MICROLAND®
Making digital happen

WHITEPAPER

COVID-19 and the Cloud Imperative: The seamless workplace in challenging times

With the COVID-19 outbreak, businesses are forced to renew their focus on remote work to ensure business continuity. Over the years, many options have arisen for accessing systems and data remotely via Virtual Private Network (VPN), Screen Sharing, Remote Desktop Services (RDS), Virtual Desktop Infrastructure (VDI) to name a few. VPN and VDI are the most commonly adopted strategies, but not without challenges of their own. While VDI allows for quick access to internal resources in a centralized and secure environment, not many businesses have adapted to VDI due to the huge upfront expenditure. On the other hand, VPN has been a popular option due to lower capex and simpler deployment. VPN allows remote access to internal resources with a decentralized approach, offering some security benefits but also leaving a lot of issues unaddressed. As times are changing, more and more workloads being moved to the Cloud, VPN is becoming obsolete as the services are scattered across cloud and data center. In this scenario, how do businesses control access to internal resources while keeping robust security posture?

The new emerging world of VDI

When it comes to delivering a rich user experience, mobility and flexibility, VDI fits the bill and is a star in this category. VDI is focused on centralized data management and prevents data breaches as the data does not reside on the endpoints, rather in the centralized data center storage. Users can access internal resources using a secure encryption protocol even on a low-bandwidth connection, as the data is accessed via a stream of pixels and not by downloading data onto the endpoints like in the case of VPN. Both VPN and VDI can be secured, but VDI presents less amount of risk, thus enabling use-cases with BYOD devices to work remotely. But VDI scares away businesses as it requires huge upfront expenditure. Many businesses deal with the harsh economic reality of tighter budgets and commitment to lower capital expenditures, forcing them to explore new options to make a transition. One such option that is gaining a lot of traction is VDI on Cloud or Desktop-as-a-Service (DaaS). There are various companies in the market that offer DaaS which include market leaders VMware and Citrix, runner-up AWS workspaces and latest entrant Microsoft's Windows Virtual Machine (WVD).

In DaaS, you get all the capabilities of VDI plus the following benefits:

- Financial shift - CapEx to OpEx model
- Faster and easier deployment
- Support for pervasive mobility
- Adaptive end-user experience
- Improves security and compliance posture
- Data centralization
- Always upto data platform
- Minimal IT skills
- Pay-as-you-go

How to Move Users From Physical to Virtual Machines

In order to enable users to work remotely, businesses need to plan for the following in order to deliver a rich user experience and maintain security posture while using DaaS.

User Profile: The problem with migrating user profiles is carrying the problems that would have persisted in legacy desktops environments. If you are migrating to a newer operating system, it will be even more complicated since a lot of useless information will be moved to the new operating system. If you are using User Environment Manager (UEM) products that's great! Your migration is on the fast lane. UEM products offer low-level customization, that abstract user settings from the OS thus making it possible to manage each setting at a granular level. Consider introducing UEM products if you haven't already as a part of your DaaS journey.

Data: File services make it simple to migrate to DaaS, as that's where all the user data reside, and the first thing users would like to see on their new desktops. Consider moving data closer to the virtual desktop to provide seamless access.

Applications: Most of the DaaS vendors offer their own application virtualization stack that fit well within their desktop virtualization stack. It's not mandatory to use the application virtualization stack provided by the vendor. If you are already using SCCM, Thinapp's or App-V you may decide to extend it to DaaS. Alternatively, granting access to applications is often a function of the nature of the access.

Connectivity: There needs to be a significant assessment done on the network side to make realistic assumptions on the traffic flows between your LAN/WAN and DaaS provider. Consider using software defined networks working with cellular circuits as one of the options for reliable connectivity. .

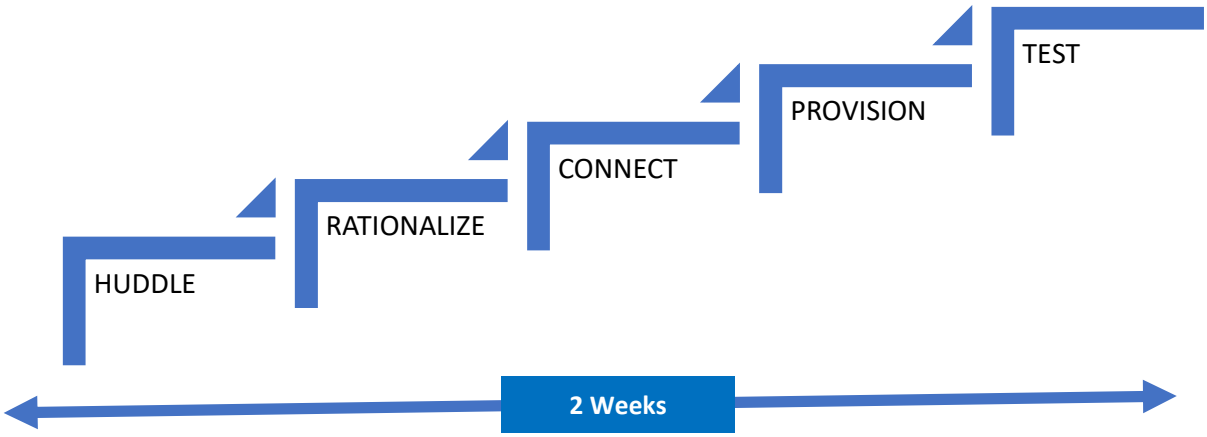
Security: Typically, in VDI, the data is not stored on the endpoint. The following key approaches can be taken, factoring-in security and compliance needs:

- Allow only using encrypted protocols
- Host internet-facing VDI components in DMZ
- Implement and tweak GPO's provided by the VDI vendors
- Select the right cloud that meets the requirements
- Use anti-virus and malware protection
- Use latest and up-to-date solutions

Enable Remote Workstyle with Cloud-based VDI – The Microland Way

Microland can help you rapidly build a new or hybrid Cloud VDI environment. Be it on a Citrix or VMware environment, we will remotely build an extended VDI in the Cloud within 2 weeks. Leveraging our pre-defined architecture for Citrix and VMware on AWS or Azure, we will rapidly deploy the Cloud VDI environment based on your business fitment while complying to security requirements.

The following points detail our approach towards implementing VDI extensibility and the recovery strategy in a cloud environment.



Step 1: HUDDLE for a quick discussion-cum-workshop to understand the business requirements and technological capabilities of the current environment which will influence the extensibility strategy required.

Step 2: RATIONALIZE the classification of organization technology stack based on tier provides visibility, flexibility and potential cost saving.

Step 3: CONNECT by identifying and establishing right connectivity type between the on-premise and cloud networks for seamless integration and accessibility between the resource locations.

Step 4: Provision the required VDI block and services on the cloud / on-premise based on the requirements and incorporating recommended best-practices and validated designs options.

Step 5: Test extensibility and plan to validate its operation and ability to serve its core purpose.
Using our vast experience in helping global organizations across their desktop virtualization journey, we have developed VDI-based life cycle tools that will help customers in every step of their desktop virtualization journey.

- **R-Assess:** A Microland VDI Readiness Assessment framework that focuses on analyzing enterprise users' fitment & IT's readiness to adopt, deploy and manage VDI ecosystem
- **EMDaaS:** A Microland solution framework to design, build and operationalize the VDI environment and enable Desktop-as-a-Service
- **Cloud-XPRESS:** A Microland solution framework to assess, build and migrate / extend the existing VDI environment to the Cloud for availability, scalability, security & cost benefits
- **MPASS:** An Audit framework to analyze & optimize existing VDI environment for manageability, performance, availability, scalability & security
- **ManageD:** A Microland VDI environment management framework to monitor and manage an end-to-end VDI environment

Welcome to the world of the Microland XPRESS CLOUD, your quick cloud upscale solution.

For more information visit www.microland.com/digital/digital-workplace, or reach out to our digital experts.

About the Author(S)

Raj Kumar Thakur, Associate Vice President – Digital Workplace:
RajKumarT@microland.com

Raj Kumar Thakur has over 20 years of experience in the IT Infrastructure Management space and has played various roles in Service Creation, Service Delivery, Service Management Consulting and Solution Engineering. In Microland as Head of Digital Workplace Services Practice, he is responsible for building service capabilities in the areas of Digital Workplace, Cloud based messaging & collaboration and NextGen End user support ecosystem.

Abhishek Hiremath, Principal Architect – Digital Workplace:
RajKumarT@microland.com

Abhishek is a VMware, AWS and Microsoft certified solutions architect with over 14 years of experience. As a Principal Architect in Digital Workplace Services Practice at Microland , Abhishek brings an innovative and pragmatic approach to analyzing complex business needs, conceptualize, and offer cutting edge solutions to customers in their digital transformation journey.

About Microland

Microland's delivery of digital and "Making Digital Happen" allows technology to do more and intrude less. We make it easier for enterprises to adopt nextGen Digital infrastructure. We enable this using our expertise in Cloud and Data Centers, Networks, Digital Workplace, Cybersecurity and Industrial IoT, ensuring the embrace of brilliance is predictable, reliable, and stable.

Incorporated in 1989 and headquartered in Bengaluru, India, Microland has more than 4,500 digital specialists across offices and delivery centers in Asia, Australia, Europe, Middle East and North America