semperis

¿Su plan de recuperación tras desastres de Active Directory cubre ataques cibernéticos?

POR GUIDO GRILLENMEIER Y GIL KIRKPATRICK

RECUPERACIÓN DE ACTIVE DIRECTORY DE LAS AMENAZAS ACTUALES

Hace dieciséis años, Gil Kirkpatrick (arquitecto jefe de Semperis) y Guido Grillenmeier (tecnólogo jefe de Semperis), cuando cada uno trabajaba en empresas distintas, se reunieron para compartir su experiencia y conocimientos sobre la protección y recuperación de Active Directory (AD). El resultado de esta colaboración fue la publicación en 2005 del libro blanco «Una guía definitiva para la recuperación tras desastres de Active Directory». El documento técnico atendió una necesidad crítica en la industria, ya que la mayoría de las empresas habían aceptado de facto AD como el servicio de directorio estándar para controlar el acceso a su red corporativa y a las aplicaciones y servicios para sus usuarios.

En ese entonces, la información sobre recuperación total o parcial de un AD era escasa y no muchos profesionales de AD comprendían la realidad del desafío. El documento técnico explicaba la mecánica de la recuperación de AD y aclaraba cuán necesario era que las empresas se prepararan para recuperarse adecuadamente de diferentes problemas de AD. Describía cómo recuperarse tras diferentes tipos de desastres, como la eliminación inadvertida de objetos de AD, la configuración incorrecta de las directivas de grupo y los controladores de dominio de AD fallidos. El documento finalizaba con una breve descripción del proceso para recuperar un entorno de AD después de un colapso total, con la siguiente salvedad: «Sin embargo, la probabilidad de [necesitar] una recuperación total del bosque AD es muy reducida».

Eso era antes. El panorama de la ciberseguridad ha cambiado drásticamente. No pasa una semana sin que la red de Windows on-premise de alguna organización sea arrasada por un ataque de ransomware o de un software malicioso. Por ejemplo, para 2019 y principios de 2020 tenemos (con costos de recuperación estimados):

- Ciudad de Nueva Orleans (más de $3 millones)
- Ciudad de Baltimore ($18 millones)
- Norsk Hydro ($70 millones)
- Demant ($80 millones)

Y existen decenas de casos más. El punto es que la capacidad para recuperar el entorno de AD por completo a partir de una copia de seguridad ya no representa una buena opción para un evento poco probable. Es una necesidad.

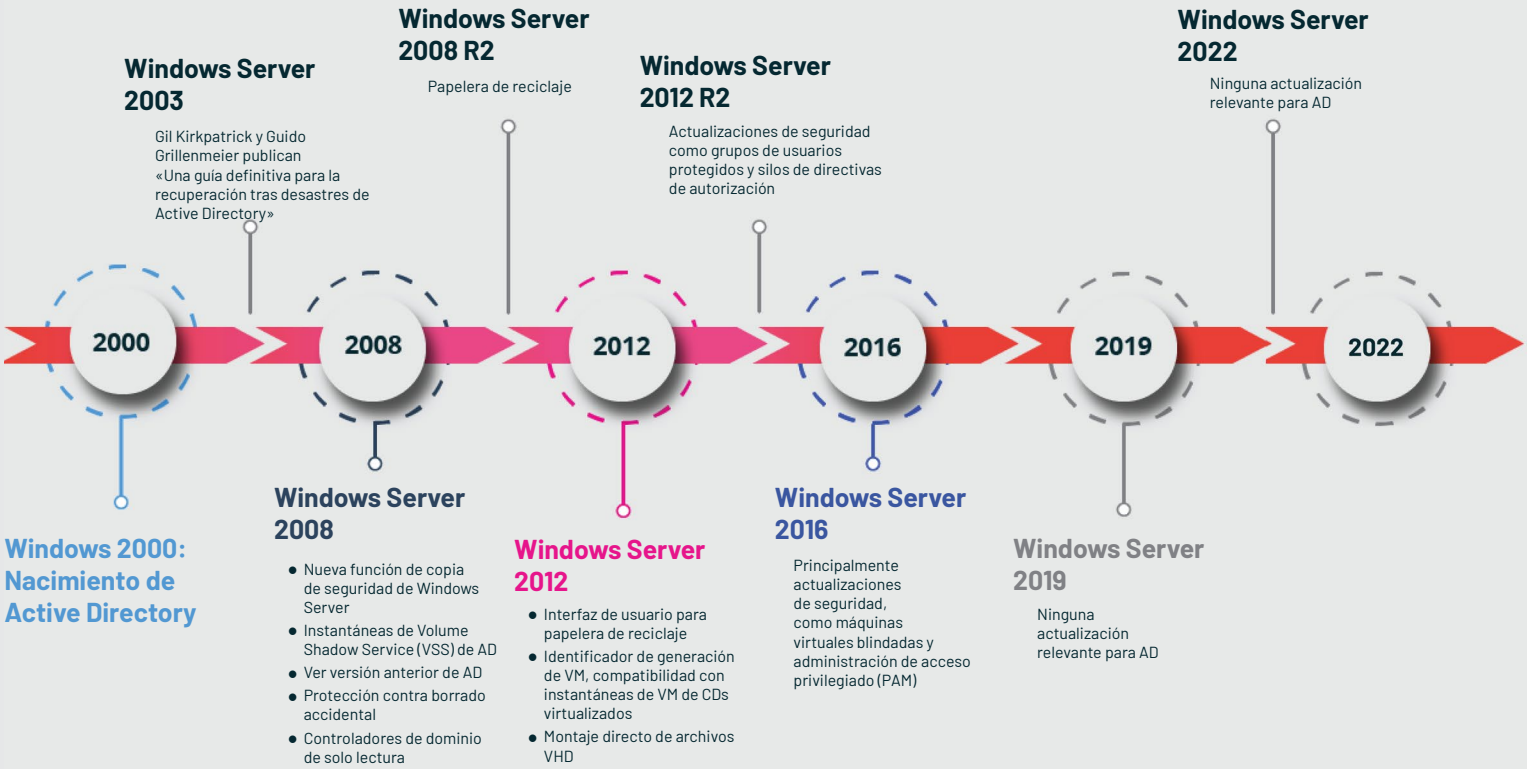
En la medida que el modelo de amenazas se ha transformado drásticamente desde 2005, también lo ha hecho el sistema operativo (SO) de Windows Server y su servicio de Active Directory integrado. Microsoft mejoró sustancialmente la seguridad de Windows, añadió funciones y capacidades para simplificar la recuperación de objetos de AD y mejoró el comportamiento de AD cuando se ejecuta en un entorno virtualizado. Pero los problemas fundamentales para recuperar un bosque completo de Active Directory a partir de una copia de seguridad no han cambiado. Todavía es un proceso complejo y propenso a errores que requiere planificación y práctica para todas las implementaciones de AD, excepto las más triviales.

Cabe destacar que las dos últimas versiones de Windows Server (Windows Server 2019 y 2022) son las primeras versiones de Windows Server sin actualizaciones relevantes para el servicio de AD en sí. Aparentemente, desde el punto de vista de Microsoft, no hay más problemas para reparar en AD y no se requieren más mejoras en el servicio. Concretamente, la recuperación tras desastres de AD no será nada fácil.

Necesitamos ahora evaluar las capacidades de recuperación de una empresa en el contexto de las nuevas ciberamenazas que afectan a AD hoy en día, de las que no teníamos que preocuparnos en 2005. Lamentablemente, el aumento de los ataques significa que las empresas deben prepararse con urgencia para una remediación rápida de los ataques contra su AD corporativo. Las mejoras que Microsoft ha realizado en el núcleo del servicio de AD a lo largo de los años pueden resultar de poca ayuda para recuperar su AD si recibe un ataque. ¿Está lista su empresa para recuperar rápidamente su propio AD corporativo en caso de un verdadero desastre que destruya todo el servicio de AD?

«Las empresas deben prepararse con urgencia para una remediación rápida de los ataques contra su AD corporativo».

Cambios relacionados con la copia de seguridad de Active Directory a lo largo del tiempo



¿Está lista su empresa para recuperar rápidamente su propio AD corporativo en caso de un verdadero desastre que destruya todo el servicio de AD?

POR QUÉ ES TAN IMPORTANTE PROTEGER ACTIVE DIRECTORY

Active Directory (AD) se encuentra en producción desde hace más de 20 años. Tal y como se diseñó originalmente, esta función de servidor de Microsoft proporciona:

Autenticación: Autentica a los usuarios on-premise que inician sesión en sus PC y en la red corporativa y a los usuarios remotos que inician sesión en aplicaciones alojadas internas o escritorios virtuales

Autorización: Controla a qué recursos integrados de AD, como servicios de archivos, impresión, Exchange Server, SharePoint Server y SQL Server, tienen permisos para acceder

Seguridad y control: La directiva de grupo puede aplicar configuraciones de directiva a cada ordenador, servidor y usuario que se une a AD

Directorio: Una sola ubicación para descubrir usuarios y recursos

DNS: DNS integrado en AD para proporcionar resolución de nombres de red

PKI: Los servicios de certificados de Active Directory proporcionan certificados para usuarios y equipos de dominio.

El aumento de la popularidad del sistema operativo Windows Server para proporcionar servicios básicos de uso compartido de archivos e impresiones, y otros servicios administrativos como correo electrónico, mensajería y colaboración, ayudó a consolidar AD como el directorio de red preferido. Microsoft hizo evolucionar prácticamente todas sus aplicaciones populares para basarse en él, lo que convirtió a AD en uno de los servicios de software más ubicuos en la empresa actualmente. Más del 90 % de las organizaciones de todo el mundo con más de 500 empleados utilizan AD.

El auge de la computación en la nube no ha cambiado esta dependencia. De hecho, la computación en la nube ha aumentado la importancia de AD para la empresa. Hay dos factores detrás de la importancia de AD para la nube.

En primer lugar, el modelo de computación en la nube no depende de redes confiables como lo hace la computación on-premise tradicional porque, a diferencia de las redes corporativas tradicionales, el tráfico entre los clientes y los recursos a los que acceden ocurre con mayor frecuencia a través de la Internet pública. Este tráfico no queda asegurado por el hecho de DÓNDE está, sino por el hecho de QUIÉN es. Como lo explica Microsoft, «la identidad es el plano de control» mediante el cual se controla el acceso a los recursos de la nube. La identidad de un usuario ocupa una posición central en la seguridad de la nube.

En segundo lugar, AD es la base de la arquitectura de identidad híbrida que se usa comúnmente en la actualidad. En esta arquitectura, las organizaciones sincronizan su almacén de identidad on-premise, generalmente AD, en el servicio de identidad en la nube de su elección, como Azure Active Directory, Okta o Amazon Web Services (AWS). Este enfoque permite a los usuarios usar su identidad corporativa para acceder a los recursos (por ejemplo, Office 365 o Salesforce) que están integrados en el servicio de identidad en la nube de la organización.

Además, muchas empresas todavía no confían tanto en los servicios en la nube como en sus sistemas internos controlados que están completamente administrados por su propio personal de TI; por tanto, muchas han decidido configurar un marco de autenticación federado utilizando los Servicios de federación de AD (ADFS) o soluciones similares para conectarse con soluciones en la nube, por ejemplo, Azure AD. En este caso, la validación de la identidad del usuario, es decir, la autenticación, continúa ocurriendo con su AD local. Luego, ADFS crea un token adecuado, el token SAML, que confirma al servicio en la nube (por ejemplo, Azure AD y aplicaciones asociadas) que el usuario que se conecta es realmente quien dice ser. Dado que el token SAML está cifrado convenientemente con una clave compartida solo entre ADFS y Azure AD, Azure AD confía plenamente en este token y otorga al usuario acceso a los recursos de la nube respectivos. Básicamente, en esta configuración Azure AD confía plenamente en su AD local.

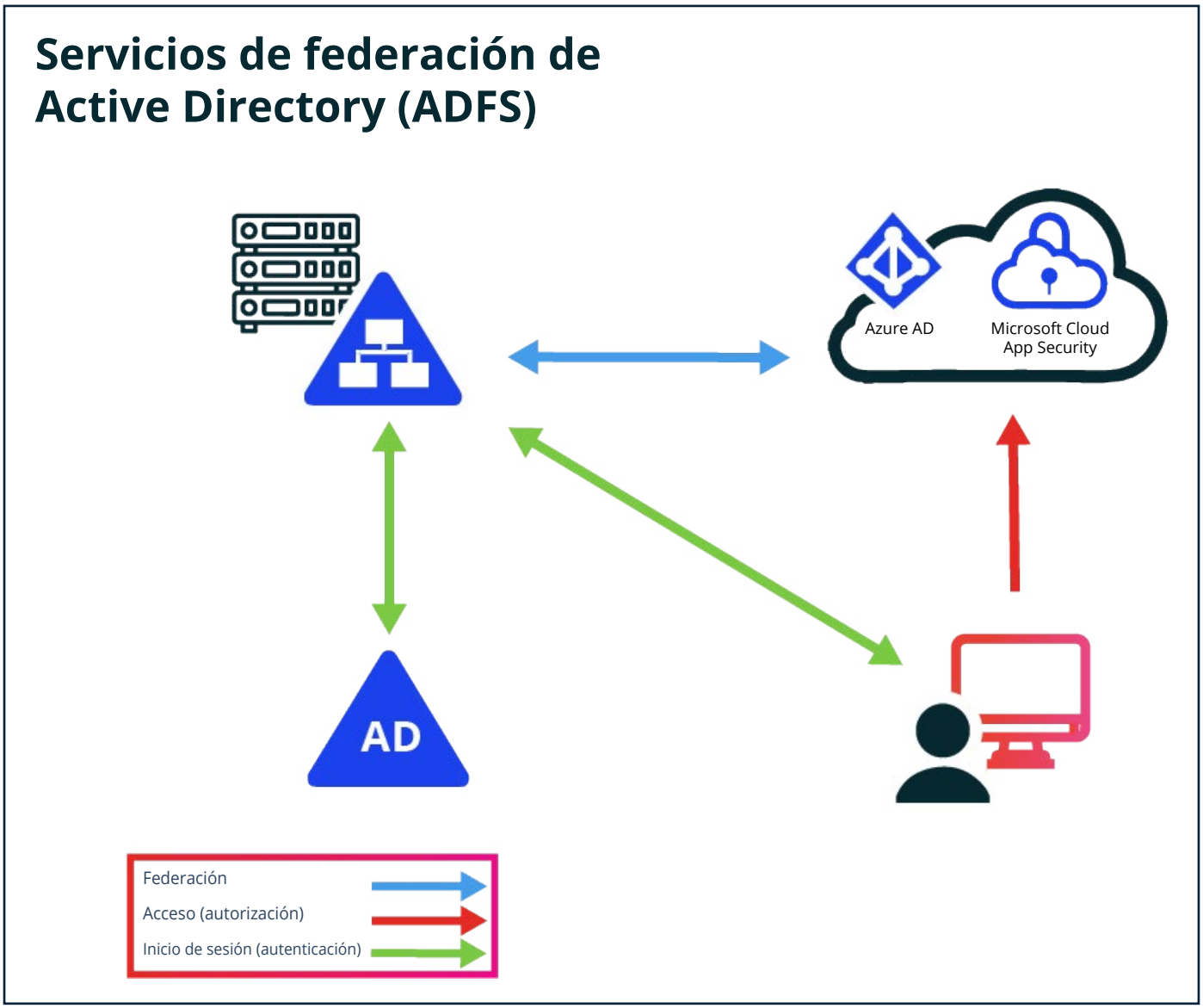


Figura 1: La federación generalmente se basa en su AD local para certificar la identidad de sus usuarios

Agregue a esto el hecho de que, a pesar de toda la promoción y el cambio a la computación en la nube, todas las organizaciones de cualquier tamaño o antigüedad tienen operaciones on-premise sustanciales y regulares que dependen de AD. Como resultado, AD hoy en día no solo sigue siendo esencial para acceder a los recursos on-premise, sino que también es un componente crítico de la empresa híbrida actual y todas sus aplicaciones.

CÓMO HA CAMBIADO EL PANORAMA DE AMENAZAS

Cuando se escribió la «Guía definitiva para la recuperación tras desastres de Active Directory», los principales desastres por los que los administradores de AD tenían que preocuparse se dividían en dos grupos: desastres físicos (como una falla de energía, un bloqueo del disco o una inundación) y errores administrativos (involuntarios o maliciosos) que modifican o eliminan objetos de AD de forma inapropiada. La tercera categoría, una falla de servicio en todo el bosque, era teóricamente interesante, pero casi nunca ocurría en la vida real. Aunque los efectos de una falla en todo el bosque fueran desastrosos, era tan poco probable que el riesgo residual resultante era algo con lo que la mayoría de las organizaciones simplemente vivían.

En 2021, ese cálculo de riesgo se invirtió por completo. AD continúa manejando bien los problemas del servidor físico y del sitio, y después de 10 a 20 años de experiencia, la mayoría de las organizaciones pueden administrar su Active Directory de manera confiable y segura. Pero los ciberdelincuentes, armados con sofisticadas herramientas de phishing y el último malware de reconocimiento, persistencia y cifrado de datos, pueden arrasar con un entorno Windows empresarial completo en unos pocos minutos. Las estadísticas recientes de ransomware son aleccionadoras.

En 2020:

El 51 % de las empresas se vieron afectadas por un ataque de ransomware. (Pentest Magazine)

El ransomware cuesta a las organizaciones aproximadamente $75 mil millones al año (Datto)

La exigencia de rescate promedio fue de $178 mil, con el mayor pago publicitado de $11,8 millones

La pérdida de todo el servicio de Active Directory se ha trasladado del peldaño inferior de la escalera de riesgos a la parte superior.

Active Directory es un objetivo prioritario para los ciberdelincuentes

Active Directory está bien diseñado para manejar desastres físicos. Si falla un DC, o incluso si todo un centro de datos se desconecta, AD seguirá funcionando con los controladores de dominio restantes. Microsoft añadió la función Papelera de reciclaje de AD en Windows Server 2008 R2, que cumple razonablemente bien con la recuperación de objetos eliminados de forma inadvertida. En lo que respecta a deshacer cambios involuntarios en los objetos de AD, prácticamente deberá actuar por su cuenta.

Está claro que AD es un servicio central crítico en casi todas las organizaciones. AD almacena credenciales de usuario, ordenador y servicio, y controla la autenticación y la autorización en todo el entorno on-premise. Esto convierte a AD en un objetivo apetecible para los autores de amenazas por tres razones:

- Como servicio de directorio, AD es un punto de concentración de la información que los autores de amenazas necesitan para moverse lateralmente a través de la red y elevar sus privilegios.
- Como servicio principal de autenticación y autorización, AD constituye un único punto de ataque que puede inutilizar el resto de la red.
- AD, como solución de facto de administración de la configuración de puntos finales, a través de la directiva de grupo, es otra herramienta que los atacantes pueden usar para distribuir malware y ganar persistencia en múltiples máquinas en la red.

Si bien por lo general nunca encontramos detalles técnicos en los artículos de prensa sobre ataques cibernéticos, comenzamos a notar que se menciona a Active Directory con mucha más frecuencia:

- El Active Directory de Virgin Mobile se vio comprometido y sus datos se vendieron en la Dark Web.
- NTT Communications admitió que su Active Directory se vio comprometido como parte de una violación de datos.
- Se ha demostrado que el ransomware Ryuk modifica la directiva de grupo para propagarse a los puntos finales a través de un script de inicio de sesión.

A decir verdad, siempre supimos identificar la posibilidad de que Active Directory formara parte de un ataque; ahora tenemos datos para probarlo.

POR QUÉ ACTIVE DIRECTORY ES VULNERABLE

Active Directory funciona bastante bien y su diseño ha resistido la prueba del tiempo. Sin embargo, el mundo ha cambiado a su alrededor, con la aparición de versiones criptográficas, su apertura a consultas, Kerberos y la creciente sofisticación de los ataques que emplean herramientas como Mimikatz.

Amenazas persistentes avanzadas (APTs): Infiltración y vulneración

Los ataques contra AD han aumentado drásticamente en los últimos años, ya que los malhechores se han dado cuenta de que si se apoderan de AD, se apoderan de los recursos de TI de la organización. Es evidente que AD «tiene las llaves del reino», pero incluso esa frase subestima el riesgo: El servicio también contiene un «mapa del tesoro» para todos los recursos integrados de AD de la organización que dependen de él. Si bien los usuarios finales no son conscientes de su dependencia de AD, las diversas herramientas y procesos comerciales que utilizan todos los días podrían no funcionar si AD no funciona. Esto incluye aplicaciones para servicios críticos como correo electrónico (Exchange), uso compartido de archivos (SharePoint, recursos compartidos de archivos normales), colaboración (Skype) o incluso la capacidad de imprimir. Muchas empresas utilizan además la autenticación integrada de Windows para muchas de sus aplicaciones y bases de datos comerciales, en la que «Windows integrado» es simplemente otro término para «AD integrado», es decir, las aplicaciones no dependen de su propia lista de usuarios, sino que «confían» en el token de acceso de un usuario generado por AD para otorgar el acceso adecuado a la aplicación. AD no solo controla el acceso a esas aplicaciones para usuarios legítimos, sino que también permite que los intrusos entiendan qué aplicaciones se han integrado en una infraestructura y, por lo tanto, las usen contra usted.

A medida que ha crecido la comprensión de que AD es un objetivo valioso, también lo han hecho los conjuntos de herramientas para atacarlo. PowerSploit, Bloodhound, Death Star, Cobalt Strike y especialmente Mimikatz han permitido a los atacantes encontrar rápidamente credenciales, realizar un reconocimiento horizontal en toda la red, encontrar la ruta más corta hacia los derechos de administración del dominio y dirigirse a esa ruta.

Estas herramientas reducen el tiempo para conseguir dominar un dominio de días a horas. Por consiguiente, atacar Active Directory con éxito es ahora más fácil que nunca.

El desastre cibernético: ataques DoA

AD es maravillosamente tolerante a fallas frente a desastres naturales o físicos. Los huracanes, tornados, terremotos, cortes de energía y otros eventos que destruyen un centro de datos afectarán localmente a un AD bien diseñado, pero permitirán que el resto de la red continúe utilizando el servicio. Cuando esa sección dañada de AD vuelva a funcionar, cualquier cambio que haya ocurrido en la red durante la interrupción fluirá automáticamente hacia la sección restaurada. Un incidente que elimine todo un dominio o bosque de AD tendría un impacto muy alto, pero también sería extremadamente raro debido a las precauciones que las empresas han tomado para distribuir geográficamente sus infraestructuras de AD. Por tanto, el riesgo de que AD no esté completamente disponible nunca se clasificó como más que moderado. Combinando esto con el hecho de que la continuidad comercial y la recuperación ante desastres (BCDR, por sus siglas en inglés) de Active Directory son muy costosas (hablaremos de ello más adelante), la planificación de BCDR tradicionalmente ha descuidado la recuperación del bosque.

Introduzca los ataques de denegación de disponibilidad (DoA). Las variantes más conocidas de esta categoría son el ransomware y el wiperware. Casi todo el mundo sabe qué es el ransomware. Cada vez son más frecuentes las noticias acerca de clientes, servidores y datos de alguna empresa que se encuentran encriptados y requieren cierta cantidad de bitcoins para obtener la clave de descifrado de los atacantes. El wiperware destruye sus ordenadores y datos, ya sea mediante el cifrado o la eliminación directa de datos, sin posibilidad de recuperación.

El ataque de NotPetya de 2017 es el ejemplo más conocido de esta especie hasta la fecha. La empresa de transporte de contenedores Maersk fue una de las principales víctimas. NotPetya borró miles de ordenadores y servidores de Maersk y, sí, todos los controladores de dominio de AD a nivel mundial, incluidas sus copias de seguridad. Tuvieron la suerte de que un corte de energía impidiera que el malware se propagara al controlador de dominio en su sitio de Ghana: Finalmente pudieron usar ese DC para recuperar su AD. Después de someterse a una recuperación muy costosa, que se estima costó a Maersk entre $250 millones y $300 millones, decidieron hablar públicamente sobre su situación para concienciar a otras compañías sobre el riesgo de ataque del malware moderno en su infraestructura. Las empresas deben prepararse contra esta amenaza, ya que la mayoría no sobreviviría a una interrupción de nueve días de su TI central, que es el tiempo que tardó Maersk en recuperar completamente su Active Directory.

Otras víctimas fuertemente afectadas por el ataque de NotPetya fueron, entre otros, FedEx, Saint-Gobain, Reckitt Benckiser y Mondelēz. Y el ataque de NotPetya no fue de ninguna manera el último ataque contra AD. Fue simplemente el comienzo de una nueva era de ataques de ransomware de rápida propagación que usan e impactan en Active Directory. Lamentablemente, los vectores de ataque contra AD son abundantes: recientemente, un ataque exitoso de Nefilim pudo usar una cuenta de administrador de dominio altamente privilegiada perteneciente a un empleado fallecido para abrir todas las puertas a los intrusos.

Sus copias de seguridad de Active Directory no le ayudarán a recuperar su servicio de AD

En caso de desastre cibernético, las copias de seguridad normales de Active Directory no le ayudarán a recuperar las operaciones comerciales después del ataque. La función «Proteger objetos de eliminación accidental» ayuda a evitar fallas humanas, pero no aborda la actividad maliciosa en su AD.

Lo mismo ocurre con la Papelera de reciclaje, que le permite recuperar objetos eliminados pero no puede ayudarle a deshacer los cambios a nivel de atributo, ni los cambios en los GPO o la configuración en su AD. La papelera de reciclaje tampoco puede ayudar a recuperar todo su dominio o bosque y las particiones de aplicaciones relacionadas.

El uso de instantáneas puede permitir la detección de cambios a nivel de atributo y ayudar a deshacerlos, pero añadirá una gran complejidad al proceso de recuperación.

Pero ninguno de estos métodos para restaurar datos de Active Directory será suficiente para ayudarle a recuperar el servicio de AD propiamente dicho: su dominio o bosque completo. Si bien todos esperamos no necesitarlo nunca, una corrupción de esquema debido a un cambio malicioso realizado por un intruso o el cifrado de todos sus DC por un malware puede requerir una recuperación a nivel del bosque de su AD. Para esto, necesitamos aún una copia de seguridad adecuada de los DC de AD.

Preparación de una copia de seguridad que permita la recuperación del servicio de Active Directory libre de malware

La recuperación del servicio de Active Directory, lo que significa que la recuperación de NTDS.dit y los archivos y configuraciones del sistema operativo relacionados para permitir la replicación adecuada de los datos de AD, es una tarea mucho más desafiante que la simple recuperación de objetos de AD específicos. Si todos los cambios en todos los objetos y atributos se mantuvieran en un único servidor de base de datos de AD (un único controlador de dominio), la capacidad de recuperación del servidor sería un asunto sencillo, similar a la de un servidor de archivos.

Sin embargo, el gran poder y éxito de Active Directory se basa en que, a diferencia de sus antecesores, los cambios realizados en el directorio no están restringidos a producirse en un solo servidor, o un solo maestro. En su lugar, AD se diseñó como una arquitectura de base de datos multimaestro, lo que permite que se produzcan cambios en cualquier controlador de dominio (de escritura) en la red de una empresa. Esto es lo que hizo posible la escalabilidad y la distribución geográfica del servicio de Active Directory y permite que un dominio o bosque de AD preste servicio a múltiples sitios que se encuentran repartidos por todo el mundo.

En la «Guía definitiva» completa cubrimos con más detalle puntos específicos sobre la copia de seguridad global de DC, pero tener en cuenta la distribución geográfica de sus DC de AD y sus copias de seguridad es tan importante como realizar la copia de seguridad en sí. En algún momento durante la planificación de la copia de seguridad de AD, debe considerar si las copias de seguridad de DC elegidas son suficientes para recuperar rápidamente su bosque de AD. Esto es particularmente desafiante en un bosque multidominio, es decir, un bosque con múltiples dominios secundarios o árboles paralelos que forman parte de la misma estructura de bosque de AD. Cuando tenga más de un dominio en su bosque de AD, el Catálogo global es una funcionalidad de AD necesaria que deberá reconstruirse y reactivarse durante el proceso de recuperación del bosque, antes de que los servicios de autenticación puedan comenzar nuevamente. Y reconstruir ese catálogo global llevará mucho más tiempo si no tiene al menos un DC de cada dominio de su bosque ubicado en el mismo sitio de AD. Más adelante mencionaremos otros retos para recuperar su bosque rápidamente.

Integración con Volume Shadow Copy Service

Huelga decir que la herramienta de respaldo que usa para hacer copias de seguridad de sus DC de Active Directory debe integrarse con la función Volume Shadow Copy Service (VSS) del sistema operativo Windows Server. Esta integración garantiza un estado coherente de su base de datos de AD en el momento de realizar una copia de seguridad; es decir, todas las operaciones de escritura en curso habrán finalizado y se habrán escrito en el disco, mientras que los nuevos cambios entrantes en la base de datos de AD se detendrán en el momento en que se realice una instantánea de la base de datos de AD. Este proceso toma solo unos segundos, tras lo cual la herramienta de respaldo tiene todo el tiempo que necesita para copiar el estado consistente de la base de datos de AD a un destino de su elección, mientras las operaciones de escritura en la base de datos de AD original pueden continuar manteniendo el controlador de dominio de AD funcionando como de costumbre.

La herramienta Windows Server Backup (WSB) integrada es un buen ejemplo de herramienta de copia de seguridad completamente integrada con VSS y le permite realizar dos tipos de copias de seguridad:

1. SSB (copia de seguridad del estado del sistema)
2. BMR (recuperación completa)

Las dos opciones son bastante diferentes en sus casos de uso, así que tenga cuidado con las diferentes funciones cuando planifique su estrategia de copia de seguridad.

Las copias de seguridad del estado del sistema pueden contener malware

La opción de copia de seguridad del estado del sistema realiza una copia de seguridad de todas las partes críticas del sistema operativo del servidor de un DC, incluida la base de datos de AD (NTDS.dit), la carpeta SYSVOL, la base de datos de registro de clase COM+, el registro del servidor y los archivos de inicio, pero evitando cualquier dato de usuario, discos adicionales y datos que podrían haberse añadido para otras aplicaciones que se ejecutan en el mismo servidor. Si bien la copia de seguridad usa las capacidades de VSS para crear una instantánea adecuada de los discos utilizados por el servidor, la transferencia de la copia de seguridad del estado real del sistema es una copia basada en archivos, de los archivos relevantes para el destino de la copia de seguridad, lo que no permite realizar copias de seguridad incrementales, es decir, siempre debe transferir el estado completo de su sistema a la ubicación de la copia de seguridad de destino. Además de su base de datos de AD, una copia de seguridad del estado del sistema almacena aproximadamente 11 GB de los archivos del sistema operativo Windows en cada copia de seguridad de DC.

La recuperación de la copia de seguridad del estado del sistema debe realizarse en la misma instancia de Windows Server e instalación del sistema operativo a partir de la cual se creó, lo que significa que se ha concebido para ayudar en caso de problema en el sistema operativo o a nivel de datos, pero no en caso de un problema de hardware que requiera reconstruir el servidor completo. Por tanto, una copia de seguridad del estado del sistema está bien para recuperar la base de datos de AD en los casos en que necesite restaurar con propiedad partes de una base de datos de AD para recuperar objetos eliminados accidentalmente de AD. Sin embargo, una copia de seguridad del estado del sistema no está destinada a ayudarlo a recuperar su copia de seguridad en un servidor recién implementado y ciertamente tampoco en uno con un hardware diferente o incluso con un cambio de arquitectura de física a virtual, o viceversa. Por supuesto, una copia de seguridad del estado del sistema puede ser su única opción si, después de un ataque cibernético, necesita recuperar sus DC de AD rápidamente en otro hardware o máquinas virtuales que podrían estar disponibles para usted con mayor rapidez. En cualquier caso, tenga en cuenta que la copia de seguridad del estado del sistema incluye varios archivos del sistema operativo del que se realizó dicha copia, lo que significa una probabilidad significativa de reinfección del malware del cual se realice una copia de seguridad con su AD.

> ***«Tenga en cuenta que la copia de seguridad del estado del sistema incluye varios archivos del sistema operativo del que se realizó dicha copia, lo que significa una probabilidad significativa de reinfección del malware del cual se realice una copia de seguridad con su AD».***

«Al igual que con las copias de seguridad del estado del sistema, se requiere precaución al restaurar AD desde las copias de seguridad BMR tras un ataque cibernético para evitar la reintroducción de malware».

Las copias de seguridad BMR también pueden contener malware

Como su nombre lo indica, las copias de seguridad creadas con la opción de recuperación completa (BMR), también llamadas copias de seguridad de «servidor completo», le permiten recuperar un servidor determinado a su estado de copia de seguridad, incluida la recuperación completa del sistema operativo y los servicios que se ejecutan en él, así como Active Directory. El objetivo es protegerlo de las fallas clásicas a nivel de hardware, como los discos averiados. Pero las copias de seguridad de BMR también tienen el potencial de reintroducir malware si se usan para restaurar AD.

La opción BMR realiza una copia de seguridad de todos los discos que utiliza el sistema operativo, lo que también incluye el estado del sistema. También puede optar por realizar copias de seguridad de discos adicionales en el servidor respectivo. Como se crea una copia de seguridad BMR con el método de copia de seguridad basado en bloques, también tiene la opción de configurar copias de seguridad solo de aquellos bloques que se modificaron desde la última copia de seguridad: Puede ejecutar una copia de seguridad incremental, haciendo sus respaldos aún más rápidos. Las copias de seguridad incrementales funcionan si ha configurado la opción adecuada en los ajustes de rendimiento de la copia de seguridad en su servidor y el disco de destino de la copia de seguridad está alojado en el mismo servidor del que está realizando la copia de seguridad. El último enfoque puede ser contrario al sentido común, pero funcionará si tiene mecanismos adicionales a mano para almacenar los archivos de copia de seguridad creados en algún otro destino de almacenamiento seguro posteriormente.

En el momento de la recuperación, debe iniciar el servidor reparado con un disco de instalación del sistema operativo Windows Server adecuado antes de poder recuperarlo desde el archivo de copia de seguridad respectivo. Tenga en cuenta que la instalación de este servidor también debe ser del mismo tipo de hardware y arquitectura. Por ejemplo, la opción BMR no le permite recuperar una copia de seguridad de un servidor Dell en uno nuevo de HPE ni elegir una máquina virtual como destino para la recuperación. Debido a esta limitación, y debido a que existe una opción sencilla para crear una nueva réplica de un controlador de dominio de AD, mediante su promoción después de una instalación limpia del sistema operativo en el hardware de cualquier elección, el método BMR rara vez se usa para realizar copias de seguridad de los DC de Active Directory. Al igual que con una copia de seguridad del estado del sistema, las copias de seguridad BMR están sujetas al mismo riesgo de incluir el malware que podría haber afectado sus DC de AD antes de volverse activo y dañar su bosque de AD. Al igual que con las copias de seguridad del estado del sistema, se requiere precaución al restaurar AD desde las copias de seguridad BMR tras un ataque cibernético para evitar la reintroducción de malware.

Tenga en cuenta también que ni las copias de seguridad SSB ni BMR están cifradas por la función de copia de seguridad de Windows Server, lo que significa que sus copias de seguridad son vulnerables en tránsito y ciertamente en reposo, si no ha cifrado el disco que contiene sus copias de seguridad. Esto también significa que no debe copiar los archivos de copia de seguridad en otro sistema de almacenamiento de destino al que puedan acceder los administradores que no pertenecen al dominio sin antes cifrarlos correctamente.

Asegúrese de almacenar los archivos de copia de seguridad de forma segura, asegurándose de que solo los administradores del servicio de AD tengan acceso a ellos.

Tenga cuidado con las instantáneas

¡Las instantáneas son malas! ¡Las instantáneas al rescate!

Ambas afirmaciones tienen cierto nivel de veracidad. Hasta el lanzamiento de Windows Server 2012, que añadió un identificador adecuado de la versión de una VM al usar instantáneas a nivel de VM (VMGenID), Microsoft tuvo que advertir continuamente sobre la falta de compatibilidad de tomar instantáneas de DC en entornos virtuales. Los administradores podían cometer fácilmente el error de «hacer retroceder en el tiempo» un DC sin usar el método de recuperación de AD adecuado para informar a otros DC en el entorno sobre esta reversión. Ese descuido podía causar todo tipo de problemas de replicación al interrumpir la lógica de replicación integrada del complejo ecosistema de AD. Podía ocurrir una reversión del número de secuencia de actualización (USN) y, con ello, un estado de objeto no confiable en el bosque de AD con el potencial de crear SID duplicados y objetos persistentes.

Suponiendo que a estas alturas todos sus controladores de dominio en todo el mundo funcionan al menos con Windows Server 2012 y está utilizando un hipervisor que admite la lógica VMGenID (todos los principales hipervisores lo han estado haciendo durante años), podemos ahorrarnos los detalles de por qué revertir los controladores de dominio a una versión anterior a través de una instantánea de VM fue algo realmente malo. Si bien todavía no es un mecanismo de respaldo para su bosque de AD, al menos ya no puede dañar su AD cuando usa la tecnología de instantáneas de VM.

En el próximo documento técnico, «La nueva guía definitiva para la recuperación tras desastres de Active Directory», cubriremos los cambios críticos que Microsoft introdujo con Windows Server 2008 que afectaron la copia de seguridad y la recuperación nativas de AD: La integración de la base de datos de AD con las capacidades VSS del sistema operativo. También cubriremos la característica renovada de Windows Server Backup (WSB), también introducida con Windows Server 2008, que hizo que los datos de copia de seguridad fueran accesibles como un archivo VHD. Y proporcionaremos detalles sobre la práctica característica que Microsoft agregó con la versión de 2012, la capacidad de montar archivos VHD directamente en un cliente de Windows existente, lo que permite la búsqueda rápida de una versión anterior de la base de datos de AD.

Todos estos cambios facilitan a los administradores, por ejemplo, recuperar archivos de una versión anterior de su carpeta SYSVOL o usar una versión de solo lectura de sus datos de AD para recuperar atributos sobrescritos de cualquiera de sus objetos. La clave aquí desde la perspectiva de cerrar las brechas de seguridad de Active Directory es proteger adecuadamente sus archivos de respaldo, ya que cualquier persona que tenga acceso a esos archivos confidenciales puede hacer todo lo que usted puede. Incluso pueden usar otras herramientas de edición fuera de línea para obtener los hash de contraseñas y otros datos confidenciales de la copia de seguridad de AD. Asegúrese de almacenar los archivos de copia de seguridad de forma segura, asegurándose de que solo los administradores del servicio de AD tengan acceso a ellos.

Tenga cuidado con las limitaciones de las herramientas de respaldo de terceros

Esencialmente, cualquier herramienta de respaldo que reivindique realizar una copia de seguridad de AD hoy en día se integrará también con las capacidades VSS del sistema operativo o incluso podría aprovechar la función Windows Server Backup (WSB) y simplemente ganar en inteligencia para realizar una copia de seguridad centralizada de una selección adecuada de sus DC.

Sin embargo, al igual que con la herramienta WSB incorporada, poder realizar una copia de seguridad de los controladores de dominio de AD no significa automáticamente que una herramienta pueda ayudarlo a recuperar rápidamente su bosque de AD en caso de que su esquema esté dañado o todos sus DC hayan sido infectados por un malware o algún otro ciberataque. Tenga en cuenta que la mayoría de las soluciones de respaldo que se concentran en copias de seguridad a nivel del sistema operativo pueden funcionar bien para recuperar servidores individuales, incluso controladores de dominio, pero (como se aclara en la siguiente sección) no son capaces de coordinar el complejo proceso de recuperación que se requiere para restablecer su bosque de AD después de un ciberataque.

Otra consideración aleccionadora: El riesgo de volver a introducir el malware que podría haber estado almacenado en el sistema operativo Windows de sus DC de AD durante muchas semanas o meses sin ser detectado. Es probable que dicho malware se almacene en sus copias de seguridad de AD si una herramienta de terceros realiza la copia de seguridad estándar del estado del sistema o la copia de seguridad BMR de sus DC, como es el caso de la herramienta WSB integrada.

MÁS RECURSOS

WHITE PAPERS

- Evaluación de la rentabilidad de la inversión de una recuperación rápida de Active Directory
- Informe: Recuperación de Active Directory ante desastres cibernéticos

WEBINAR

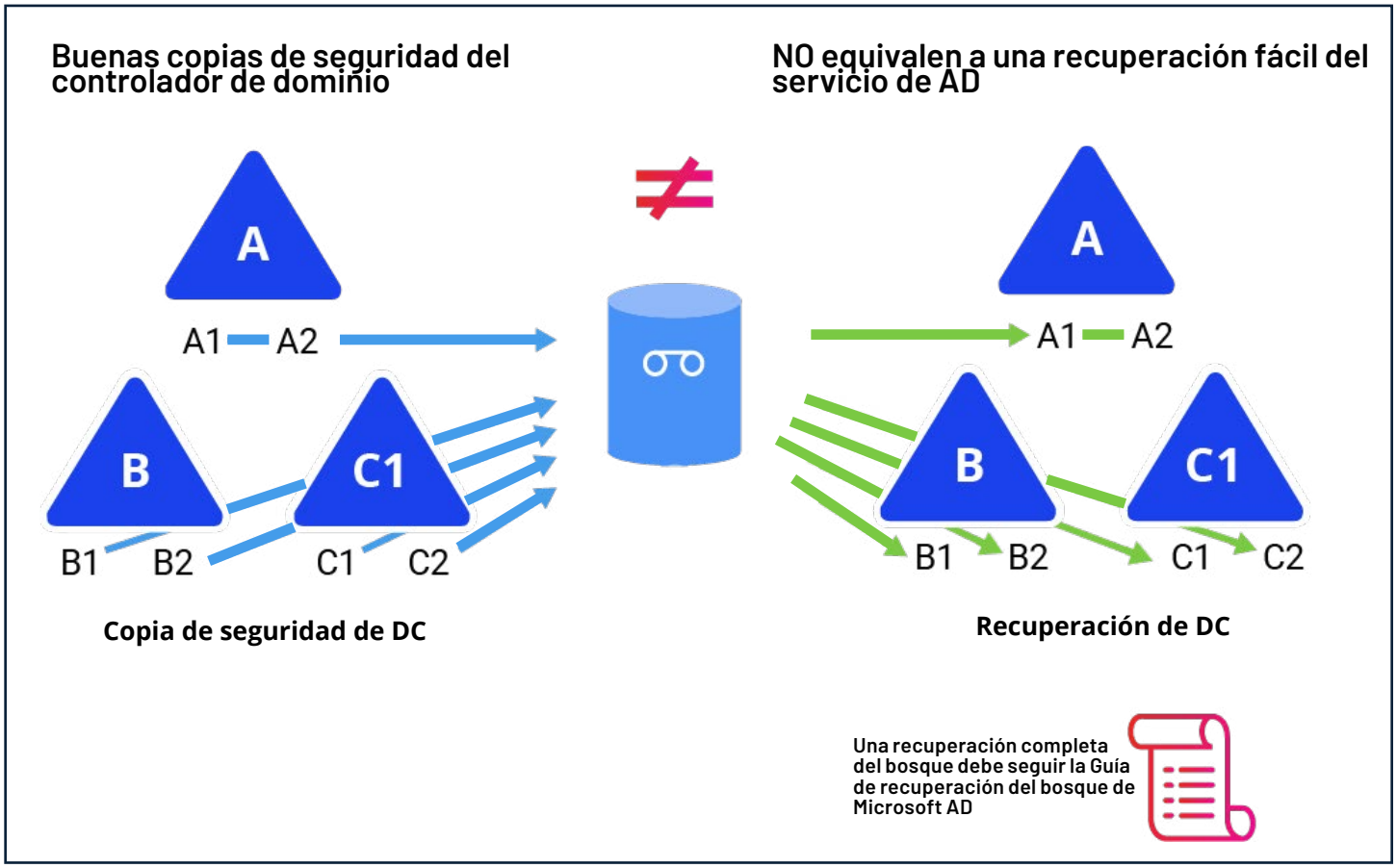
- El enfoque «Cyber-First» para la recuperación ante desastres

BLOGS

- Ahora es el momento de repensar la seguridad de Active Directory
- ¿Es hora de dejar atrás ADFS para la autenticación en entornos híbridos?
- Lo que se debe y no se debe hacer en la recuperación de Active Directory
- Cronología de un ataque de Hafnium

RECUPERACIÓN DE ACTIVE DIRECTORY

Cuando se habla de la recuperación de Active Directory, es importante distinguir entre la recuperación de datos (usuarios, grupos, equipos, directiva de grupo, etc.) y la recuperación del servicio AD: la aplicación distribuida que se ejecuta en múltiples servidores designados que contienen la carga de trabajo de los servicios de dominio de Active Directory, configurada en una topología específica. El hecho de que todos los controladores de dominio en el bosque compartan la configuración de la topología de AD y el esquema de la base de datos dentro de su propia base de datos de AD no facilita esta tarea.



El hecho de que haya realizado una copia de seguridad de todos los controladores de dominio de AD necesarios no significa que tenga una «manera fácil» de restaurar el servicio de AD completo, todo el bosque de AD, si precisa hacerlo en caso de un verdadero desastre. Cuando el malware está eliminando todos sus DC, deberá seguir el penoso proceso de recuperar su AD desde una instalación mínima.

El proceso de recuperación del bosque de Active Directory puede ser penoso

Como se expuso, en el panorama de amenazas de creciente vulnerabilidad que enfrentan los sistemas de TI, las redes, las aplicaciones y la seguridad de la identidad, no la geografía, determinan el alcance de un desastre. La tolerancia a fallas establecida por tener múltiples centros de datos se torna inútil frente al malware sofisticado que se propaga a través de una red en minutos.

Como consecuencia, el riesgo de un bosque de AD completamente destruido ha pasado de ser un temor inquietante para los administradores de AD a una posibilidad muy real.

Recientemente, los clientes de Microsoft se enfrentaron al siguiente gran ataque a un producto muy estrechamente integrado con su AD local: cuatro nuevas vulnerabilidades de día cero en Microsoft Exchange permitieron que el grupo de ciberdelincuentes de China llamado «Hafnium» inyectara un código malicioso en servidores Exchange de más de 30 000 organizaciones, antes de que pudieran parchearse correctamente. El ataque da a los intrusos un control total y remoto sobre los sistemas afectados. Debido a los permisos generalizados que tiene Microsoft Exchange en Active Directory, este último es un siguiente objetivo fácil. Por lo general, AD se infiltraría primero para elevar los privilegios de los intrusos a fin de obtener datos confidenciales de la organización atacada que se copian a un objetivo externo bajo el control de los intrusos. En la siguiente etapa, los intrusos suelen tardar un día o semanas en propagar y distribuir ransomware a todos los sistemas a los que pueden acceder. Mientras tanto, la organización objetivo aún no se da cuenta de que ha sido pirateada y realiza tranquilamente copias de seguridad de los sistemas infectados con sus rutinas de respaldo diarias (en promedio, según FireEye, un atacante permanece alrededor de 72 días sin ser detectado en una red comprometida). Finalmente, activan el ransomware que cifra los sistemas afectados e incluiría todos los sistemas miembros de la organización en AD, así como todos los controladores de dominio de AD. En un último paso, los ciberdelincuentes responsables solicitan un enorme rescate a la organización afectada por la promesa (pero sin garantía) de una clave de descifrado y de no vender los datos robados.

¿Por qué no simplemente restaurar desde copias de seguridad?

Entonces, en el caso de un verdadero desastre de su servicio de AD, ¿por qué no simplemente restaurar todos sus DC desde las copias de seguridad? Como se mencionó anteriormente, una «buena copia de seguridad» de esos servicios con la función AD DS instalada (los controladores de dominio) no significa un proceso fácil para la recuperación del servicio de Active Directory. Hay muchos pasos que debe seguir para restaurar su servicio AD a un estado confiable.

Superar con éxito el proceso de recuperación requiere la coordinación entre los ingenieros de AD, los equipos de operaciones de recuperación y, muy probablemente, los equipos de administración de virtualización, en cada ubicación en la que pretenda recuperar sus DC.

El proceso de recuperación de AD

Con el tiempo, muchos administradores de AD se han convencido a sí mismos de que lo tienen todo cubierto, pero no se trata solo de «seguir los pasos» de la Guía de recuperación de bosques de AD en línea cuando llegue el momento. Y no es solo el proceso lo que dificulta la recuperación del bosque; también es un desafío logístico y de formación. Superar con éxito el proceso de recuperación requiere la coordinación entre los ingenieros de AD, los equipos de operaciones de recuperación y, muy probablemente, los equipos de administración de virtualización, en cada ubicación en la que pretenda recuperar sus DC. Todos deben ejecutar sus tareas a la perfección, en el orden correcto, probablemente en el entorno de mayor estrés de sus carreras.

Hoja de ruta de alto nivel para la recuperación del bosque de AD

A continuación, una síntesis rápida de los pasos involucrados en la recuperación de un bosque de AD a un estado seguro conocido:

1. Determinar la estructura del bosque y las copias de seguridad disponibles

2. Identificar un DC único para cada dominio con una copia de seguridad válida

3. Apagar todos los DC en el bosque

4. Recuperar en primer lugar el dominio raíz del bosque

5. Recuperar luego un DC de cada dominio secundario

6. Limpiar y volver a promover todos los demás DC en el bosque

- Garantice la recuperación de la jerarquía de confianza y los registros de recursos críticos de DNS

- Garantice la recuperación de los dominios principales antes de sus dominios secundarios para mantener la jerarquía de confianza

La recuperación ante desastres de AD no es fácil

La recuperación ante desastres de AD no es una tarea sencilla. Idealmente, se prepara con un análisis de riesgo completo para su propio entorno: ¿La estrategia de mitigación es demasiado costosa o el riesgo residual es demasiado alto?

Además del equipo que administra Active Directory, debe involucrar a otros equipos, como su equipo de respuesta a incidentes, en la planificación para enfrentar esta tarea. Tenga criterios claros para invocar el plan de recuperación ante desastres de AD y responsabilidades claras para ejecutarlo. Combine ello con una estrategia de comunicación clara.

Sobre todo, considere cuidadosamente las inversiones para la prevención de desastres; esto puede resultar más económico que la recuperación tras los desastres.

SOBRE LOS AUTORES

GUIDO GRILLENMEIER es tecnólogo jefe de Semperis. Establecido en Alemania, Guido fue MVP de Microsoft para servicios de directorio durante 12 años. Pasó más de 20 años en HP/HPE como ingeniero jefe. Presentador frecuente en conferencias tecnológicas y colaborador de revistas técnicas, Guido es coautor de Fundamentos de seguridad de Microsoft Windows. Ha ayudado a diversos clientes a proteger sus entornos de Active Directory y ha respaldado su transición a Windows 10/m365 y los servicios en la nube de Azure.

GIL KIRKPATRICK es arquitecto jefe de productos en Semperis. Gil lleva muchos años creando productos comerciales para TI empresarial, centrándose principalmente en la gestión de identidades y productos relacionados con la seguridad. Ha sido 15 veces MVP de Microsoft para Active Directory y Enterprise Mobility, autor de Programación de Active Directory y fundador de la Conferencia de expertos en directorios. Gil interviene sobre temas de seguridad cibernética, identidad y recuperación ante desastres en conferencias de TI en todo el mundo.

+1-703-918-4884
info@semperis.com
www.semperis.com

221 River Street
9th Floor
Hoboken, NJ 07030

Semperis garantiza a los equipos de seguridad encargados de defender los entornos híbridos y multinube la integridad y la disponibilidad de los servicios de directorio empresariales críticos en cada fase del proceso de "cyber kill chain" (o cadena de exterminio de la ciberseguridad) y reduce el tiempo de recuperación en un 90%. La tecnología patentada de Semperis se ha creado específicamente para asegurar los entornos híbridos de Active Directory y protege más de 50 millones de identidades frente a los ciberataques, las violaciones de datos y los errores operativos. Las organizaciones líderes de todo el mundo confían en Semperis para detectar las vulnerabilidades, interceptar los ciberataques en curso y recuperarse rápidamente del ransomware y de otros sucesos que afectan a la integridad de los datos. Semperis tiene su sede en Nueva Jersey, en los Estados Unidos, y opera internacionalmente. Su equipo de investigación y desarrollo está repartido entre San Francisco, en los Estados Unidos, y Tel Aviv, en Israel.

Semperis es la anfitriona de la galardonada conferencia sobre Protección de Identidad Híbrida (www.hipconf.com). La empresa ha recibido las más altas distinciones del sector; recientemente ha sido considera como la empresa n.º 157 de la lista Inc. 5000 y como la cuarta compañía con un crecimiento más rápido de la zona estadounidense de los tres estados y se ha situado en el puesto 35 de la clasificación global de la lista Technology Fast 500™ de 2020 de Deloitte. Semperis está acreditada por Microsoft y ha sido reconocida por Gartner.

semperis