CONTENT PROVIDED BY

July 2013 | Redmondmag.com

Redmond

THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

CLOUD READY

How Windows Azure Active Directory will change how IT authenticates users and devices.

1105 MEDIA

Extend Active Directory to the Cloud with Okta

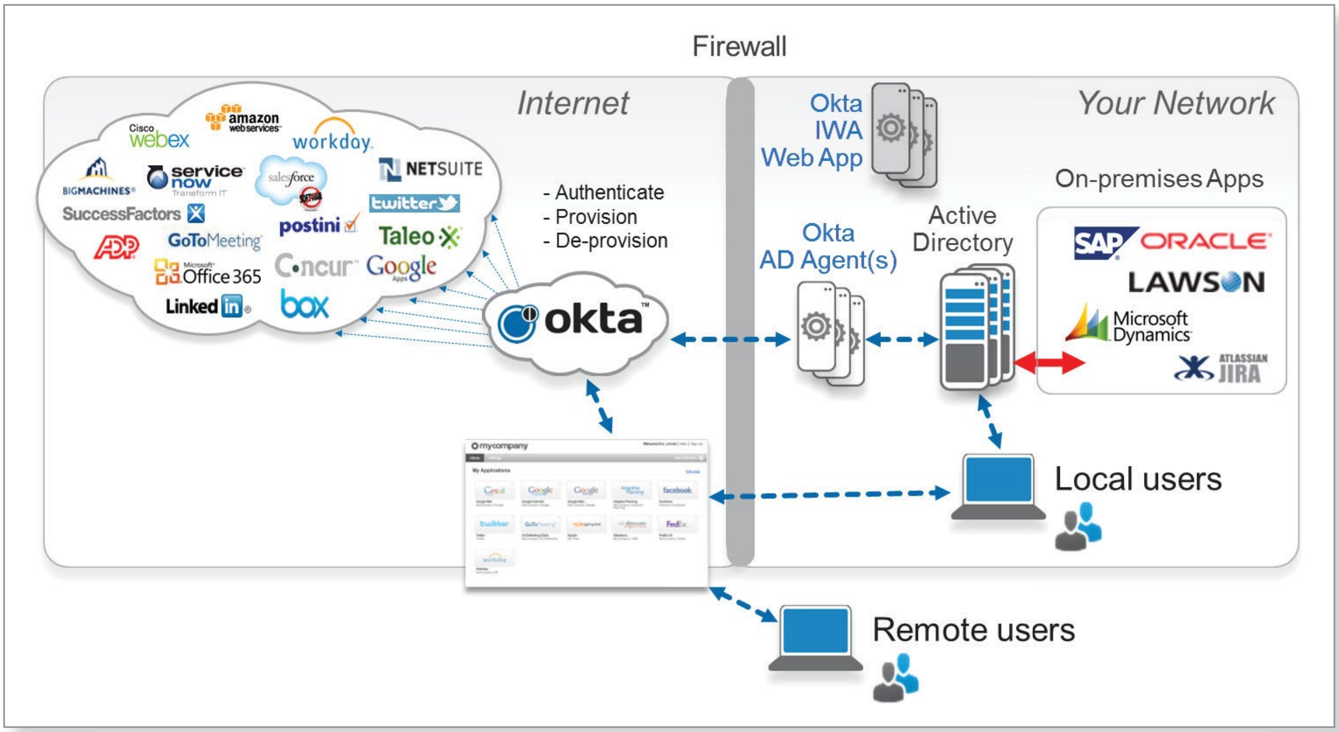
Simple, robust Active Directory driven single sign-on and user management for all your web applications

For most companies, Microsoft Active Directory (AD) plays the central role in coordinating identity and access management policies. AD typically serves as a "source of truth" for user identities, and it provides access control to on-premises resources such as networks, file servers, and web applications. A byproduct of the transition to cloud applications is the proliferation of separate user stores as each cloud application typically is rolled out independently and therefore has its own unique database of user credentials.

Okta's comprehensive identity management solution includes:

- A single integration point to manage all your users and apps
- Pre-built integrations for over 2,000 apps
- High availability
- Single sign-on (SSO) for cloud and on-prem web apps
- User management across apps

Visit **Okta.com/Free** to get started using Okta Cloud Connect and learn more about Okta's Active Directory integration. Learn how you can Okta eliminates the pitfalls that come with trying to build and manage multiple on-premises AD integrations yourself.



Visit Okta.com/Free for Okta Cloud Connect

okta
Enterprise Identity, Delivered

CLOUD IDENTITY

Windows Azure Active Directory bridges Microsoft single sign-on technology from the datacenter to the cloud.

BY JEFFREY SCHWARTZ

Just two months after releasing WAAD, Microsoft says it's already a success.

Over the past decade, enterprises of all sizes have standardized on Microsoft Active Directory for managing user identity and authentication and setting Group Policies. This is largely due to Microsoft's long-ago decision to bundle Active Directory with Windows. The ubiquity of Windows Server and Exchange, along with the robust Active Directory identity management infrastructure, have made Active Directory the choice of enterprise IT decision makers to securely front-end their networks. Now Microsoft is repeating that formula in the cloud with its new Windows Azure Active Directory (WAAD).

Released in April, anyone can provision a WAAD tenant for his organization running in Windows Azure by simply going to at **aka.ms/waadsignup** (for more on how to use WAAD, see "Provision Active Directory Online" on p. 6). Just like Microsoft provides Active Directory free with Windows Server, the company is offering WAAD at no charge to organizations using Windows Azure or Office 365 (which includes Exchange, SharePoint and Lync Online), as well as any of the company's other cloud offerings such as Windows Intune and Dynamics CRM Online.

Will enterprises take to WAAD as they did to Active Directory? That remains to be seen. It's not the only source of user-identity management—stakeholders ranging from Salesforce.com Inc. to Google Inc., Oracle Corp., Amazon Web Services Inc. and even Facebook, among others, have their eyes on managing user identities. But the installed base of Active Directory makes WAAD a strong contender, especially for Microsoft-based infrastructure, services and software.

Today 90 percent of *Redmond* magazine readers say Active Directory is their primary store for user identity and authentication. Remarkably, that number will rise to 94 percent over the next two years, according to 1,128 respondents in a recent readership survey.

"Pretty much everyone has got Active Directory," says independent consultant and speaker Mark Minasi, an expert in Windows infrastructure. "It really is *the* security infrastructure. It's like electricity or dial tone."

Just like the on-premises version, WAAD lets you manage user identities and control security access rights to apps and internal resources.

Billions Served

Just two months after releasing WAAD, Microsoft says it's already a success. Brad Anderson, corporate VP of the Microsoft Windows Server and System Center group, says WAAD has processed 265 billion authentication requests from around the world. It services more than 1 million authentication requests in a period of two minutes, or 9,000 per second. Customers have created more than 420,000 unique domains, according to Anderson, who talked up WAAD in his keynote address at the annual TechEd 2013 conference, held in New Orleans in June.

"Everything starts with the identity of that user inside of Active Directory," Anderson said. "We can extend your capabilities of Active Directory to the cloud with you in complete control about what you want to have appear inside that [Windows] Azure Active Directory."

The appeal of WAAD is it provides single sign-on (SSO) to or from the on-premises version of Windows Server Active Directory, according to Anderson. "Windows Azure Active Directory is really just extending your Active Directory out to the cloud," said Anderson, in an interview with *Redmond*.

While extending Active Directory to the cloud is a natural extension, it also was a much-needed upgrade for Windows Azure, especially now that the Infrastructure as a Service (IaaS) option is available. Rather than using the now-defunct Live ID (once called Passport but now referred to as simply a Microsoft account) to access Windows Azure, users can now authenticate with the same Active Directory credentials they have on-premises.

The WAAD Portal

When admins log in to the Windows Azure portal, it now has an Active Directory tab. Clicking that tab creates an enterprise directory, which prompts you to establish a domain name and create an Active Directory instance in Windows Azure. Just like the on-premises version, WAAD lets you manage user identities and control security access rights to apps and internal resources. It also lets you map the DNS to any domain.

WAAD evolved from the Access Control Service (ACS) in the Windows Azure AppFabric, a collection of components Microsoft has since decoupled. Because AppFabric (as a collection of services) is no more, Microsoft has shifted ACS to WAAD.

ACS effectively federates identities from external sources, notably on-premises Active Directory, but also external providers such as Google, Yahoo! and Facebook. Microsoft says other external providers are in the works.

"It's basically like Active Directory on-premises, except running out in the cloud," says Eric Boyd, a Windows Azure MVP and CEO of responsiveX, a consulting firm based in Chicago. "It's central to the Microsoft cloud services. Now, instead of using a Live ID for your Windows Azure management portal, you can create your Windows Azure subscription using the Windows Azure Active Directory store."

With the rapid growth of Office 365, that means IT can take Active Directory running in the datacenter and sync it to the cloud using a tool called DirSync, which populates the WAAD instance that also underlies Office 365. This enables a customer to use those identity objects from Active Directory for Windows Azure, versus creating a bunch of Windows Live ID accounts. With the latter option, administrators were unable to centrally manage those accounts from Active Directory.

> "Windows Azure Active Directory is really just extending your Active Directory out to the cloud."
>
> *Brad Anderson, Corporate VP, Microsoft Windows Server and System Center Group*

Graph API

"It's becoming a central identity component for Microsoft cloud services," Boyd says of WAAD. "Basically, as a developer, I can tap into that and do my own authentication against the Windows Azure Active Directory account; I can navigate the directory store using the REST-based Graph API. So if you're familiar with the Facebook Graph API, there's a Graph API for Windows Azure Active Directory as well, where I can navigate the hierarchy, or organizational structure, if you will."

The appeal of the Graph API in WAAD is it provides a queryable social graph that proponents say is much easier to work with than Lightweight Directory Access Protocol (LDAP), the Internet directory-access standard that all major directories support, including Active Directory.

"It's not nearly as complicated as working with LDAP and understanding what organizational units and domains and all that other stuff is," explained Michael Collier, a Windows Azure MVP and a principal cloud architect at Aditi Technologies, during a talk for developers at the recent Visual Studio Live! conference in Chicago (which, like *Redmond* magazine, is produced by 1105 Media Inc.).

"This is a very easy Graph–all REST-based–API, to walk through to get information about the user," Collier said. "You'll get that XML logic coming up as well. The nice thing about this is it's easy to access from any platform or device that you're working with. It doesn't have to be just Web applications, it can be Windows Store applications, mobile apps and anything that's REST-based."

"You can't join your machines in your domain to a Windows Azure Active Directory like you do an Active Directory on-premises."

Eric Boyd, CEO, responsiveX

While one of the attractive features in WAAD is that IT organizations can import identities from Windows Server Active Directory instances using DirSync, Microsoft doesn't pretend to suggest the two directories are identical. When running on-premises in Windows Server, Windows Server Active Directory includes Active Directory Domain Services (AD DS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS), Active Directory Certificate Services (AD CS) and Active Directory Rights Management Services (AD RMS).

Right now WAAD only offers ACS, the critical component for access control, which uses DirSync to connect to Windows Server Active Directory and external providers. "Windows Azure Active Directory doesn't have the ability to manage printers and devices and support Group Policy like Windows Server Active Directory," Collier noted. "It's more targeted around users, authentication and properties for those users."

Patrick Harding, CTO of Ping Identity Corp., believes over time WAAD will become a key method of cloud authentication. But Harding believes organizations will need third-party tools like his company's PingOne SSO cloud-based service, which has identity providers that connect to a wide swath of Software as a Service (SaaS) and enterprise software solutions.

"I think we're in for a significant period of time where Active Directory and WAAD will be working together, and they need to be synchronized," Harding says, adding that customers complain DirSync, while serviceable, has limitations. He explains: "Ping is focused on providing a robust directory-synchronization tool that can not only synchronize Active Directory with WAAD but with other cloud services as well. This is going to be quite important."

With the rapid growth of Office 365, that means IT can take Active Directory running in the datacenter and sync it to the cloud.

PingOne doesn't yet have connectors to WAAD, nor does another recently released tool, Centrify for SaaS & Apps from Centrify Corp.–though Centrify does plan to support it.

"We see there will be increasing usage of Windows Azure Active Directory over time," says Cory Williams, Centrify senior director of product management. Williams and others also point to the absence of a key feature offered in the on-premises-based version of Active Directory: Group Policy.

"You can't join your machines in your domain to a Windows Azure Active Directory like you do an Active Directory on-premises," says Boyd, of responsiveX. While his customers have indicated they'd like to see Group Policy in WAAD, Boyd is urging them not to expect it any time soon. "There are certainly challenges with doing that, if that's the only source of authentication for your company," he says.

Microsoft's Anderson is non-committal. "I see doing a much more light version of Group Policy, but right now we're delivering that through Windows Intune," he says. "So think about these things as all interrelated and things we're building on together. So as we think about [Windows] Azure Active Directory and Intune, we're doing common planning and engineering milestones across those two things." **R**

Jeffrey Schwartz is editor of Redmond *magazine.*

PROVISION ACTIVE DIRECTORY ONLINE

Learn how to connect your on-premises enterprise directory to the new Microsoft Windows Azure Infrastructure Services.

BY BRIEN M. POSEY

On the surface, the idea of extending your existing Active Directory forest to Windows Azure seems deceptively simple.

Although it's possible to use the new Windows Azure Infrastructure Services to build a datacenter that resides completely in the cloud, it's also well-suited to acting as an extension to your on-premises datacenter (or as a secondary datacenter). However, these types of deployments require special planning, especially when it comes to utilizing Active Directory for authentication and authorization.

Microsoft has offered Windows Azure since early 2010. But the April release of Windows Azure Infrastructure Services now allows IT to use the cloud service to deploy VMs and apps designed to run on Windows Server, including SQL Server, SharePoint, and other apps and infrastructure (see the June 2013 feature, "Deploy VMs in Windows Azure," for more on Windows Azure Infrastructure Services [**Redmondmag.com/Posey0613**]).

If you're planning to use Windows Azure as an extension of your datacenter, it makes sense to create a hybrid Active Directory forest in which domain controllers exist on-premises and in the cloud. The reason for this is many server applications require Active Directory access, and you really don't want apps running in the cloud to have to consult an on-premises DC every time they need to perform an operation. Not only is doing so inefficient, but a WAN failure could cause an app to malfunction due to its inability to contact an on-premises DC. As such, it's important to extend your Active Directory to the cloud. Windows Azure Infrastructure Services now lets you do that.

On the surface, the idea of extending your existing Active Directory forest to Windows Azure seems deceptively simple. After all, Windows Azure makes use of VMs running exactly the same Windows OSes that can be run on-premises. Besides, organizations routinely extend Active Directory forests to off-site datacenters all the time, so why should extending an Active Directory forest to a Windows Azure cloud be any different?

Creating a hybrid Active Directory by using a mixture of on-premises and cloud-based DCs is no different than building a multi-site Active Directory forest. As is the case with many things in IT, the devil is in the details.

Creating a hybrid Active Directory by using a mixture of on-premises and cloud-based DCs is no different than building a multi-site Active Directory forest.

Prerequisites to Deployment

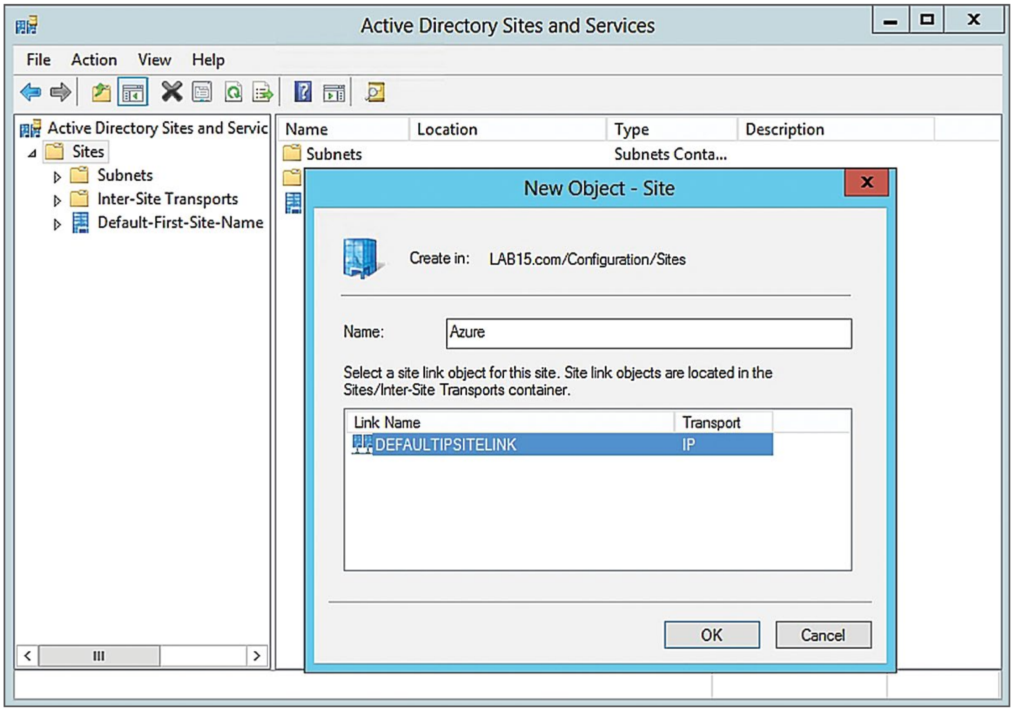
As I guide you through the process of extending your Active Directory to the cloud, I'll presume you already have an on-premises directory in place. I'll also assume you have a basic working knowledge of Active Directory and DNS.

Just as important, your on-premises network must include an externally accessible VPN server. You should provision this VPN server with a static IP address that's publicly accessible. It requires a VPN in order to establish connectivity between the servers that are hosted on Windows Azure and your on-premises servers.

Throughout the course of my deployment evaluation, I established a virtual network on Windows Azure, but this virtual network wasn't externally accessible. The easiest way to establish connectivity between the on-premises network and the Windows Azure virtual network is to make use of your on-premises VPN.

Set up a Hybrid Active Directory

The first step in the process is to open the Active Directory Sites and Services tool and create a new cloud site. To do so, right-click on the Sites container and choose the New Site command from the shortcut menu. When the New Object - Site dialog box appears, enter "Azure"



Create in: LAB15.com/Configuration/Sites

Name: Azure

Select a site link object for this site. Site link objects are located in the Sites/Inter-Site Transports container.

Link Name	Transport
DEFAULTIPSITELINK	IP

Figure 1. *Enter "Azure" as the name of the new site.*

The easiest way to establish connectivity between the on-premises network and the Windows Azure virtual network is to make use of your on-premises VPN.

as the site name, select the DEFAULTIPSITELINK and click OK (see **Figure 1**). Upon doing so, you should see a message indicating the new site has been created. Click OK to clear this message.

Build a replica DC on a VM running on top of Windows Azure. Set this up with the presumption that Windows Server is already installed on the replica DC and the replica DC has been assigned an IPv4 address. Make note of the address that you're using for your replica DC.

Go back to the on-premises DC and, from within the Active Directory Sites and Services console, right-click on the Subnets folder and choose the New Subnet command from the resulting shortcut menu. When the New-Object Subnet dialog box appears, enter the subnet in the Prefix dialog box. The prefix must be entered in Classless Inter-Domain Routing (CIDR) notation (for example, 157.54.208.0/20). Select the Azure site object before clicking OK.

So far you've configured the on-premises Active Directory forest to recognize a new site, but haven't yet established communication between the two sites. Furthermore, the cloud-based Active Directory components are dependent on DNS. Typically the on-premises DNS server used by Active Directory isn't externally accessible. This is a problem because the replica DC hosted on Windows Azure will need access to the on-premises DNS.

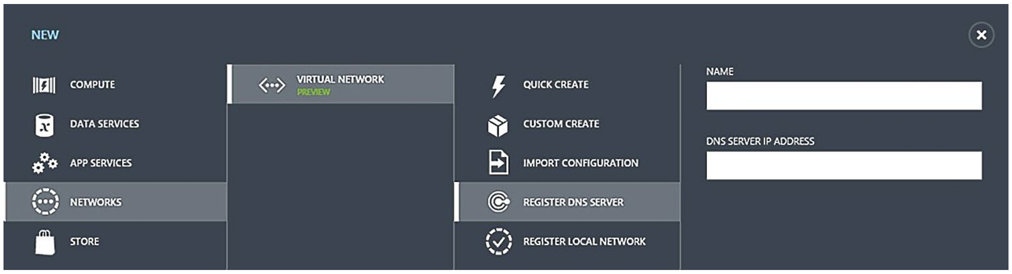


Figure 2. *You'll need to register your on-premises, Active Directory-integrated DNS server.*

The first step in making the server externally accessible is to register the on-premises Active Directory-integrated DNS server with Windows Azure. This allows you to associate the DNS server with the Windows Azure virtual network. To accomplish this, you can open the Windows Azure Management Portal and click on the Networks link found in the navigation pane. Then click the New button and select the Networks | Virtual Network | Register DNS Server options (see **Figure 2**). Enter the name of your on-premises DNS server into the name field and then enter the DNS server's IP address into the DNS Server IP Address field.

You're also going to need to register your DNS server with Windows Azure. Therefore, click the New button and navigate to Networks | Virtual Network | Register DNS Server. Now, enter the name and IP address that you'll use for your cloud-based DNS server.

Once you've registered the on-premises and the cloud-based DNS servers, the next task is to provide connectivity between the two networks.

Establish Connectivity

Once you've registered the on-premises and the cloud-based DNS servers, the next task is to provide connectivity between the two networks. This is done by establishing site-to-site VPN connectivity between the on-premises network and the Windows Azure virtual network.

From the Windows Azure Management Portal, click on the Networks link and then click on the New button. Next, click on Networks | Virtual Network | Custom Create. Windows Azure will launch the Create a Virtual Network Wizard. Enter a name for the virtual network and then select the appropriate affinity group.

At this point, you must click the arrow icon to move to the Address Space and Subnets page. Click on the CIDR button and then use the Add Address Space button (and, optionally, the Add Subnet button) to define the address space and any required subnets for the virtual network (Azure, which you named earlier).

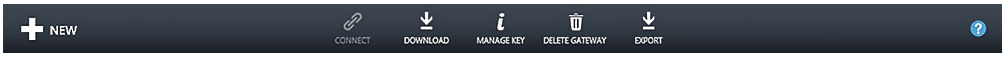


Figure 3. *The toolbar at the bottom of the screen contains a Manage Key and a Download button, both of which are useful during the configuration process.*

Click the arrow icon to move on to the next page, where you can define DNS servers and the local network. Here you must select your on-premises DNS server as the first DNS server and your cloud DNS server as the secondary DNS server. The interface doesn't explicitly list the DNS servers as primary and secondary. The only way to ensure that your on-premises DNS server is treated as the primary DNS is to select it first.

After specifying your DNS servers, select the Configure a Connection to the Local Network checkbox. Upon doing so, you must use the Gateway Subnet field to enter the gateway subnet for the on-premises network. You must enter this subnet using CIDR notation.

Click the arrow icon and you'll land on the Specify a New Local Network page. You must now enter a name, VPN device IP address, and address space for your local network. Once again, the address space must be entered in CIDR format. Once you've finished entering your address space details, click the checkmark icon.

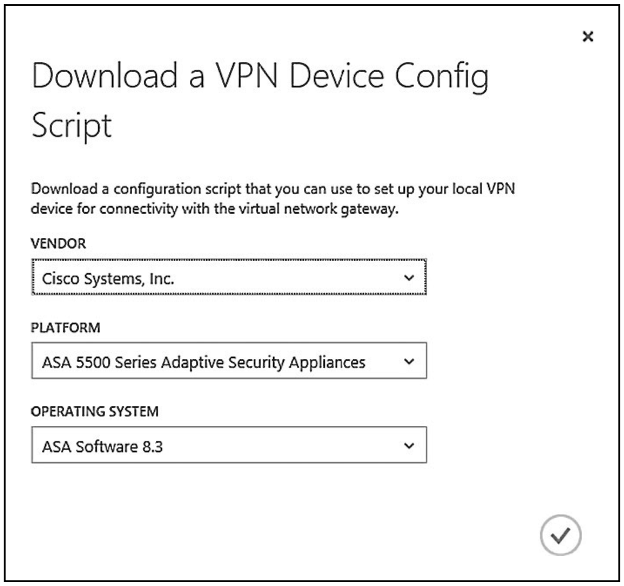
The next step in the process is to establish the site-to-site VPN gateway. To do so, click on Networks and then click the New button. Now, click on your virtual network. This will cause the virtual network's dashboard page to display. Click the Create Gateway button and, when prompted, click on the Yes button to create a site-to-site gateway. It's worth noting that it can take Windows Azure several minutes to create the gateway, and you'll have to wait until the creation process completes before continuing.

Once you've created the gateway, you must establish site-to-site connectivity. The exact process for this can vary widely depending on the type of VPN you're using. However, Windows Azure does provide a couple of resources to help you through the process.

If you're planning to use Windows Azure as an extension of your datacenter, it makes sense to create a hybrid Active Directory forest in which domain controllers exist on-premises and in the cloud.

Windows Azure Gateway

The first of these resources is a Manage Key button located at the bottom of the screen. The Windows Azure gateway is designed to use pre-shared keys for connection authentication. Clicking the Manage Key button retrieves the managed shared key. The resulting dialog box also contains a Regenerate button that you can use to create a new key.



Download a VPN Device Config Script

Download a configuration script that you can use to set up your local VPN device for connectivity with the virtual network gateway.

VENDOR

Cisco Systems, Inc.

PLATFORM

ASA 5500 Series Adaptive Security Appliances

OPERATING SYSTEM

ASA Software 8.3

Figure 4. *You can download a VPN device configuration script from Windows Azure.*

The toolbar at the bottom of the screen also contains a Download button (see **Figure 3**). When you click the Download button, you're directed to the Download a VPN Device Config Script page (see **Figure 4**). Microsoft has provided configuration scripts for a number of different VPN devices. You can select your VPN vendor, platform, and OS and then download a script that's designed to automate the configuration process.

Build a Domain Replica

Once you've established the necessary site-to-site VPN connectivity, the last step in the process is simply to build a replica DC on a Windows Azure-hosted virtual server. This process is really no different from that of setting up any other VM, except that you'll need to make sure the VM is connected to the virtual network you created earlier.

Once the VM is up and running, you'll also need to make sure that the new virtual server has been assigned an IP address that conforms to the range used by the virtual network. If not, then you'll need to manually assign an appropriate IP address to the VM.

At this point, you should be able to verify that the newly created virtual server is able to communicate with your on-premises servers. Assuming that you're able to verify connectivity and you're able to resolve the DNS names of the on-premises servers, then you can make the new virtual server a replica DC. Doing so involves joining your on-premises domain, using Server Manager to install the Active Directory Domain Services, and then promoting the server to DC status.

The overall process of building a hybrid Active Directory deployment is relatively straightforward.

Active Directory Cloud-Enabled

As you can see, the overall process of building a hybrid Active Directory deployment is relatively straightforward. The only real ambiguity in the process is in establishing site-to-site connectivity, but the downloadable VPN configuration scripts should greatly help reduce the complexity of this process. **R**

Brien M. Posey is a seven-time Microsoft MVP with more than two decades of IT experience. He's written thousands of articles and several dozen books on a wide variety of IT topics. Visit his Web site at brienposey.com.