CrucialLogics
consulting with a conscience™

TIRED OF CITRIX?

Implement Azure Virtual Desktop With Tips From The Pros

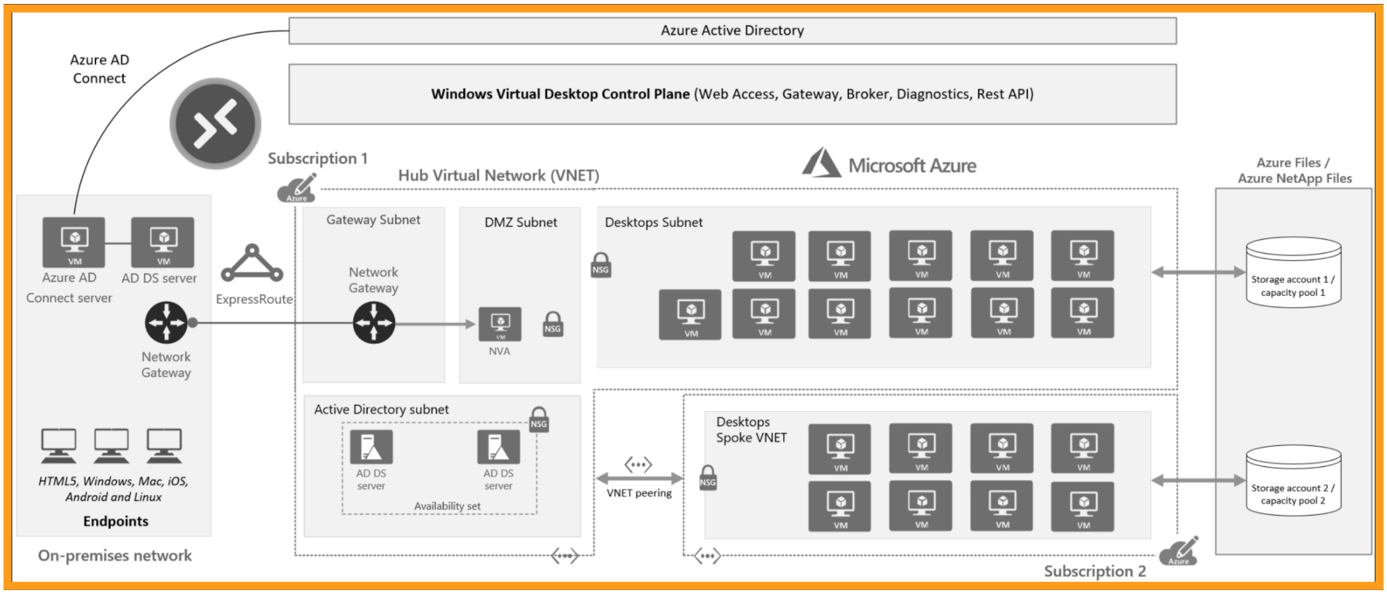
In today's work environment, impacted by COVID-19 lockdowns and social distancing, 64% of Canadian employees are now working remotely vs 6% prior to the pandemic.[1] We are in the midst of a massive shift in the way people work, and IT environments need to adapt. Forward-thinking companies are implementing virtual desktop environments to ensure user productivity, business continuity and operational efficiency while future-proofing for events like pandemics.

Virtual desktop infrastructure (VDI) can enable IT teams to better control corporate data and keep it secure

VIRTUAL DESKTOPS EXPLAINED

A virtual desktop or virtual machine (VM) has the same look and feel of a physical desktop, except the operating system and apps are hosted on a server or in the cloud rather than residing on the hardware. Azure Virtual Desktop (AVD) infrastructure, for example, is a cloud-hosted desktop and app virtualization, powered by fast Azure backbone connectivity. Regardless of whether the device is corporate or BYOD (bring your own device), and running Windows, Mac, iOS or Android, employees can connect to the virtual desktop and have the familiar Windows experience.

Virtual desktop infrastructure (VDI) can enable IT teams to better control corporate data and keep it secure, no matter where the employee is working, and companies benefit from having a standardized IT environment with centralized data protected by firewalls, security protocols and policies.



COMPARING VIRTUAL AND PHYSICAL DESKTOPS

A virtual desktop has the same interface, the same icons, runs the same apps and looks the same as working on a physical device. The user experience is almost identical, however the virtual desktop is accessible over an internet connection from anywhere. None of the data resides on the local device, so it will not be lost or at risk if the device is compromised. While physical desktops are also often portable and enable users to work from anywhere, disparate physical devices and systems make data security much more complex, especially if your company supports BYOD.

When it comes to software, unlike physical desktops, virtual desktops run only company-approved software, which is stored and distributed from a central location. It is also easier to scale compute power and storage on VDI, while a physical desktop would require an upgrade to a more powerful machine or a bigger hard drive. Virtual desktops also enable companies to easily scale the number of authorized users for apps.

For connectivity, virtual desktops require continuous, low latency connectivity to a VDI data center. Physical desktops, on the other hand, require fast, stable internet speeds – or downloading and uploading large files can be frustrating.

One of the key elements that virtual and physical desktops share is that their roll-outs require proper planning. For a virtual desktop roll-out, the focus is on centralization – the centralization of IT infrastructure, data security, file management, software licensing, user authorizations and more. We will talk about the planning and design process a little later in the Pro Tips section, but for now, here are some key advantages and disadvantages of virtual desktops to consider.

> Virtual desktops also enable companies to easily scale the number of authorized users for apps.

Virtual desktops are scalable to business needs, from powering 3D graphics rendering to enabling simple email and web browsing capabilities.

ADVANTAGES OF A VIRTUAL DESKTOP ENVIRONMENT

Provides Better Security
Virtual desktops offer more security than physical ones because data is not cached, so files never reach the user's uncontrolled premises where there is high potential for data leakage. Firewalling the virtual desktop environment can also help keep data secure. While virtual desktops are not reliant on secure physical endpoint device configuration, Microsoft Intune, a cloud-based endpoint management tool, can add another layer of protection with policies set up and configured according to your company requirements.

Natively Supports MFA
Having all users log in with MFA (multi-factor authentication) every time is part of an effective zero-trust security model, whereby no one gains access to the network without proper validation. MFA can increase data security, along with sessional controls and additional layers of protection, to safeguard user identity, devices and data. At CrucialLogics, we apply security best practices from Microsoft, ensuring your VDI is as secure as possible out of the box, including implementing MFA. We then custom configure according to your password policies, encryption settings and more.

Offers Higher Control
Maintaining control across all user devices can get complicated, especially in a BYOD scenario with a diversity of hardware, software and security capabilities. A centralized virtual desktop ensures that there is security standardization and control over the data. For example, reaching out to a user's BYOD endpoint to remove compromised mailbox data or downloaded malware can be very challenging, but if corporate data is kept in its own isolated area, like in a virtual desktop environment, it is much easier to control, manage and protect.

Delivers Potential Cost Savings
With virtual desktops, hardware requirements are lighter. VDI is essentially screen sharing and keyboard functionality transmitted across a network, so less expensive machines can be used. Additionally, virtual desktop data is not cached, so bandwidth needs are reduced, and home users can experience good fidelity even with a slower connection.

Provide Flexibility and Scalability
Virtual desktops are scalable to business needs, from powering 3D graphics rendering to enabling simple email and web browsing capabilities. They also enable companies to easily add or delete users from the virtual desktop experience, to simplify employee on- and off-boarding.

Eases the Transition to Windows 10
Rather than configuring and distributing new hardware, virtual desktop infrastructure can enable companies to easily transition employees from Windows 7 to Windows 10. Users can easily be upgraded into the latest Windows infrastructure so unsupported legacy systems can be transitioned off the environment.

DISADVANTAGES OF VIRTUAL DESKTOP INFRASTRUCTURE

When making a business case for virtual desktops, it is important to look at total cost of ownership. On the one hand, cost savings can be found in the use of cheaper, less powerful hardware, slower connectivity and in the consolidation and simplification of app management and licensing needs. On the other hand, some companies cite the yearly cost and complexity of virtual desktops as key disadvantages.

Some companies opt for a compromise, by rolling out virtual desktops to a subset of employees. For instance, an architectural firm could roll out VDI for AutoCAD and 3D rendering, which require heavy graphics power. In a virtual desktop scenario, rather than purchasing prohibitively expensive high-end hardware in the tens of thousands of dollars, a regular laptop connected through a virtual desktop could be used, and then disconnected when not needed to save utilities. VDI requires a new way of thinking, planning and working, but it can be used quite effectively to control costs.

In general, calculators are available to help companies figure out their needs based on density of users, usually on a per hundred basis, and on how powerful the virtual machines need to be. Calculating whether virtual desktops are right for a company really does depend on the number of users and what they will be using them for, such as Office versus graphics card work.

For companies with Microsoft 365 or Windows per-user licences, employees can be given lower end equipment and use Azure Virtual Desktop with no additional licencing costs. It comes as a free service.

Additionally, multiple concurrent sessions can be easily run with the same deployment on Windows 10 multi-session, while reducing IT management costs. Overall, virtual desktop infrastructure enables operational expenses to be better aligned with business usage.

> VDI requires a new way of thinking, planning and working, but it can be used quite effectively to control costs.

Virtual desktops are known for being an efficient, flexible and secure approach for workplace productivity.

PRO TIPS FOR IMPLEMENTING VIRTUAL DESKTOP INFRASTRUCTURE

Virtual desktops are known for being an efficient, flexible and secure approach for workplace productivity. When it comes to designing and building your virtual desktop infrastructure, here are some pro tips.

Analyze Network Latency

Virtual desktops require continuous, low latency connectivity to a VDI data center. High latency connections can make sessions feel sluggish. So, it is very important to check the latency between the home user's location and where they are connecting to the data center. The closest physical site is not necessarily the fastest connection. Running tests is essential to ascertain the fastest in-region data center in relation to each virtual desktop. In the case of a Microsoft environment, there is a website that can help. Go to http://azurespeedtest.azurewebsites.net from your site or server to see the nearest Microsoft Azure Data Center.

Ensure App Compatibility

The next important consideration is the compatibility of your apps. In a Azure Virtual Desktop environment there can be two modes: personal desktop and pooled.

Personal Desktop Mode: is when each user is assigned to a dedicated virtual machine. This model is used when there are applications that require one-to-one mapping.

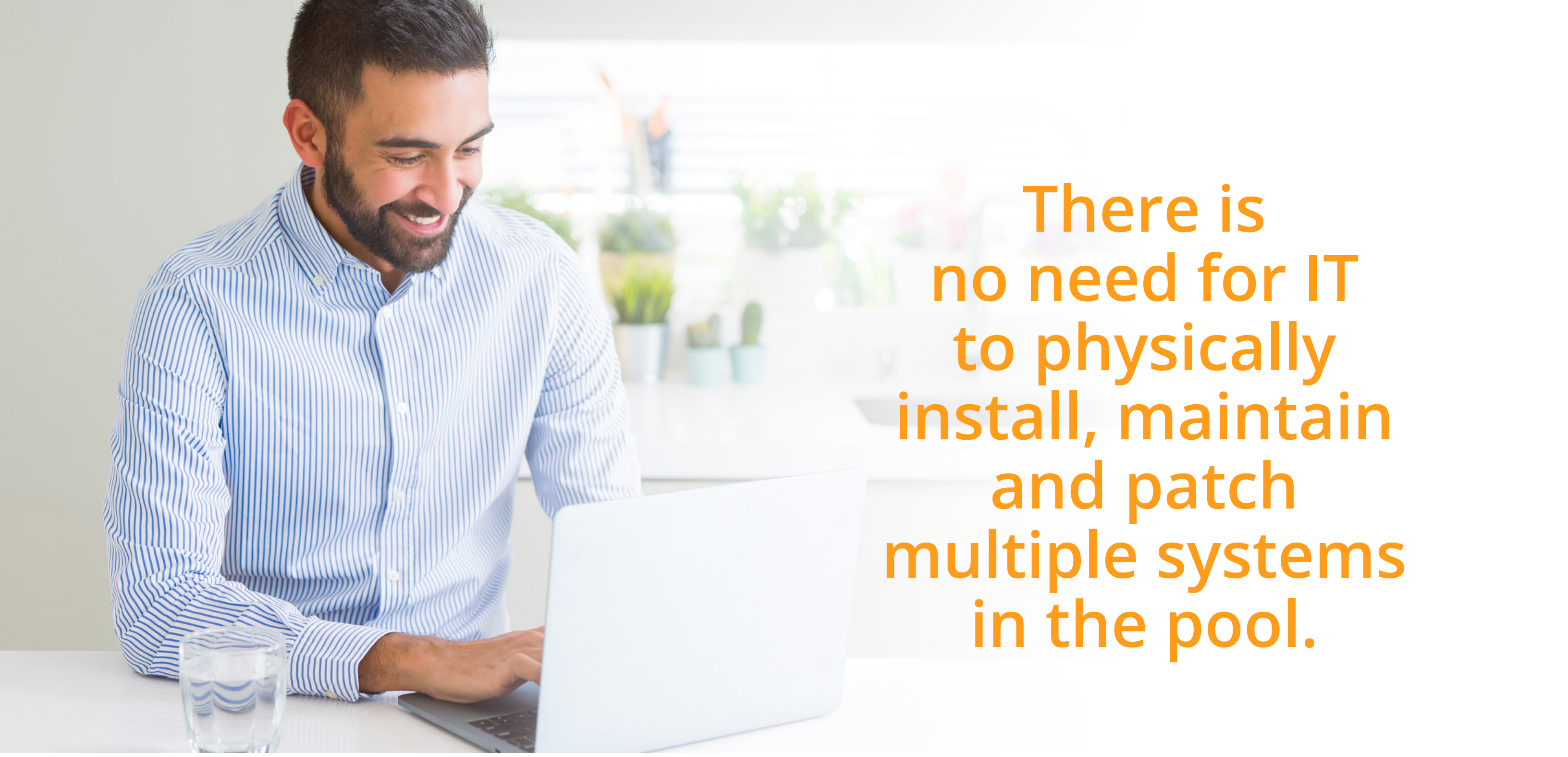
Pooled Mode: is when there is a pool of virtual machines and multiple users can log into that pool, which scales according to needs, such as a pool of 3 virtual machines that can allow up to 9 users. In this case, applications must be multi-user-friendly, like Microsoft Office or a web browser. Pooled mode provides opportunities for app resource sharing, and thus savings, but first you need to understand your application compatibility.

Build to 80% Capacity

At CrucialLogics, we make sure we only build to 80% of your load capacity, meaning out of 10 systems in a pool, we keep 2 in reserve as a fail-safe. This ensures systems are always up and running, and even if we need to take a system down for maintenance, users can fail over onto one of the other systems and stay productive.

Plan for Optimization

A virtual desktop environment requires a rethink of how data flows. Services such as OneDrive and SharePoint, for example, cache files. In a physical desktop environment, if a OneDrive file is opened, it downloads via the internet and caches to the local hard drive. But this is something to prevent in a virtual desktop environment. Virtual desktops provide quick access in what is essentially a live stream directly to the device, with Microsoft Azure services on the back end. To avoid bloat and unnecessary use of internet bandwidth, when a OneDrive file is opened in a virtual desktop, you don't want it to download and cache on the local machine, you just want it to



There is no need for IT to physically install, maintain and patch multiple systems in the pool.

open and be connected live. This is possible with Azure Virtual Desktop infrastructure because the virtual desktop is directly plugged into the Azure backbone.

So, to optimize WVD, caching must be disabled, and the reason is storage. The cost of storage would increase, and the system would be sluggish if it were full of gigs of OneDrive cached files, and it would also complicate the virtual infrastructure on the back end. Plus, if the same user were to go offline and then log into a second VM to access the same files, they would cache a second time, causing storage sprawl.

Another optimization strategy is to set up user profiles, which are managed centrally and which load onto the virtual desktop for each user. Profile Container is a handy software that redirects the entire user profile to whichever VM the employee is using in the pool, including just the apps that are authorized for that user. The apps, themselves, are stored in a central repository and authorized apps quickly load when users log onto the virtual desktop. There is no need for IT to physically install, maintain and patch multiple systems in the pool. Each update needs to happen only once, licensing only needs to be purchased for users with permission, and the user profile system manages user access. All of this can represent a huge savings on administrative overheads associated with app management and optimization.

When it comes to optimizing audio/visual capabilities, virtual desktops optimize media for Microsoft Teams users. In fact, audio, video and desktop sharing are seamless between the client system and the remote session, without overloading the virtual infrastructure or the network. Less sophisticated and less expensive hardware is required, and internet bandwidth is saved, because a direct P2P internet connection is established. This also makes the experience smoother and faster.

Plan for Internet Redundancy

If there is no internet, there is no accessing the virtual desktop, so an internet redundancy plan is key. Cellular backup by the same carrier, or even better, a different carrier, will enable users to tether to a working cell network if the home office internet goes down.

Pilot for a Significant Amount of Time

It is important to go through a proper design and build process, and then test and pilot. A system that is properly designed for one particular environment or use case, may turn out to not work with certain security software or certain production level systems once the pilot is launched. So, make sure the pilot is run for a significant amount of time, at least one or two weeks, to enable users time to test and provide valuable feedback.

SUMMARY

It was recently reported in Forbes that not only do employees want to work remotely after the pandemic, 58% say they would “absolutely look for a new job” if they were no longer allowed to work remotely in their current position.[2] Another 33% would like to consider a hybrid arrangement, with a mix of office and at-home work.[2] Virtual desktop infrastructure has the power to keep office and remote workers productive, while enabling IT teams to better control, secure and manage your corporate data and apps in a centralized environment. If you would like to learn more about what Azure Virtual Desktops can do for your business, let’s talk.

References

1. PWC Canada. Canadian Workforce of the Future Survey. 2020. https://www.pwc.com/ca/en/today-s-issues/upskilling/canadian-pulse-survey.html
2. Forbes, Future of Work: What The Post-Pandemic Workplace Holds For Remote Workers’ Careers, May 2, 2021. https://www.forbes.com/sites/bryanrobinson/2021/05/02/future-of-work-what-the-post-pandemic-workplace-holds-for-remote-workers-careers/?sh=bbd0f517f5b8

If you’re ready to discuss your company’s needs, **let’s chat.**

ABOUT US

We help technology and business leaders make better IT decisions by seeing things you haven’t seen before. We are advisors first who review your enterprise vision, identify technology gaps and develop an IT or business transformation strategy with key decision points translated into business outcomes. We identify where you need to be and the decision points along the way to digital transformation. We have been awarded Top 50 Best Managed IT Companies 3 years in a row.

Gold Microsoft Partner
Microsoft

IT COMPANIES 50 BEST MANAGED

CrucialLogics
consulting with a conscience™

cruciallogics.com