Cómo optimizar su AD para Windows Server 2016

Escrito por Ron Robbins, gerente sénior de productos, Quest

INTRODUCCIÓN

Con el lanzamiento de Microsoft Windows Server 2016, muchas empresas comenzaron a evaluar los beneficios y desafíos de hacer la transición a la nueva plataforma. 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. Mientras que los contenedores de Windows Server y Nano Server han recibido mayor prensa hasta ahora, Microsoft también ha realizado varias mejoras en Active Directory (AD).

Si bien puede ser tentador apresurarse para implementar algunas de estas funcionalidades 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 de Windows y tomarán medidas para minimizar el impacto de la migración en la empresa. Pero también deberá examinar su infraestructura existente y considerar las necesidades de su empresa en el futuro, de modo que pueda utilizar la migración como una oportunidad para establecer un entorno de Windows Server 2016 que permita el crecimiento, ofrezca flexibilidad y garantice seguridad y cumplimiento.

Lea esta documentación técnica para conocer las nuevas funciones de Windows Server 2016, las consideraciones clave para migrar de plataformas heredadas y optimizar su Active Directory, y el modo en que Quest puede ayudarlo a prepararse para la migración, a migrar de manera eficiente y a administrar su nuevo entorno de manera eficaz.

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 a un usuario o 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.

Su migración a Windows Server 2016 es una oportunidad para establecer un entorno flexible, escalable, seguro y compatible que soporte e incluso impulse a su empresa.

Servicios 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 acceda 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 funcionalidad 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, entre las que se incluyen:

- **Políticas del DNS**: Una de las nuevas funcionalidades más significativas es la capacidad 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 funcionalidades 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.

CONSIDERACIONES DE LA MIGRACIÓN

Por supuesto que migrar a Windows Server 2016 desde versión anterior u otra plataforma de servidor requiere una planificación cuidadosa. Un objetivo importante debe ser minimizar el impacto de la migración en la empresa. Pero también debe utilizar la migración como una oportunidad para establecer un entorno flexible, escalable, seguro y compatible que soporte e incluso impulse a su empresa.

Análisis de su entorno existente

Uno de los errores más grandes que puede cometer es lanzarse a una migración importante sin revisar completamente sus entornos existentes. Su evaluación previa a la migración debe estar dirigida a los usuarios, las aplicaciones, las listas de distribución, los grupos, las carpetas públicas y, por supuesto, Active Directory. Antes de realizar la migración, es fundamental identificar todos los flujos de trabajo, las casillas de correo, los programas y otras partes de la infraestructura que puedan resultar afectados. En particular:

- Debe comprender totalmente aquello que se debe migrar y aquello que no. Por ejemplo, debe asegurarse de migrar almacenes de datos, casillas de correo y usuarios activos, pero no debe perder tiempo y recursos en cuentas que no se utilizan, datos obsoletos y casillas de correo vacías.
- Además deberá realizar un análisis de todas las aplicaciones, los procesos y los usuarios que requieren acceso. Así garantizará que los recursos y las aplicaciones adecuadas estén disponibles durantela migración y después de ella.

Mejora de la seguridad y el cumplimiento de AD

Otra área de consideración de migración crítica es la seguridad y la delegación, es decir, controlar quiénes pueden realizar cambios en los objetos de AD de Windows y sus propiedades. Muy a menudo, las empresas conceden un excesivo acceso a los objetos de AD para solucionar un problema inmediato y no eliminan correctamente esos permisos,. Asegúrese de implementar los controles adecuados para administrar el acceso a AD y quiénes pueden cambiarlo.

También deberá monitorear continuamente qué actividades se realizan en AD para cumplir con los requisitos internos y las normas externas. Mientras que Microsoft Windows Server y AD tienen de manera nativa la habilidad de auditar eventos realizados con ellos, estos eventos de auditoría nativos pueden ser muy detallados, recorrerse con rapidez en entornos congestionados y carecer de sentido si se los considera individualmente a su valor nominal. Por lo tanto, contar con una capacidad de análisis y agregación de auditoría de AD coherente es crítica para localizar cambios inadecuados en AD, detectar el uso no autorizado de recursos corporativos y AD, realizar un seguimiento de la actividad del usuario en todos los sistemas del área de TI y demostrar el cumplimiento a los auditores.

Garantía de compatibilidad de aplicaciones

Considere postergar la migración hasta que las aplicaciones de terceros de las cuales depende su empresa estén certificadas para funcionar con Windows Server 2016. Además deberá probar todas las aplicaciones internas críticas para asegurarse de que funcionarán correctamente en el nuevo entorno.

Impacto minimizado en la empresa

Por supuesto, la compatibilidad de aplicaciones es solo un factor para minimizar el impacto de la migración en la empresa. También deberá hacerse esta pregunta crítica: ¿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 puntos de acceso. Puede evitar muchos de 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 y la productividad.

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

Aprovechamiento de la oportunidad de reestructurar su AD

La migración a Windows Server 2016 no debe ser una tarea rutinaria simplemente: es también una oportunidad para reestructurar su Active Directory, a fin de satisfacer mejor sus necesidades actuales y futuras. Muchas empresas implementaron por primera vez Active Directory en Windows Server en 1999 o 2000, y la topología de AD aún se parece bastante. Sin embargo, muy probablemente

La coexistencia es esencial en cualquier migración de AD porque los usuarios necesitan mantener el acceso a los recursos que los mantienen productivos.

el modelo comercial y las necesidades de su empresa hayan cambiado bastante desde que adoptó AD, y su infraestructura del área de TI haya evolucionado debido a fusiones, adquisiciones, reestructuración, crecimiento y la disponibilidad de nuevas tecnologías.

Considere cuántos dominios y cuántos bosques necesita ahora. Puede descubrir que debe consolidar algunos bosques o mantener partes nuevas de la infraestructura para las oficinas remotas que no existían cuando implementó originalmente Active Directory.

CÓMO PUEDE AYUDAR QUEST

Quest ofrece soluciones que lo ayudarán a planificar y ejecutar una reestructuración o consolidación eficiente de AD a medida que migra a Windows Server 2016, y luego a asegurar y administrar eficazmente su nuevo entorno.

PREPARACIÓN

- **Evaluación de su entorno actual**: Enterprise Reporter le ofrece una evaluación integral previa a la migración de su infraestructura actual, incluidos Active Directory, Windows Server y también SQL Server. Por ejemplo, pueden informar la cantidad de cuentas en su Active Directory y ver cuáles están inactivas o deshabilitadas. De manera similar, puede determinar fácilmente cuántos grupos posee, si hay algún grupo duplicado o si hay grupos vacíos que tal vez no necesite migrar. Como vimos anteriormente, comprender su entorno actual y realizar una limpieza antes de la migración permitirá que Windows Server 2016 sea más seguro y fácil de administrar.
- **Descubra las consultas sobre AD y LDAP**: Change Auditor para consultas de Active Directory identifica y realiza un inventario de los servidores de la aplicación que dependen de los dominios de AD que se migrarán, de modo que pueda resolverlos o redirigirlos a los nuevos controladores de dominio.

MIGRACIÓN, CONSOLIDACIÓN Y REESTRUCTURACIÓN

- **Consolidación y reestructuración de Active Directory**: Migration Manager for Active Directory ofrece una reestructuración y consolidación sin afectar a Active Directory (ZeroIMPACT). Migration Manager proporciona una coexistencia sin interrupciones: Tanto los usuarios que hayan migrado como aquellos que aún no lo hayan hecho mantienen un acceso seguro a las workstations, los recursos y el correo electrónico a lo largo de todo el proyecto.
- **Migración de datos de Windows Server**: Secure Copy es una solución automatizada para migrar y reestructurar rápidamente los datos archivados en el servidor. Todos los puntos de seguridad y acceso a los datos se mantendrán a medida que se migren los datos. Las sólidas herramientas de informes permiten que sea la herramienta perfecta para planificar y verificar una migración exitosa de los datos archivados en el servidor de Windows.
- **Migración de Novell eDirectory a Microsoft Active Directory**: Migrator for NDS ayuda a las empresas a realizar la transición de Novell eDirectory a Active Directory. Además del directorio, la herramienta también migra todos los datos que se encuentran en Novell y vuelve a enviar el permiso a las nuevas identidades de Active Directory de los usuarios medida que migra los datos.

SEGURIDAD Y CUMPLIMIENTO

- **Control de cambio y auditoría**: Change Auditor para Active Directory le brinda un registro completo de auditoría de todo lo que se haya cambiado en Active Directory, incluidas las cinco preguntas: quién realizó el cambio, cuál fue el cambio, cuáles fueron los valores antes y después, dónde ocurrió el cambio y de qué workstation provino el cambio. Esta información granular es valiosa para la solución de problemas. Por ejemplo, si tiene problemas para la replicación y llama a Microsoft, lo primero que preguntarán es: "¿qué ha cambiado?" Con Change Auditor, sabrá exactamente cómo responder. Además, Change Auditor puede evitar cambios en primer lugar. Por ejemplo, puede rechazar la eliminación de unidades organizativas (UO) importantes y la modificación de ajustes de la política grupal.
- **Control de acceso**: Roles activos ayuda a garantizar la seguridad y el cumplimiento al permitirle controlar el acceso a través de la delegación con un modelo de privilegios mínimos. Puede generar y reforzar estrictamente las reglas de acceso basadas en políticas y permisos administrativos definidos; por ejemplo, puede especificar quienes pueden modificar la membresía de grupo o cambiar la política grupal. Roles activos también automatiza la creación de usuarios, grupos y casillas de correo, y cambia o elimina automáticamente los derechos de acceso basados en los cambios de roles.

Al garantizar que los usuarios tengan el mismo acceso a los recursos luego de la migración, Migration Manager promueve la seguridad y el cumplimiento en su nuevo entorno de Windows Server 2016.

- **Administración centralizada de permisos**: Security Explorer mejora la administración del Control de acceso dinámico (DAC) de Microsoft al permitir a los administradores agregar, eliminar, modificar, respaldar, restaurar, y copiar y pegar permisos que incluyan expresiones condicionales desde una única consola. Puede realizar cambios específicos o en bloque en los permisos del servidor y aprovechar las funciones mejoradas de administración de DAC, como la capacidad de otorgar, revocar, modificar y clonar permisos, buscar permisos, recuperar permisos aplicados incorrectamente e informar permisos.
- **Monitoreo de actividad de usuarios**: InTrust le permite recopilar, almacenar e informar y alertar de forma segura sobre datos de registro de eventos para garantizar el cumplimiento de las normas externas, políticas internas y mejores prácticas de seguridad. InTrust ofrece información sobre la actividad del usuario al auditar el acceso de este a los sistemas críticos desde el inicio de sesión hasta el cierre de sesión. Además le permite detectar eventos inadecuados o sospechosos relacionados con el acceso en tiempo real. Por ejemplo, InTrust puede saber que un usuario determinado generalmente inicia sesión a un horario determinado desde una ubicación determinada, y alertarlo si hay un intento de inicio de sesión desde cuenta desde una ubicación remota o en un horario inusual, cualquiera de los cuales podría ser una amenaza de seguridad.

ADMINISTRACIÓN Y RECUPERACIÓN

- **Administración de Active Directory**: La política grupal puede ser una manera excelente de controlar el acceso y bloquear su infraestructura, pero si no se administra correctamente, los objetos de política grupal (GPO) también pueden ser la causa de muchos daños. Por ejemplo, si posee un GPO que define los ajustes de proxy para acceder a Internet, pero están configurados de manera incorrecta, es posible que los usuarios tengan problemas para acceder a los recursos que necesitan. GPOADmin automatiza las tareas de administración de la política grupal y proporciona un flujo de trabajo que garantiza que los cambios se registren y aprueben antes de comenzar la producción de GPO, lo cual reduce el esfuerzo de administración y aumenta la seguridad. Además puede comprobar y comparar las versiones de los GPO con el transcurso del tiempo para confirmar la coherencia de sus ajustes de GPO.
- **Recuperación de datos de Active Directory**: Active Directory es fundamental para las operaciones comerciales, de modo que las empresas deben ser capaces de recuperar rápidamente los elementos individuales que se hayan cambiado o eliminado de manera accidental o incorrecta. Recovery Manager for Active Directory permite esa recuperación granular. Por ejemplo, si un usuario o grupo se eliminó de manera accidental o un GPO se cambió de manera incorrecta, Recovery Manager for Active Directory puede comparar rápidamente el estado actual y activo de Active Directory para respaldar e informar sobre las diferencias, y restaurar el objeto que se cambió.
- **Recuperación ante desastres**: Además de la recuperación granular, las empresas también necesitan la recuperación ante desastres. Si pierde un dominio o se daña todo un bosque, Recovery Manager for Active Directory Forest Edition puede recuperarlo de manera fácil y rápida.

CONCLUSIÓN

Windows Server 2016 ofrece una gran cantidad de funciones y mejoras nuevas diseñadas para mejorar la seguridad, optimizar la administración y facilitar una mejor experiencia del usuario. Para garantizar una transición exitosa, es crítico planificar cuidadosamente el proceso de consolidación de AD, aprovechar las oportunidades que ofrece y prepararse para administrar su nuevo entorno eficazmente. Las herramientas de Quest lo ayudarán en cada paso del proceso, de modo que pueda ofrecer un entorno flexible y seguro de Windows Server 2016 y AD que posicione su empresa para el futuro.

ACERCA DEL AUTOR

Ron Robbins es gerente sénior de productos de Quest, en donde es responsable de orientar la dirección de las soluciones de migración de Quest para mensajería y Active Directory, y brinda asistencia a los clientes y socios estratégicos. Con más de 15 años de experiencia en el área de TI, Ron ha sido autor de varias documentaciones técnicas y artículos sobre la migración y administración de Exchange. Antes de unirse a Quest, Ron brindó servicios de soporte del área de TI y consultoría a varias empresas diferentes, incluidas las empresas de Fortune 500. Ron tiene una licenciatura de Mount Vernon Nazarene University.

Las soluciones de Quest lo ayudarán a planificar y ejecutar una migración eficiente a Windows Server 2016, y luego a asegurar y administrar eficazmente su nuevo entorno.

ACERCA DE QUEST®

Quest ayuda a nuestros clientes a reducir las tediosas tareas de administración a fin de que usted pueda centrarse en la innovación necesaria para que su empresa crezca. Las soluciones de Quest son escalables, asequibles 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 del personal 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.