Modernización de Active Directory para Azure y Office 365

Pautas para una implementación de Office 365 sin problemas con Azure Active Directory

Escrito por Darren Mar-Elia, presidente y director de Tecnología de SDM Software y Microsoft MVP

INTRODUCCIÓN

En medianas y grandes empresas, los servicios en la nube de Microsoft están tomando velocidad. Los productos basados en la nube como Office 365 son atractivos si usted es un gerente del área de TI que preferiría administrar servicios (Active Directory, Exchange Online, Lync Online, SharePoint Online, OneDrive y otros) en lugar de servidores.

Microsoft hace que la transición sea fácil al ofrecer herramientas gratuitas, en especial para migrar o integrar desde su AD en las instalaciones a AD de Azure. De hecho, puede que sea demasiado fácil si usted comenzó a comprar las licencias y a migrar recursos a la nube antes de organizar el trabajo preliminar para una transición sin problemas. Mientras que las herramientas pueden ayudarlo a tener éxito en dejar atrás el hardware, inadvertidamente, quizás también migre años de desorden y datos obsoletos a su nuevo entorno en la nube.

AD de Azure está diseñado para aprovechar al máximo los servicios en la nube de Microsoft, como Office 365, y para ayudar a las empresas a dar vuelta la página en la autenticación de usuarios. Cuando esté sincronizando con la nube desde un AD interno que ya organizó, administró y limpió (es decir, modernizó), su AD de Azure le servirá a usted y a su estrategia en la nube de manera más eficiente.

Mediante esta documentación se enfatiza la importancia de modernizar el AD de su empresa antes de migrar de Azure y de Office 365. Ofrece perspectivas sobre cómo modernizar e integrar su AD en las instalaciones en Azure, de manera que pueda disfrutar de menos administración en el hardware y el software de las instalaciones y presentar su empresa a la identidad como un servicio.

REEVALUACIÓN DE SU ACTIVE DIRECTORY

El apuro por adoptar Office 365 está en marcha, con una cantidad de puestos comerciales en uso de Office 365 que prácticamente duplica los de 2013 a 2014[1].

Puesto que AD de Azure es el servicio de autenticación de usuarios basado en la nube que utiliza Office 365, ese apuro puede tomarlo por sorpresa. Antes de pasar la empresa a Office 365, primero asegúrese de tener su casa de AD en orden. AD y AD de Azure juegan un rol prominente a la hora de adoptar con éxito los servicios en la nube de Microsoft. Para disfrutar de los costos más bajos de hardware, software y mantenimiento que su estrategia en la nube promete, primero tiene que pensar en su AD interno, luego en AD

[1] Paul Rubens, "Microsoft Office 365 Adoption Takes Off, War With Google Apps Rages On" (Copias de adopción de Microsoft Office 365, la guerra con Google Apps se propaga), CIO.com, 22 de enero de 2015

Antes de pasar la empresa a Office 365, primero asegúrese de tener su casa de AD en orden.

de Azure y luego en los servicios como Office 365.

Puede que esa sea una nueva mentalidad en su empresa, sobretodo si depende de AD para cosas esenciales, como la autenticación y la autorización de usuarios, el acceso al servidor de archivos, las aplicaciones y la infraestructura. Pero con una tecnología como la de AD cuyo tamaño y complejidad han crecido de manera constante en muchas empresas desde 1999, vale la pena prestar atención a la recomendación de Microsoft de pasar a la nube con un AD económico:

"Microsoft cree que es un buen momento para modernizar su infraestructura, ya que han habido grandes avances en la tecnología durante la última década que pueden traer beneficios significativos al área de TI y al valor empresarial. Es importante y necesario tener un entorno de AD limpio y optimizado cuando se aprovechan todos los beneficios de tecnologías, como la de Office 365 y otras aplicaciones e infraestructuras basadas en la nube. La modernización es especialmente importante para aquellos que pasan de Windows Server 2012, ya que su implementación exitosa requiere de un Active Directory limpio y administrable". Mark Linton, gerente general de OEM Product Management Group, Microsoft.

Considere algunos de los factores que pueden afectar el estado de AD y la migración a AD de Azure:

- Las tiendas del área de TI que han utilizado AD desde su infancia y han crecido orgánicamente con él pueden haber adoptado maneras no tan óptimas de organizar AD. Es posible que aún cuenten con procesos heredados en torno a quién está creando, editando y eliminando objetos y dónde se crean esos objetos.
- Las prácticas comúnmente aceptadas solían incluir la creación de un dominio de AD raíz sin recursos. Si siguiera y mantuviera esa práctica, podría tener un impacto sustancial en su transición al mundo de Office 365.
- Microsoft solía recomendar el uso del dominio como el límite de seguridad para aislar recursos en Active Directory, y luego cambió su consejo a favor de utilizar el bosque. Algunos administradores comenzaron a crear múltiples bosques, que ahora tal vez quieran reorganizar o consolidar antes de integrarlos en AD de Azure y Office 365, ya que integrar múltiples bosques en AD de Azure crea varias complejidades que pueden prolongar sustancialmente la implementación.
- Las empresas que enfrentan requisitos gubernamentales o normativos puede que deban ser selectivas en los objetos que sincronizan entre su AD interno y AD de Azure, para asegurar el cumplimiento constante. Esto puede ser difícil si su AD interno está "desorganizado" o caracterizado por objetos regulados que están mezclados con objetos no regulados.

En consecuencia, la transición a Office 365 establece las bases para modernizar AD[2].

LOS CUATRO ASPECTOS BÁSICOS DE LA MODERNIZACIÓN DE ACTIVE DIRECTORY

La modernización de AD es el proceso de tomar una mirada nueva de su organización y mantenimiento. Una estructura AD modernizada facilita ejecutar Office 365 y AD de Azure en cuatro áreas en particular:

1. Estructura normalizada

En general, menos dominios y bosques es mejor. Normalizar el AD significa reducir la cantidad de bosques y los límites de seguridad que representan tanto como sea posible. Las empresas inteligentes administran su acceso y privilegios sistemáticamente a través de una implementación de AD, y tienen bien controlados a los grupos que representan esos accesos, y organizados por funciones comerciales.

2. UO consolidadas y limpias

Uno de los mayores obstáculos para implementar Office 365 sin problemas es una estructura de unidad organizativa (UO) dispersa. Si concede acceso a casillas de correo y recursos de SharePoint basado en los grupos, cuyos objetos existen en muchos árboles o jerarquías distintas dentro de Active Directory, los problemas no se harán esperar.

AD de Azure sincroniza todos los contenedores en su AD de manera predeterminada (para clases de objetos específicos tales como usuarios, grupos y contactos) a menos que lo configure para sincronizar solo UO específicas. Eso significa que la UO es su nivel ideal de control como administrador, de modo que sirve consolidar asegurándose de que todos los objetos de usuario estén bajo una sola estructura de UO o una estructura anidada, por ejemplo.

[2] Para obtener más información sobre la reevaluación de su AD, consulte la documentación técnica de Quest "Modernizing Your Active Directory Environment" (Modernización de su entorno de Active Directory).

La mejor estructura de UO es la que se ajusta a su empresa, ya sea por una cuestión geográfica, de funciones o de unidad empresarial. Pero es importante evitar tener objetos de usuario desparramados por distintas jerarquías dentro de AD, lo cual es común en implementaciones de AD que se han extendido por mucho tiempo.

Supongamos que tenía objetos de usuario en tres estructuras distintas dentro de un solo dominio de AD en las instalaciones. Debería sincronizar esas tres UO a AD de Azure de manera separada, lo cual es una molestia, especialmente si esas UO también contienen objetos que no desea sincronizar (por ejemplo, cuentas de servicio de aplicaciones o grupos de seguridad). Lamentablemente, sería una molestia mayor sincronizar el dominio completo, con todas las cuentas de administración y servicio que no tienen ninguna relación con la ejecución de Office 365 en AD de Azure. La falta de una estructura de UO consolidada lo obligaría a dedicar tiempo y esfuerzo repetidamente filtrando lo que desea sincronizar, y su proceso se volvería más frágil cuando tuviera que mover objetos.

3. Buena delegación de seguridad y buena administración

En una estructura de UO sólida, sus grupos, usuarios y computadoras están bien delegados. En otras palabras, está bien asegurada, con el acceso a objetos concedido solo a las personas que lo necesitan. Mientras que no hay una correlación directa entre la estructura de AD interna y AD de Azure (AD de Azure no soporta el concepto de UO de hoy), hay un modelo de delegación dentro de AD de Azure, así que garantizarle que tiene una buena idea de "quién administra qué" lo ayudará a pasar la administración a AD de Azure. Además, AD de Azure está presentando el concepto de "unidades administrativas", que son una manera de delegación que le permite acordonar ciertos objetos para que subconjuntos de administradores los administren. Tener una estructura de delegación limpia en su AD interno puede ayudar a facilitar el aprovechamiento de estas construcciones de AD de Azure en el futuro.

4. Aprovisionamiento sólido y cancelación de aprovisionamiento

En teoría, conceder acceso a los usuarios cuando lo necesitan y quitarlo cuando ya no lo necesitan es perfecto. En la práctica, mantener ese proceso es más difícil.

Naturalmente, los usuarios asumen y cambian los roles en la empresa y necesitan acceso a distintos recursos durante su permanencia. Cuando se van, la empresa elimina su acceso. Si su empresa es rigurosa en aprovisionar, reaprovisionar y cancelar aprovisionamiento a los usuarios en AD local, disfrutará de beneficios similares con AD de Azure. Pero toma seis meses deshabilitar la cuenta del usuario en el AD local cuando un empleado renuncia, entonces pagará seis meses de tarifas por usuario para suscripciones de AD de Azure y Office 365 que nadie está utilizando.

LA IMPORTANCIA DE OFFICE 365

Una vez que su casa de AD esté en orden, puede prestarle atención a la pregunta de por qué Office 365 es importante. Los índices de adopción sugieren que muchas empresas ya se han contentado con una variedad de respuestas:

- **Costo**: El motivo más convincente es que ejecutar Office o productos como Exchange, Lync y SharePoint es costoso, en especial a escala. Los productos crecen en complejidad con cada lanzamiento, lo que motiva a muchas empresas a salir del negocio de mantener la infraestructura de soporte operativo.
- **Criticidad para la empresa**: La comunicación, la productividad y la colaboración personificada en los productos de Office es esencial, así que, en efecto, ahora requiere conocimiento administrativo especializado, alta disponibilidad y procesos del área de TI sólidos para mantener su empresa en ejecución. No todas las empresas tienen aquellos recursos o pueden costearlos.
- **Estado de lujo**: A menos que derive ingresos de lo destinado a servicios del área de TI y que mantenga la estructura en ejecución, aquellas funciones no son las más importantes en su empresa. Los objetivos de su empresa se lograrán mejor al comprar servicios y al permitir que Microsoft los provea.
- **Modelo financiero**: Incluso para las pequeñas y medianas empresas (SMB), Office 365 tiene el potencial de cambiar el modelo financiero para el área de TI. En lugar de invertir en grandes gastos de capital en hardware de back-end, red y en el monitoreo y la administración que van con ellos, las empresas pueden pasar a

AD de Azure sincroniza todos los contenedores (pero no todas las clases de objetos) con su AD a menos que lo configure para sincronizar solo UO específicas.

> Si le toma seis meses deshabilitar una cuenta de usuario innecesaria en su AD en las instalaciones, entonces pagará seis meses de tarifas por usuario para suscripciones que nadie está utilizando.

gastos operativos de un costo por usuario mensual.

- **Facilidad de transición**: Microsoft está facilitando la transición de servicios en las instalaciones a aquellos basados en la nube al ofrecer herramientas gratuitas, como OnRamp for Office 365, IDFix, Exchange Server Deployment Assistant y muchos otros kits de herramientas relacionados. Incluso los equipos más pequeños del área de TI tienen lo que necesitan para una migración exitosa.

Administrar servicios, no servidores

Sin embargo, para autenticar los usuarios de Office 365, aun tendrá que almacenar las identidades de usuarios en el AD de Azure, lo que significa sincronizar en las instalaciones de AD a la nube. Todavía necesitará tomar decisiones sobre contraseñas de sincronización o federación, basado en el tamaño de su empresa, sus preocupaciones de seguridad y su profundidad técnica.

Pero el proceso de toma de decisiones se reduce a administrar servicios o servidores.

OBTENER LA IDENTIDAD COMO UN SERVICIO CON EL AD DE AZURE

Entre los servicios más importantes que las empresas comenzarán a administrar está la identidad basada en la nube. En el contexto de Office 365, el AD de Azure representa este tipo de identidad como un servicio.

¿En qué difiere el AD de Azure del AD local?

Mientras que algunos servicios en la nube simplemente replican las funciones de las aplicaciones en las instalaciones, el AD de Azure es un servicio de múltiples arrendatarios diseñado para soportar la administración de identidades y accesos. Está más estrechamente relacionado con los Active Directory Lightweight Directory Services (ADLDS) que con el AD local en términos de su estructura (si bien hoy no soporta una interfaz de LDAP), con muchas mejoras:

- El AD de Azure solo puede almacenar un subconjunto de las clases de objetos y los atributos asociados con los AD locales, como los objetos de usuario, los contratos, los grupos y las membresías de grupo.
- En lugar de UO, el AD de Azure tiene unidades administrativas, cuyo objetivo es delegar objetos en un arrendatario del AD de Azure.
- Usted administra el AD de Azure con PowerShell o con RESTful Graph API, en lugar de con LDAP.
- El modelo de delegación del AD de Azure es mucho más simple que el AD regular, con tan solo algunos roles administrativos disponibles.
- El AD de Azure no soporta Kerberos ni la autenticación NTLM. Utiliza una autenticación simple si las contraseñas se mantienen en el arrendatario o, de no ser así, la autenticación federada se mantiene en su AD local.

El AD de Azure simplemente no es una controladora de dominio de AD que se ejecuta en la nube[3]. Se lo creó para la autenticación y la autorización del soporte de los servicios basados en la nube como Office 365 que buscan integrarse en una identidad de AD de Azure. En consecuencia, la identidad como un servicio.

Sincronización del AD local con el AD de Azure

Cuando aprovisiona una casilla de correo en Office 365, esta se asocia con un objeto de usuario del AD de Azure. Primero, sin embargo, su identidad del AD de Azure se asocia con su identidad de usuario en las instalaciones. Microsoft provee un par de mecanismos para integrar Office 365 en su AD de Azure o AD local, así que tiene algunas decisiones que tomar.

Para poblar (o aprovisionar) el AD de Azure debe sincronizarlo con los usuarios, los contactos y los grupos de AD locales. Microsoft provee herramientas de sincronización gratuitas, como DirSync; su sucesor Azure AD Sync Services; y pronto, una nueva oferta llamada Azure AD Connect que es incluso más liviana.

- ¿Gratuito, básico o premium? — Microsoft ofrece tres ediciones diferentes de AD de Azure[4]:
  - La gratuita ofrece administración de usuario y de grupo, admite hasta 500.000 objetos de directorio y abarca los primeros pasos hacia la integración de identidades en AD de Azure. Si simplemente está intentando tener Office 365 en funcionamiento,

[3] Observe que esto es posible en una red privada virtual entre las controladoras de dominio y las máquinas virtuales que se ejecutan en AD en Azure. Sin embargo, el resultado no es el mismo que el que brinda AD de Azure.

[4] Para obtener una comparación detallada de las ediciones gratuitas, básicas y de primera calidad de Azure Active Directory, visite http://azure.microsoft.com/en-us/pricing/details/active-directory/.

puede utilizar la edición gratuita y la sincronización unidireccional o bidireccional para integrar todos sus usuarios y grupos en el AD de Azure.

  - La básica agrega la administración de acceso basada en grupos, el restablecimiento de contraseñas de autoservicio para aplicaciones en la nube y un entorno personalizable para lanzar aplicaciones.
  - La premium agrega características de protección como la autenticación multifactor, características de administración de dispositivos móviles y un inicio de sesión único basado en grupos para miles de aplicaciones SaaS.

- ¿Unidireccional o bidireccional? — La sincronización unidireccional empuja las actualizaciones solo de su AD local al AD de Azure. Alternativamente, la sincronización bidireccional (disponible en todas las ediciones) permite aplicaciones de autoservicio como el restablecimiento de contraseñas y la administración de grupo para ejecutarla en la nube de AD y escribir los cambios en el AD de Azure, que luego se escriben en el AD local.

- ¿Autenticación local o en el AD de Azure? Cuando inicia sesión en un servicio en la nube como Outlook Web App en Office 365, debe ingresar las credenciales (nombre de usuario y contraseña) del AD local. Existen dos maneras de hacerlo, según sus requisitos de seguridad:
  - Sincronización de contraseñas de AD local para cuentas de usuario que utilizan Azure AD Sync Services o Azure AD Connect y validan la contraseña en el AD de Azure. Esta opción es preferible para pequeñas o medianas tiendas del área de TI.
  - Valide la contraseña con el AD local. Esta opción es más apropiada para empresas. Una configuración de muestra podría incluir una relación SAML o WS-Trust entre software como AD Federation Services (ADFS) que se ejecuta localmente y AD de Azure que se ejecuta en la nube. Una vez configurada, el proceso de inicio de sesión pasará sus credenciales de manera transparente de las instalaciones al arrendatario Office 365 sin acciones especiales de su parte.

Una vez en el AD de Azure, las posibilidades se amplían

Una vez que sincronizó su AD local modernizado con AD de Azure, puede aprovechar otros servicios Microsoft Azure relacionados con la identidad:

- Inicio de sesión único (SSO) en la nube: En lugar de tener que ejecutar sus servicios de federación en las instalaciones, puede federar en la nube. Las relaciones de Microsoft con los proveedores de SaaS, como Salesforce y Workday le permiten realizar todas las autenticaciones y autorizaciones en el AD de Azure.

- Autenticación multifactor (MFA): De manera similar, puede agregar MFA a sus identidades en la nube en lugar de implementarlas en las instalaciones.

- Acceso a Office 365 ProPlus: Muchas empresas se han suscripto a Office 365 ProPlus para el acceso a la nube tanto de versiones móviles como de equipos de escritorio de aplicaciones, como Word, Excel, Outlook y PowerPoint. Activar aquellas aplicaciones requiere credenciales en el AD de Azure.

- Administración de identidades basadas en la nube: Lo más importante es que las ventajas de la administración de identidades basada en la nube comience a estar dentro del alcance del AD de Azure. En lugar de tener que aprovisionar y cancelar el aprovisionamiento de identidades en las instalaciones, puede utilizar las herramientas en el AD de Azure (en especial, la edición Premium) para la administración de autoservicio de contraseñas y grupos, y utilice el Graph API para aprovisionar y cancelar el aprovisionamiento de objetos de manera programática. Eso prepara el camino para la identidad como un servicio.

La modernización de AD es el primer paso

La integración del AD de Azure no es un proceso que se hace de la noche a la mañana. Incluso mientras comience a aprovisionar el AD de Azure, su AD local continuará siendo su anclaje en las actividades diarias, como unir los equipos al dominio, administrar Group Policy y autenticar usuarios de aplicaciones en las instalaciones para el futuro previsible.

Tener ambos pies bien asentados en los dos mundos requiere un AD local modernizado y bien administrado porque gran parte de lo que aquí se hace también llega al AD de Azure. Cuando los objetos no utilizados se sincronizan con el AD de Azure, pueden llevar a la confusión, a accesos no autorizados a los recursos en la nube, a cambios innecesarios por usuario y a la pérdida de algunas ventajas de administración del AD por las que se designó a Azure.

En lugar de invertir en grandes gastos de capital en hardware de back-end, red y en el monitoreo y la administración que van con ellos, las empresas pueden pasar a gastos operativos de un costo por usuario mensual.

Antes de pasar la empresa a Office 365, primero asegúrese de tener su casa de AD en orden.

CONCLUSIÓN

Office 365 requiere de AD de Azure y un AD de Azure estable requiere un AD local modernizado, con una estructura normalizada, UO consolidadas, buena delegación de seguridad y un aprovisionamiento sólido. Si esta modernización falla, las complejidades de integrarlo en el AD de Azure crecen y los beneficios de Office 365 se achican.

El movimiento de Microsoft a los servicios en la nube representa una oportunidad para independizarse del centro de datos y comenzar a ejecutar su back-end en la nube. A medida que reduce la cantidad de áreas que requieren conocimientos internos, se elimina a usted mismo de la infraestructura de administración empresarial y, en cambio, puede enfocarse en administrar servicios (en especial, la identidad como un servicio) para sus usuarios.

SU TURNO

Microsoft facilita evaluar el AD de Azure en microsoftazure.com. Con una cuenta Microsoft usted puede activar un servidor de sincronización desde el AD en las instalaciones al arrendador de AD de Azure que le permite crear usuarios y grupos. Explore los conceptos descritos en esta documentación y estime lo necesario para esta empresa.

Visite http://azure.microsoft.com/en-us/documentation para obtener documentación, videos, scripts de automatización y otros recursos.

ACERCA DEL AUTOR

Darren Mar-Elia es MVP de Microsoft además de presidente y director de Tecnología de SDM Software. Posee más de 30 años de experiencia en el desarrollo de software y del área de TI, incluida su labor como director de Tecnología para soluciones de administración de Windows en Quest.

Darren ha escrito o realizado contribuciones para muchos libros sobre administración de Windows y es editor colaborador de la revista Windows IT Pro. También creó el popular sitio web GPOGuy.com sobre Política de grupo y es un orador frecuente en conferencias sobre temas de infraestructura de Windows.

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.