Infrassist
Managing I.T.

Case Study

Azure File Share & On-Premises Authentication

The Customer:

ABC*

Industry:

Retail

Location:

South Africa

Overview

The end customer ABC* is a company that sells and pawns quality second-hand goods. It has four locations in South Africa and all four locations has AD-DNS & GC servers. They are running on an on-premises Windows Server 2012 R2 & Windows Server 2016. ABC* wants to move their File Servers to cloud with Azure File Share. Also, ABC* has created a VM called Pastel on Azure portal with the same AD-DNS & GC role. All four sites interconnected with MPNL line and Azure VM connected with Azure VPN gateway with company's firewall.

(*As we are white-labelled service providers, we cannot disclose the actual names of our customers. Hence all customer names that we use in our case studies are hypothetical- unless they give us the permission to use their names)

Challenges

Technical Challenges

Multiple challenges were faced during the setup of Azure File Share:

- It must have updated password update for Azure File Share to avoid “Access denied” issue while mounting Azure file share.
- Built-in AD account did not sync with Azure AD (e.g administrator@domain.com).
- To work around, we edited service object under Azure AD tool call Idfix tool, which syncs all built-in accounts to Azure AD if it is under selected OU on Azure AD Connect. User accounts are hybrid identity to mount Azure File Share.

Solution

Solution

A successful and seamless implementation and configuration of Azure File Share & On-Premises Authentication.
Following procedures were carried out for Azure File Share & On-Premises Authentication.

- Enabled AD DS authentication on storage account follow by installed AzFilesHybrid module on AD server.
- Assigned Share level permission for a share to the Azure Hybrid identity on Azure Portal
- Mounted Azure File Share on AD server with Storage Account key, followed by configured windows ACL(NTFS) permission over SMB for directories and files.
- Updated password of storage account identity in AD DS
- To validate it, mounted an Azure File share to domain joined devices with AD identity.

Once above steps are successfully performed, then the users can access Azure File share as mounted drive (Map Drive) like local or network drive.

Technologies

Technologies used

Azure
Active Directory

Azure Storage Account and key, Azure File Share, Virtual Network

Result

Accomplishment

A Successful implementation of Azure File Share & On-Premises Authentication took place which led to an enhanced performance and reliability

About Infrassist

Empowering MSPs by leveraging technology and human talent to help them transform and scale their business. We act as a catalyst and provide next-generation services and processes with reliable, cost-effective, agile and scalable IT solutions. Assisting MSPs with solutions that are designed to meet the demands of today's always-connected, digital world.

India
B1 - 9th Floor, Westgate
Business Bay, SG Highway,
Makarba, Ahmedabad, Gujarat,
India- 380051

Australia
St. Kilda Road towers, Level 1,
1 Queens Road,
Melbourne,
VIC 3000, Australia

UK
Norton Park Ascot,
Berkshire
SL5 9BW London,
UK

✉ **partners@infrassist.com**

50+
Technology Experts

75+
MSPs Served

2015
Year of Establishment

30000+
nodes

24x7x365
operations

27001:2013
Certified

3 Offices
India | Australia | UK