Windows Server 2016: Novedades y cómo impacta en Active Directory

INTRODUCCIÓN

Windows Server 2016 representa un importante avance para el sistema operativo Windows. Al igual que Windows Server 2012 y 2012 R2, Windows Server 2016 incluye cientos de nuevas funciones y ofrece capacidades nuevas e interesantes que, anteriormente, no estaban disponibles para los administradores de Windows. Si bien puede ser tentador apresurarse para implementar algunas de estas capacidades nuevas tras el lanzamiento del sistema operativo, los administradores prudentes usarán el tiempo que precede a la implementación para evaluar el estado y la preparación de los entornos de su Active Directory (AD).

NOVEDADES SOBRE WINDOWS SERVER 2016

Windows Server 2016 ofrece una gran cantidad de funciones y mejoras nuevas. Las siguientes son algunas de las mejoras de Active Directory que vale la pena destacar:

Membresía de grupo temporaria.

La membresía de grupo temporaria permite a los administradores agregar un usuario a un grupo de seguridad por un tiempo limitado. Por ejemplo, un administrador podría permitirle al usuario ser miembro de un grupo por un tiempo suficiente como para que instale una aplicación o complete un proyecto en particular. Sin embargo, cabe destacar que esta función requiere que Active Directory opere al nivel funcional de Windows Server 2016. Por lo tanto, las empresas deben comenzar a pensar en qué se requerirá para la transición al nivel funcional necesario.

Servicio de Federación de Active Directory

Microsoft también está realizando cambios importantes en los Servicios de Federación de Active Directory (AD FS). Los siguientes son especialmente importantes:

- **Control de acceso condicional**: En el pasado, el control de acceso basado en Active Directory era relativamente directo, ya que los administradores generalmente podían suponer que los usuarios iniciarían sesión desde un equipo unido a dominio que se había protegido adecuadamente a través de la política grupal. Una vez que los usuarios eran autenticados con éxito en Active Directory, podían acceder a cualquier recurso para el cual se les había otorgado permisos.

  Sin embargo, hoy en día los usuarios acceden a los recursos desde todo tipo de dispositivos, muchos de los cuales no están unidos al dominio y funcionan fuera del perímetro de la empresa. Para mejorar la seguridad en esta realidad moderna, Microsoft

está presentando la función de Control de acceso condicional, que permite a los administradores controlar mejor los intentos de acceso a los recursos por parte de los usuarios, mediante la creación de criterios adicionales que puedan aplicarse según las aplicaciones individuales. Por ejemplo, un administrador podría requerir la autenticación multifactor y un dispositivo compatible cada vez que un usuario accede a aplicaciones empresariales especialmente confidenciales.

- **Soporte para LDAP v3**: Otro cambio importante que Microsoft está implementando con respecto a AD FS es el soporte para LDAP v3. Esta nueva capacidad facilitará mucho más la federación de identidades en múltiples tipos de directorio. Por ejemplo, una empresa que usa un directorio que no es de Microsoft para el control de identidad y acceso puede federar estas identidades en Office 365 o en la nube de Azure. De manera similar, el soporte para LDAP v3 facilitará la configuración del inicio de sesión único para las aplicaciones de SaaS.

DNS

Es imposible hablar de Active Directory sin analizar también el DNS. Desde su introducción, Active Directory de Windows ha tenido dependencia de DNS. Si bien los servicios del DNS de Windows han permanecido relativamente intactos durante muchos años, Windows Server 2016 ofrece muchas mejoras y funciones nuevas del DNS, incluidas las siguientes:

- **Políticas del DNS**: Una de las nuevas capacidades más significativas es la habilidad para crear políticas de DNS. Las políticas de DNS permiten a los administradores obtener control sobre la manera en que el DNS responde a varios tipos de consultas. Por ejemplo, estas políticas son útiles para el equilibrio de carga y el bloqueo de las solicitudes del DNS desde direcciones IP o dominios conocidos por ser maliciosos.

- **Límite de índice de respuesta**: Los administradores ahora también pueden limitar el índice del servidor de DNS o la respuesta a las consultas. Esta función posibilita la defensa contra los ataques por denegación de servicio al limitar la cantidad de veces por segundo que el DNS puede responder a las solicitudes de un cliente.

- **IPAM de Microsoft**: La mejora más importante en el DNS está relacionada con la función de Administración de direcciones IP (IPAM) de Microsoft, que ayuda a los administradores a realizar un seguimiento del uso de direcciones IP. Aunque la función IPAM de Microsoft siempre se ha integrado muy bien en el DHCP, su integración en el DNS ha sido mínima. Con Windows Server 2016 se pretende cambiar esto al incluir las capacidades de administración del DNS y alojar la colección de inventario de registros. No obstante, la función de IPAM más aceptada tal vez sea el soporte para múltiples bosques de Active Directory. La función IPAM de Windows Server 2016 podrá administrar el DNS y los servidores DHCP en múltiples bosques de Active Directory, siempre que exista una confianza mutua entre estos bosques, y la función IPAM de Windows Server 2016 esté instalada en cada bosque.

LIMPIAR O REESTRUCTURAR ACTIVE DIRECTORY

Antes de implementar Windows Server 2016, es importante tomarse tiempo para limpiar y, posiblemente, reestructurar Active Directory. Si sigue los pasos que se indican a continuación, puede reducir los costos y los plazos de migración a Windows Server 2016, y entregar un nuevo entorno seguro, menos costoso y mucho más fácil de administrar.

> Antes de que implemente Windows Server 2016, tómese el tiempo para limpiar y, posiblemente, reestructurar Active Directory.

Realizar un inventario de los controladores de dominio

Uno de los primeros pasos en el proceso de limpieza es realizar un inventario de los controladores de dominio. Lo ideal sería que todos los controladores de dominio se actualicen a Windows Server 2016. Si su empresa necesita conservar los controladores de dominios heredados, recuerde eliminar o actualizar los que estén en ejecución en Windows Server 2003, que ya no cuenta con soporte. También asegúrese de que los niveles funcionales del dominio y bosques sean superiores a Windows Server 2003.

Registre sus aplicaciones

Además, realice un inventario de todas las aplicaciones que dependen de Active Directory, para asegurarse de que las actualizaciones no sean la causa de los problemas relacionados con las aplicaciones. Como no hay herramientas nativas para lograr esto, debe considerar la opción de recurrir a una solución de terceros, como Change Auditor de Quest para consultas de Active Directory.

Compruebe la integridad de Active Directory

Los objetos de Active Directory se almacenan en bases de datos, en los controladores de dominio. Al igual que cualquier otro tipo de bases de datos, la base de datos de Active Directory puede experimentar (y a veces lo hace) problemas relacionados con la integridad de las bases de datos. La herramienta nativa NTDSUTIL de Microsoft puede verificar la suma de comprobación de la base de datos de Active Directory y realizar diversas comprobaciones de la integridad de la base de datos, pero el hecho de que Active Directory pueda distribuirse en numerosos controladores de dominio puede hacer que estas comprobaciones no resulten prácticas en entornos más grandes. Esto es especialmente cierto si se tiene en cuenta el hecho de que es importante probar la integridad de Active Directory de manera continua. Las herramientas de terceros, como Active Administrator for Active Directory Health de Quest, pueden ofrecer mejores resultados con mucho menos esfuerzo.

Identificar y eliminar los objetos huérfanos

Los objetos huérfanos de Active Directory pueden suponer un riesgo de seguridad y deben limpiarse. Las empresas más pequeñas pueden purgar manualmente Active Directory para eliminar objetos huérfanos de usuarios y equipos, pero este tipo de limpieza manual sería casi imposible de realizar en las grandes empresas, debido a la gran cantidad de objetos de usuarios y equipos que existen y la dificultad para establecer una diferencia entre un objeto que ya no se necesita y un objeto que aún está en uso.

Respecto de la limpieza manual, otro obstáculo es que las herramientas, como la consola de usuarios y equipos de Active Directory, no muestran la mayoría de los objetos en Active Directory. Microsoft sí ofrece una herramienta gratuita, ADSIEdit, que expone todos los objetos en Active Directory. Sin embargo, ADSIEdit elude los elementos de protección integrados en la consola de usuarios y equipos de Active Directory, por consiguiente, puede generar la pérdida de datos o daño en Active Directory si se usa de manera incorrecta. Por lo tanto, si desea limpiar su Active Directory mediante ADSIEdit, primero realice una copia de respaldo de Active Directory y asegúrese de entender bien las repercusiones de cada medida que tome. Puede reducir significativamente el riesgo y la complejidad de identificar y eliminar objetos huérfanos mediante el uso de una herramienta de terceros.

Considerar la reestructuración

La migración a Windows Server 2016 le da la oportunidad de entender mejor los datos que tiene archivados en el servidor y cómo están organizados. También le da la oportunidad de reestructurar su Active Directory para satisfacer mejor sus necesidades actuales y futuras. Por ejemplo, deberá entender cuáles son los datos archivados en el servidor que deben migrarse y cuáles no. También puede descubrir la necesidad de consolidar algunos bosques o mantener partes nuevas de la infraestructura para las oficinas remotas que no existían cuando implementó originalmente Active Directory. Muchas empresas implementaron por primera vez el AD en Windows Server en el año 2000 y la topología aún se parece bastante. Sin embargo, muy probablemente los modelos comerciales y las necesidades de su empresa hayan cambiado bastante desde el año 2000.

Minimizar el impacto en la empresa

El análisis exhaustivo de todos los procesos, aplicaciones y usuarios que requieren acceso lo ayudará a garantizar que los recursos y las aplicaciones adecuados estén disponibles cuando se realice la migración. Antes de realizar la migración, es fundamental identificar los flujos de trabajo, las casillas de correo, los programas y otras partes de la infraestructura que puedan verse afectados.

Debe hacerse las siguientes preguntas críticas: ¿Cómo se asegurará de que no haya tiempo de inactividad durante la transición? ¿Qué debe hacer para asegurarse de que la productividad de los empleados no se vea afectada antes, durante y después de la migración? Un error común (y posiblemente irrecuperable) es subestimar el impacto de la migración en los usuarios y las operaciones, y no analizar todos los access points. Puede evitar estos problemas al programar las tareas de migración que requieren muchos recursos para las horas de menor actividad, a fin de reducir el impacto en los sistemas de producción, los usuarios finales y la productividad.

Un descuido frecuente suele ser que no se logra proporcionar la coexistencia sin interrupciones entre los sistemas

> La migración a Windows Server 2016 le da la oportunidad de reestructurar su Active Directory, para satisfacer mejor las necesidades actuales y futuras de su empresa.

El tamaño del entorno de su AD puede tener un impacto directo y significativo en el costo del uso de Azure AD Connect, de tal manera que la limpieza del directorio es primordial.

nuevos y existentes, lo que puede llevar a la interrupción del servicio, la falta de productividad y al aumento de los costos empresariales. La coexistencia es esencial en cualquier migración, consolidación o reestructuración de Active Directory porque los usuarios necesitan mantener el acceso a los recursos que los mantienen productivos. Debe asegurarse de que sus directorios estén sincronizados y que los usuarios siempre puedan acceder a sus datos.

¿QUÉ SUCEDE CON LA NUBE?

Microsoft permite a las empresas conectar sus entornos locales de Active Directory a Azure AD y Office 365 a través de Azure AD Connect. Además de ofrecer conectividad entre los directorios locales y de la nube, Azure AD Connect también puede ofrecer servicios de sincronización de directorio. Para usar Azure AD Connect, las empresas deben implementar un servidor de Azure AD Connect. Este servidor actúa como un proxy entre los directorios locales y en la nube.

La limpieza de AD puede reducir significativamente los costos

Las empresas que planean usar Azure AD Connect deben hacer un esfuerzo conjunto para consolidar, reestructurar o limpiar de algún otro modo los entornos de Active Directory con anticipación, porque los requisitos de Azure AD Connect varían según la cantidad de objetos que haya en Active Directory, y el tamaño del entorno de Active Directory puede tener un impacto directo e importante en el costo del uso de Azure AD Connect.

Según Microsoft, Azure AD soporta, de manera predeterminada, hasta 50.000 objetos de directorio. Este límite aumenta a 300.000 objetos una vez que se verifica el uso previsto del dominio con Azure AD. Si una empresa requiere más de 300.000 objetos de directorio, entonces Microsoft requiere que se abra un caso de soporte. Aun así, el límite es 500.000 objetos de directorio. Si el directorio necesita admitir más de 500.000 objetos, Microsoft exige que la empresa compre licencias para Office 365, Azure AD Basic, Azure AD Premium o para Enterprise Mobility Suite. De por sí, las empresas con directorios más grandes pueden reducir sus costos al tomarse el tiempo para reducir la cantidad de objetos almacenados en los entornos de Active Directory.

La cantidad de objetos almacenados en el directorio de una empresa afecta no solo los requisitos de licencia de Azure AD, sino también los requisitos de licencia para el servidor de Azure AD Connect. Azure AD Connect almacena información sobre la identidad de los usuarios. De manera predeterminada, Azure AD Connect utiliza SQL Server 2012 Express, que Microsoft pone a disposición de los clientes sin costo alguno. No obstante, cabe destacar que SQL Server 2012 Express está diseñado para tareas livianas. A diferencia de otros editores de SQL Server, SQL Server 2012 Express tiene un límite de tamaño de las bases de datos de 10 GB. Según Microsoft, una base de datos de 10 GB es suficiente para almacenar alrededor de 100.000 objetos de Active Directory.

Las empresas que tienen más de 100.000 objetos en sus directorios deben configurar Azure AD Connect para usar una instalación de SQL Server separada. Dado que Azure AD Connect no soporta su uso con la base de datos SQL de Microsoft Azure, la empresa necesitará un SQL Server local con licencia completa. Este requisito no solo genera costos de licencia, sino costos relacionados con el hardware y el mantenimiento continuo de SQL Server. Por lo tanto, las empresas que deseen usar Azure AD pueden obtener ahorros importantes en los costos al limitar la cantidad de objetos de Active Directory.

Determinar la cantidad de objetos en AD

Determinar la cantidad de objetos almacenados en un Active Directory es relativamente sencillo. Solo tiene que usar Get-ADObject PowerShell cmdlet y especificar el nombre del dominio que desea examinar. Por ejemplo, para contar la cantidad de objetos almacenados en el dominio Contoso.com, usaría el siguiente comando:

```
Get-ADObject -Filter {name -like '*'}
-Searchbase 'CN=Schema,
CN=Configuration,DC=Contoso,DC=COM'
-ResultSetSize $null | Measure-Object
```

Previo a la migración, las soluciones de terceros pueden ofrecer incluso una evaluación más integral de su infraestructura actual, incluidos Active Directory, Windows Server y también SQL Server. Por ejemplo, Enterprise Reporter for Active Directory de Quest ofrece visibilidad completa de las cuentas de Active Directory, incluso la capacidad para determinar cuáles están inactivas o deshabilitadas. Esta solución le permite determinar fácilmente cuántos grupos existen y si hay algún grupo duplicado o vacío que tal vez no necesite migrar.

Con frecuencia, los administradores se sorprenden al descubrir la cantidad de objetos que existen realmente en un Active Directory. Por ejemplo, una pequeña y mediana empresa con solo diez empleados puede tener, fácilmente, 5000 o más objetos en su Active Directory.

Evaluar el estado de su Active Directory

Como se mencionó anteriormente, las bases de datos de Active Directory pueden experimentar problemas relacionados con la integridad de las bases de datos. Si bien las operaciones diarias podrían no revelar nunca síntomas de daño leve en Active Directory, estos problemas pueden hacer que la sincronización del directorio en la nube falle. Por lo tanto, antes de usar Azure AD Connect, es importante tomar medidas para comprobar el estado de Active Directory.

Como hemos visto, la herramienta nativa NTDSUTIL de Microsoft puede verificar la suma de comprobación de la base de datos de Active Directory y realizar diversas comprobaciones de la integridad de la base de datos, pero las herramientas de terceros, como Active Administrator for Active Directory Health de Quest, con frecuencia ofrecen mejores resultados con mucho menos esfuerzo.

CONCLUSIÓN

Windows Server 2016 incluye diversas mejoras para Active Directory y servicios relacionados con el directorio, como DNS e IPAM. Aunque Microsoft ofrece una ruta de actualización para Active Directory, sus recomendaciones están basadas en la suposición de que el entorno existente de Active Directory se encuentra en estado óptimo y adecuado. El intento de actualizar un Active Directory en mal estado a una versión nueva de Windows puede ser la causa de problemas graves, como así también el intento de extender un Active Directory incorrecto a la nube. Esto es muy preocupante, puesto que el daño en Active Directory no siempre genera síntomas visibles.

Por consiguiente, antes de actualizar los controladores de dominio a Windows Server 2016, es conveniente que pruebe de manera exhaustiva su Active Directory y optimice su estado. Realice un inventario de los controladores de dominio, compruebe la integridad de la base de datos de AD y elimine los objetos huérfanos. Además, observe objetivamente la topología actual de su Active Directory y determine si sería conveniente realizar una reestructuración. Finalmente, realice una planificación cuidadosa para reducir el impacto de la migración en la empresa.

Las soluciones de terceros pueden ayudarlo a limpiar y reestructurar mejor su Active Directory y con mucho menor esfuerzo que con las herramientas nativas.

INFORMACIÓN SOBRE QUEST

Quest ayuda a nuestros clientes con la reducción de las tediosas tareas de administración para que usted pueda centrarse en la innovación necesaria para que su empresa crezca. Las soluciones de Quest® son escalables, rentables y simples de usar, y proporcionan eficiencia y productividad inigualables. Además de la invitación de Quest hecha a la comunidad global para participar en esta innovación y de nuestro firme compromiso para garantizar la satisfacción del cliente, Quest continuará con la aceleración de la entrega de las soluciones más integrales para la administración de la nube de Azure, SaaS, seguridad, movilidad de la fuerza de trabajo e información impulsada por datos.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Visite nuestro sitio web (www.quest.com) para obtener información sobre nuestras oficinas regionales e internacionales.