WINDOWS VIRTUAL DESKTOP & VDI

OVERVIEW

The client is a leading global management consulting and executive search firm based in the United States. With 27 years of industry experience and annual revenue worth 700 million USD, the client offers services in Executive Search and Strategy Consulting.

PROBLEM STATEMENT & CHALLENGES

The client wanted to introduce Virtual Desktop Infrastructure (VDI) setup for improving usability for employees working from inside and outside the office. The challenge is to implement a personal WVD setup on Azure Cloud with highly secure connectivity. The aim was to enable business users to access the VDI machine from anywhere, on any device.

SOLUTION DELIVERED

Kryptos' followed a planned approach that aims at process excellence, automation, and improved end-user experience. The technical expertise and experience gained by Kryptos helped to deploy the WVD setup efficiently right from conceptualization till implementation.

Since the client wanted to implement WVD in Azure, the process started with creating virtual networks followed by necessary configurations for data security. WVD requires DNS and AD configuration with appropriate user authentication to enable secure access to IT resources and virtual desktops.

SOLUTION BENEFITS

1. End-to-End On-Premise & Azure Integration
2. Anytime and anywhere accessibility
3. Improved business agility, better efficiency
4. Instant scalability and real-time availability
5. WVD setup on Azure offers enterprise-grade security
6. Reduced CAPEX (capital expenditure) on IT infrastructure
7. A unified management experience for admins
8. Publishing multiple pools to accommodate the organization's diverse workloads

KEY RESULTS

The WVD implementation provided end-users with Windows 10 multi-session virtualized experience. The client is now able to manage all resources and workloads from a centralized console.

All the applications, data, and desktops are stored in a centralized location with enterprise-grade security solutions powered by stringent security policies.

Also, the organization's data is now secured, monitored, and is available for round-the-clock accessibility with the Azure platform.

Staff can now work from anywhere using any device and having a seamless end-user experience.

The entire process was categorized into several phases.

Phase 1: Set up and Registration

This phase involves managing consent and permissions along with assigning users and administrators.

Phase 2: Preparing the WVD Environment

While preparing the environment, the team needs to find out the Azure Subscription ID along with AD Tenant ID. It also involves configuring PowerShell and setting up Windows Virtual Desktop Tenant.

Phase 3: Configuring DC and VMs

Kryptos team created Domain Controller (DC) in Azure as a best practice as the DC in the Azure Cloud adds resilience and flexibility to the architecture. Virtual machines were created including disk configuration, network configuration, IP configurations, and DNS setup.

Phase 4: Setting Up VPN

A secure and encrypted connection is a priority to protect the integrity of the organization's data; hence, the team configured VPN. Once the deployment is successful, validation of resources, certificates, and other configurations will be completed.

Phase 5: Integration

During the integration phase, the On-premise domain controller will be synced up with Azure AD, Verifying VMs, assigning users, and finally publishing apps.