Deploying Domain Controllers in Windows Azure

Windows Azure also provides Infrastructure as a Service (IaaS), which allows you to run services and infrastructure on the Windows Azure platform. Specifically, Windows Azure IaaS provides storage, networking, database hosting, and virtual machine hosting services. All the considerations for virtualizing applications and servers in on-premises infrastructure apply when you deploy the same applications and servers to Windows Azure.

Note: Windows Server 2012 Active Directory, which has been deployed in Windows Azure, is not the same as Windows Azure AD.

Windows Server 2012 Active Directory, which has been deployed in Windows Azure, is your own roles and services (AD DS, AD LDS, AD FS, AD CS, and AD RMS) that you have deployed into Windows Azure.

When you deploy AD DS in Windows Azure, you are responsible for maintaining everything except the hardware.

Windows Azure AD is a service that Microsoft has configured in the cloud. It does not have all of the functions that an on-premises AD DS has; it is concerned primarily with identity management and access control.

With Windows Azure AD, you are responsible only for managing your data.

Windows Server 2012 is designed to make it easy for you to integrate it into cloud-based systems. One of the most important decisions that an administrator must make is whether the organization should use public-cloud IaaS or private-cloud virtualization technology, or continue to use physical servers.

When you implement AD DS in Windows Azure consider the following:

- Rollback. While Windows Azure does not provide rollback services to customers, Windows Azure servers may be rolled back as a regular part of maintenance. However, when an AD DS

system is rolled back, duplicate Update Sequence Numbers (USNs) could be created, and because domain controller replication depends on USNs, duplicate numbers could cause problems. To prevent this, Windows Server 2012 Active Directory introduced a new identifier named *VM-Generation ID*. VM-Generation ID can detect a rollback, and it prevents the virtualized domain controller from replicating changes outbound until the virtualized AD DS has converged with the other domain controllers in the domain.

- Virtual machine limitations. Windows Azure virtual machines are limited to 14 GB of RAM and one network adapter. Also, the checkpoint feature is not supported.

When you deploy Windows Server 2012 Active Directory on Windows Azure virtual machines, the deployment is subject to the same guidelines as running AD DS on-premises in a virtual machine. These guidelines include the following:

Time Synchronization. A Windows-based AD DS domain infrastructure relies loosely on all communicating machines having the correct time. When domain controller clocks and domain member clocks have a time difference of more than five minutes, clients cannot sign in or access network resources. Therefore, Windows has the Windows Time Service (w32time). This service ensures that the time is synchronized across the domain in the following manner:

- The PDC emulator of the root domain should be configured with an external time source, such as an Internet time provider by using the network time protocol (NTP).
- Domain controllers use the PDC emulator from their own domain or from their parent domain.
- Domain members obtain the time from their domain controller.

Synchronizing the time across the domain is not as easy in virtualized environments as on physical computers. The virtualization engine regulates the use of the virtualization host's central processing units (CPUs) and distributes the system's resources among the virtual machines as needed. The operating system clock relies on stable CPU cycles, which do not exist in virtual environments. Virtualization engines perform time synchronization with the guest computers by default. When virtualization hosts do not participate in time synchronization, the domain time and the virtualization host time will likely become out of synchronization. While the physical computers participate in the time synchronization, virtual machines are reset to the time on the virtualization host. To avoid this problem, you must configure the virtualization host to participate in time synchronization or disable the synchronization to the virtual domain controllers.

Single Point of Failure. Your AD DS domain controllers are the most important pieces of your infrastructure. If they fail, users are unable to sign in, access resources or applications, and certain services may not run as well as they would normally. So it is very important that your AD DS domain controllers are set up so that they are not a single point of failure.

When you virtualize domain controllers on Windows Azure, you do not control the physical infrastructure, so you cannot use the same strategy to avoid a single point of failure as for an on-premises installation. To install multiple domain controllers on Windows Azure and ensure they do not share any hardware, you can install each domain controller into a different

Windows Azure datacenter.