad durante la vida útil del marcador de exclusión, que es, según la versión del sistema operativo en donde se ha creado su dominio, 60 o 180 días. Profundizaremos sobre la duración del marcador de exclusión y su impacto sobre la capacidad de la posterior restauración en este documento. Sin embargo, como mínimo, realice la copia de seguridad al menos una vez al mes.

Para resumir, es necesario hacer lo siguiente para realizar una copia de seguridad completa de la base de datos de Active Directory:

- Asegúrese de que al menos uno de sus controladores de dominio se incluya en la copia de seguridad.
- Asegúrese de que la copia de seguridad más actualizada del controlador de dominio no sea más antigua que la duración del marcador de exclusión. En la mayoría de los casos, la duración del marcador de exclusión es de 60 días, así que la copia de seguridad no puede ser anterior a 30

días. No importa que la última copia de seguridad sea completa o incremental, puede realizar una restauración correcta desde cualquiera de las dos.

- Cree una copia de seguridad inmediatamente al producirse cualquiera de los siguientes eventos, ya que es posible que sea imposible una restauración correcta desde Active Directory desde las copias de seguridad existentes:
  - La base de datos de Active Directory o el registro se movió a una ubicación diferente.
  - Se actualizó un sistema operativo en un controlador de dominio o se instaló un service pack.
  - Se instaló un hotfix que cambia la base de datos de AD.
  - La duración del marcador de exclusión se cambió de forma administrativa.
- Asegúrese de que los archivos que conforman la base de datos de AD (archivos .dit, .chk, .log) no se encuentren en la lista de exclusión.
- Asegúrese de que la opción **Utilizar el servicio de instantáneas de volumen (VSS)** se haya seleccionado para la copia de seguridad.

4 Recuperación de Active Directory

Como se mencionó anteriormente, la recuperación de AD puede ser diferente según el tipo de recuperación necesario. Además, en algunos casos, ni siquiera necesita tocar la copia de seguridad del controlador de dominio, toda la información necesaria para la recuperación ya está disponible.

Para cubrir las situaciones más importantes en cuanto a la recuperación de AD, consideremos las siguientes situaciones de desastres:

- Un controlador de dominio se pierde, pero otros controladores de dominio están todavía disponibles. Consulte “Restauración del controlador de dominio (otros controladores de dominio están disponibles)” (pág. 8).
- Se pierden todos los controladores de dominio (o solo existe uno). Consulte “Restauración del controlador de dominio (sin otros controladores de dominio disponibles)” (pág. 9).
- La base de datos de Active Directory está dañada y el servicio de AD no arranca. Consulte "Restauración de la base de datos de Active Directory (pág. 10)".
- Cierta información se eliminó accidentalmente de Active Directory. Consulte “Restauración de información eliminada accidentalmente” (pág. 11).

4.1 Restauración del controlador de dominio (otros controladores de dominio están disponibles)

Cuando se pierde uno de los controladores de dominio, el servicio de AD todavía está disponible. Por lo tanto, los demás controladores de dominio contienen datos que están más actualizados que los datos de la copia de seguridad. Por ejemplo, si se creó una cuenta de usuario en AD después de realizar la copia de seguridad, la copia de seguridad no incluirá esta cuenta.

Por lo tanto, queremos realizar una recuperación que no afecte el estado actual de Active Directory; esta operación se llama restauración no autoritativa.

Acerca de la replicación de los datos de Active Directory

Los datos de Active Directory se están replicando constantemente entre los controladores de dominio. En cualquier momento dado, el mismo objeto de Active Directory puede tener una versión más actual en un controlador de dominio y una versión anterior en otro. Para evitar los conflictos y la pérdida de información, Active Directory realiza un seguimiento de las versiones de los objetos en cada controlador de dominio y reemplaza las versiones desactualizadas con la versión más actual.

Por lo tanto, los objetos de AD desde la copia de seguridad tienen poco valor; los objetos más actualizados de los demás controladores de dominio los sobrescribirán durante la replicación.

Pasos a seguir

Cuando otros controladores de dominio están disponibles, puede llevar a cabo una restauración no autoritativa de un controlador de dominio perdido de cualquiera de las siguientes formas:

- *Recuperar un controlador de dominio* desde una copia de seguridad.
- *Recrear un controlador de dominio* al instalar el sistema operativo y hacer que el equipo sea un nuevo controlador de dominio (con la herramienta **dcpromo.exe**).

Después de ambas operaciones se realiza una replicación. La replicación hace que la base de datos del controlador de dominio esté actualizada. Solo asegúrese de que el servicio de Active Directory se

haya iniciado correctamente. Una vez que finaliza la replicación, el controlador de dominio estará listo y funcionando nuevamente.

Recuperación vs. recreación

La recreación no necesita tener una copia de seguridad. La recuperación es normalmente más rápida que la recreación, pero no es posible en los siguientes casos:

- Todas las copias de seguridad disponibles son anteriores a la duración del marcador de exclusión. Los marcadores de exclusión se utilizan durante la replicación para garantizar que un objeto en un controlador de dominio se elimine en los demás controladores de dominio. Por lo tanto, una correcta replicación no es posible después de haber eliminado los marcadores de exclusión.
- El controlador de dominio posee un rol Flexible Single Master Operations (FSMO) y ha asignado ese rol a un controlador de dominio diferente (tomó el rol). En este caso, la restauración del controlador de dominio hará que los dos controladores de dominio posean el mismo rol FSMO en el dominio y generará un conflicto.

Recreación de un controlador de dominio que posee un rol FSMO

Algunos controladores de dominio poseen roles únicos conocidos como roles Flexible Single Master Operations (FSMO) o roles de administrador de operaciones. Un controlador de dominio puede tener múltiples roles FSMO. Sin embargo, dos controladores de dominio en el mismo dominio no pueden tener el mismo rol FSMO. Algunos roles FSMO deben encontrarse en un único controlador de dominio con toda la colección de dominios conocida como "bosque". Para obtener la descripción de los roles FSMO y sus alcances (a nivel del dominio o a nivel del bosque), consulte la ayuda de Microsoft y el artículo de asistencia técnica http://support.microsoft.com/kb/324801.

Antes de recrear un controlador de dominio que posee el rol PDC Emulator, primero debe tomar ese rol. De lo contrario, no podrá añadir el controlador de dominio recreado al dominio. Después de recrear el controlador de dominio, puede volver a transferir el rol. Para obtener información sobre cómo tomar y transferir los roles FSMO, consulte la ayuda de Microsoft y el artículo de asistencia técnica http://support.microsoft.com/kb/255504.

Para ver qué roles FSMO están asignados a qué controlador de dominio, puede conectarse a cualquier controlador de dominio conectado con la herramienta **ntdsutil.exe** según se describe en la ayuda de Microsoft y el artículo de asistencia técnica http://support.microsoft.com/kb/234790. Siga los pasos en la sección “Utilización de la herramienta NTDSUTIL” de ese artículo:

- Para los sistemas operativos 2000 Server y Windows Server 2003, siga todos los pasos que se proporcionan.
- Para el sistema operativo Windows Server 2008, en el paso que le pide que escriba **domain management**, escriba **roles**. Siga los demás pasos que se proporcionan.

4.2 Restauración del controlador de dominio (sin otros controladores de dominio disponibles)

Si se pierden todos los controladores de dominio (o había un solo controlador de dominio en el dominio y este controlador se bloqueó), el servicio de AD se cae. Por lo tanto, la restauración no autoritativa de hecho se convierte en autoritativa: los objetos restaurados de la copia de seguridad son los más actuales disponibles. La replicación de los datos de AD no puede realizarse si no existen controladores de dominio conectados. Esto significa que:

- Los cambios en AD que se produjeron después de la realización de la copia de seguridad se perderán.

- La recreación del controlador de dominio no es una opción.
- Se puede utilizar incluso una copia de seguridad con fecha del marcador de exclusión expirada.

Para resumir, deberán realizarse los siguientes pasos al restaurar el último o el único controlador de dominio:

1. Asegúrese de utilizar la copia de seguridad más actual disponible para la recuperación. Esto es especialmente importante porque toda la información creada desde la última copia de seguridad se perderá. Si su dominio posee un solo controlador de dominio, es aconsejable crear un controlador de dominio al menos una vez al día.
2. Recupere el controlador de dominio desde la copia de seguridad.
3. Reinicie el equipo. Asegúrese de que el servicio de Active Directory se haya iniciado correctamente.

4.3 Restauración de la base de datos de Active Directory

Si la base de datos de AD se daña a nivel de los archivos en vez de a nivel del esquema/lógica de AD, existen varias soluciones que no involucran la restauración de los datos desde la copia de seguridad.

Si están disponibles otros controladores de dominio, el controlador de dominio puede relegarse y después promoverse nuevamente con la herramienta **dcpromo.exe**. Durante este procedimiento, los datos se replicarán y la base de datos de AD se recuperará. La complejidad de todo el procedimiento depende de si el controlador de dominio todavía puede arrancar en modo normal. Si así fuera, puede usar simplemente el comando **dcpromo /forceremoval** para quitar el servicio de AD del equipo. Si no fuera así, se necesita un procedimiento más complejo. Puede encontrar las instrucciones detalladas en la ayuda de Microsoft y los artículos de asistencia técnica http://support.microsoft.com/kb/332199/ y http://support.microsoft.com/kb/258062.

Si no hay otros controladores de dominio disponibles, los datos deben restaurarse desde una copia de seguridad. Una forma de hacerlo es restaurar el controlador de dominio completamente. El procedimiento es similar a la situación descrita en “Restauración del controlador de dominio (sin otros controladores de dominio disponibles)” (pág. 9). Este método garantiza la recuperación completa y es razonable utilizarlo si el controlador de dominio no tiene otros datos valiosos, excepto Active Directory mismo, o si los demás datos valiosos son fáciles de guardar (p. ej. ubicados en otro volumen que no necesita restaurarse).

Otra forma es recuperar la base de datos de AD sola.

La base de datos de AD consta de los siguientes archivos:

1. **NTDS.dit** (archivo de base de datos)
2. **Edb.chk** (archivo de punto de comprobación)
3. **Edb*.log** (registros de transacciones)
4. **Res1.log** t **Res2.log** (registro de transacciones de reserva)

De manera predeterminada, estos archivos se ubican en la carpeta **%systemroot%\NTDS**. Sin embargo, la ubicación es configurable, así que asegúrese de comprobarlo. Además, si se han realizado cambios a los objetos de políticas de grupo, el volumen del sistema SYSVOL (**%systemroot%\SYSVOL**) también debe restaurarse.

Todo el proceso es el siguiente:

1. Si no hay otros controladores de dominio disponibles, asegúrese de restaurar con la copia de seguridad más actual disponible. Esto es especialmente importante porque toda la información creada después de la copia de seguridad se perderá.
2. Reinicie el controlador de dominio en el modo de restauración de los servicios del directorio.
3. Cree una copia de sus archivos de base de datos de AD.
4. Restaure los archivos desde la copia de seguridad (utilice la restauración de archivos desde una copia de seguridad de nivel del disco para lograrlo).
5. Reinicie el equipo. Asegúrese de que el servicio de Active Directory se haya iniciado correctamente.

4.4 Restauración de información eliminada accidentalmente

Un ejemplo de información eliminada accidentalmente incluye una cuenta de usuario o equipo eliminada de forma involuntaria.

Existen dos maneras de revertir dicha modificación.

Restauración de toda la base de datos

El método más obvio es restaurar la base de datos de AD desde la copia de seguridad. Como en la situación anterior, reinicie el controlador de dominio en el modo Directory Services Restore y restaure la base de datos de AD.

Si posee solo un controlador de dominio (y por lo tanto la restauración se convierte en autoritativa), esté preparado para perder cualquier cambio realizado después de la última copia de seguridad al utilizar este método.

La disponibilidad de los demás controladores de dominio le permite realizar una restauración autoritativa de solo ciertos objetos. Los demás objetos se replicarán desde otros controladores al reiniciar el controlador en el modo normal. De esta manera, restaurará involuntariamente los objetos eliminados y mantendrá los demás objetos actualizados. Una vez que haya restaurado la base de datos de AD de la copia de seguridad, asegúrese de llevar a cabo los siguientes pasos:

1. Sin reiniciar el equipo, ejecute **ntdsutil** y escriba **authoritative restore** en su entrada de comandos.
2. Escriba el correspondiente comando de **restauración**, como **restore subtree** o **restore object**, para realizar la restauración autoritativa del objeto necesario (consulte la documentación de **ntdsutil** para obtener más información). Para restaurar toda la base de datos, utilice **restore database**.
3. Reinicie el equipo. Asegúrese de que el servicio de Active Directory se haya iniciado correctamente y que el objeto restaurado esté disponible.

Utilización de marcadores de exclusión

Otra forma de restaurar un objeto eliminado accidentalmente es utilizar marcadores de exclusión. En AD, cualquier objeto eliminado se conserva durante un periodo (llamado duración del marcador de exclusión, como se explicó anteriormente). Este periodo es, de manera predeterminada, de al menos 60 días. Esto significa que cualquier objeto, aunque se elimine de AD, permanecerá en su base de datos al menos 60 días antes de borrarse definitivamente.

Con este método, las copias de seguridad no se utilizan y AD permanece disponible durante la recuperación; no hay necesidad de reiniciar el controlador de dominio. Existen varias herramientas que llevan a cabo dicha recuperación; muchas de ellas están disponibles de forma gratuita. Por ejemplo, una herramienta de línea de comando de Windows Sysinternals llamada **adrestore** puede buscar y restaurar los objetos eliminados Otro ejemplo es una herramienta gratis de MVP Guy Teverovsky llamada **ADRestore.NET**. Esta herramienta es una interfaz gráfica de usuario y puede ser más fácil de utilizar. Para obtener más información, consulte la documentación proporcionada con las herramientas adecuadas.

5 Resumen

Acronis Backup & Recovery 11 es una potente solución de copia de seguridad y recuperación que puede proteger de forma eficaz a cualquier servidor con Windows, incluyendo los servidores/controladores de dominio de Active Directory. La tecnología de copia de seguridad a nivel del disco implementada en el producto permite la recuperación eficaz de muchas bases de datos, incluyendo Microsoft Active Directory.