Azure DOMAIN CONTROLLER REPLICA

Target Customers

- Customers who do not host additional domain controller locally
- Customers who want to keep a backup of the Active Directory infrastructure outside the company

Solution Overview

Take advantage of Azure Active Directory Domain Services features like domain join, LDAP, NT LAN Manager (NTLM), and Kerberos authentication, which are widely used in enterprises. Migrate legacy directory-aware applications running on-premises to Azure, without having to worry about identity requirements. On Linux and Windows Server virtual machines on Azure, easily deploy line-of-business applications. You don't have to deploy domain controllers as Azure virtual machines or use a VPN connection back to your identity infrastructure.

Why Customers Choose This Solution

- They want to keep an Active Directory backup in a different location.
- They want to ensure the continuity of the authentication and authorisation system in case of a local disaster.
- As Active Directory stores all the company identity and password information securely, they do not trust the security service that the local hoster can provide. They request to work with a provider that is global and ISO 27001 compliant.

Challenger Questions to Customers

1. Have you located additional Active Directory in a different location?
2. Do you have a continuity plan against the interruptions and malfunctions that may occur in your Active Directory system?
3. Are you sure that your Active Directory Database is kept in a secure environment?

Solution Explanation

1. Because Active Directory performs identity management and authorisation, all processors and applications operate are Active Directory dependent. For this reason, it is very important to keep a working copy of Active Directory in a different location.
2. When you extend your Active Directory system to Azure at the virtual machine level, the server on Azure runs with a 99.99% SLA. As a result, the continuity of your authentication and authorisation system is ensured.
3. Active Directory database file (ntds.dit) can be accessed through the host. In this case, all user and password information stored on the Active Directory can also be accessed. When you extend your Active Directory structure to Azure, you can benefit from security services such as disk encryption (bitlocker), additional network security applications, and role-based access control. (unlike Local Hoster)

FIRST DISTRIBUTION™
Epsidon Technology Holdings

Sizing & Pricing Questions

1. How many users do you have in your Active Directory environment?
2. How is the CPU and RAM utilization on your existing Domain Controller?

Sample Pricing

Pricing Items:
- Virtual machine type (Additional DC)
- Virtual machine disk type and size
- VPN Gateway type
- Backup (Optional)

Sample Pricing:
- B2S Vm as DC
- Basic VPN
- Azure Backup

Average Azure Consumption Revenue / month ($)

$50/month

More Information

https://azure.microsoft.com/en-us/services/active-directory-ds/

Visit Azure Portfolio

microsoft.leads@firstdistribution.com

+27 11 540 2640