nerdio | Manager for Enterprise

Why Azure Virtual Desktop (AVD) Deployment is Important for a Hybrid Work Environment for the Enterprise

Find more:
getnerdio.com/nme

Introduction

Over the past year we have seen a fundamental shift in the way people across the globe work and run their businesses. With large corporations like Microsoft, Facebook, and Spotify opening up work-from-home (WFH) options, organizations are forced to come up with cost effective, powerful, and reliable remote solutions. In today's world, businesses are forced to consider a much more dynamic "office" with WFH users in separate geographic locations all over the country or world, and on varying networks. Understanding all this makes it important to consider robust solutions that support hybrid work environments. In this white paper, we will talk about five key reasons to consider Azure Virtual Desktop (AVD) as a fantastic solution when approaching these challenges.

1. Understanding AVD & Basic AVD Deployment

Before we begin talking about AVD, let's spend a moment discussing what AVD actually is. In Microsoft's own words, "Azure Virtual Desktop is a desktop and app virtualization service that runs in the cloud". In other words, AVD allows people to run both fully customized virtual desktops or specific remote applications in virtual environments without ever having to purchase any of the physical hardware themselves. AVD is a solution offered through Microsoft's virtual cloud platform known as Microsoft Azure. Azure provides the ability to configure a virtual office space which conforms to the highest security requirements while also being one of the most dynamic and flexible solutions on the market today. Enterprise organizations get to work with the confidence that their virtual environments are backed by Microsoft's trillion-dollar security backbone and the most modern and advanced security features. So, with this in mind let's get into some of the details.

In a typical AVD deployment, you'd have the following environment components:

1. **Virtual Network (Vnet)**
    a. Specified Subnets
    b. Network Security Group (NSG) to filter network traffic
2. **Identity Management**
    a. Options include:
        i. Azure Active Directory Domain Services (AAD DS)
        ii. Domain Controller VM with Active Directory and AD Connect installed
    b. Integration with Azure AD & O365
3. **Physical Server Infrastructure**
    a. Line-of-Business Servers
    b. User AVD Pools
4. **Backups**

As you can see, a standard AVD deployment isn't overly complex and includes many of the components that you'd expect to see in an on-premises environment. As a result, managing a AVD environment isn't rocket science, especially when you utilize a tool like Nerdio Manager for Enterprise to help you wrangle it *(more to come on this later)*. For now, let's transition into our Data Security conversation.

Security

One of the primary concerns with the modern dynamic office is security. Users are working on either company or personal devices and the networks they connect to can be anything from their own home network to a local coffee shop. As a result, the security of critical company data is at risk, especially if users are in the habit of saving folders and files on their desktop. Let's break this conversation down into three distinct categories:

1. **Network Security** – Starting on the Network layer Azure has a plethora of options for you to choose from when it comes to ensuring your client environment is secure.

These include things like Azure Firewall, Azure DDoS protection, and Azure Monitoring and Threat Detection. Utilizing one of these, or even a combination of them provides you the flexibility to shore up your environment based on best practice and the industry requirements for your client. Something as simple as leveraging the Network Security Group under the VNet and configuring it to abide by the philosophy of "deny all allow by exception" can be a great place to start. This is where you deny all traffic on the VNet except that traffic which is specified in your rules. This keeps the environment locked down and helps to secure it against outside threats.

2. **User Security** – If you've spent any time working with O365 and Azure AD you'll be familiar with Azure's Resource Based Access Control (RBAC). This allows you to set specific user layer permissions, or broader group permissions to resources within Azure. This can be something as simple as an Azure Marketplace application, or as broad as an entire Azure subscription with all the subsequent resource. As an administrator Azure RBAC allows you to abide by the philosophy of "least privilege", keeping your environment secure in the event that a user account is compromised. Through Conditional Access Policies (CAP) you can set rules to enforce MFA for all users, or a subset of users. CAPs also allow you to set things like trusted IP addresses where MFA will be required for any IP outside the specified range. This allows you to keep the environment locked down, but also provides ease of use when users are working within the trusted IPs (i.e., at home or working from the office).

3. **Data Security** – A whole paper could be written on Data Security within Azure, however for this white paper I want to focus on a very specific aspect of that topic related to end users and their typical work habits. As we all know, it's easier to invent a new coding language than it is to introduce a new process or workflow for end users to follow. As a result, introducing the cloud can be a daunting prospect. However, AVD does an excellent job of simplifying this to one easy change. Since AVD publishes an entire virtual desktop for each user that is totally unique, you can configure it so the end user experience is identical to their local machine. You can copy over their Favorites, Desktop, Documents, and even Downloads folder to the cloud. You can set their background to be identical, and even customize their taskbar settings. To add to this, AVD does an excellent job on the audio/video and USB passthrough so that local devices can be accessed from AVD and video calls can be easily taken from the

AVD session. Now this is all great, but you might be asking, "how does this help with data security?" Well, the answer is quite simple. Users working and saving data locally presents an incredible security risk, especially since the endpoint and network they are utilizing might not be secure. If you can create a parallel experience in the cloud end users will have a very easy transition and often don't even notice they are in their AVD environment when they go to login each day. If the employee leaves the company, you can rest at ease knowing sensitive data is fully secure and in a place you can control. If the end user device is lost or stolen, it is quite easy to process a password reset and send the user another device. In this case, no sensitive company data was lost since end-users have everything in the cloud.

Flexibility and Cost Savings

One of the biggest draws to the cloud is the flexibility it provides. When you build a VM in Azure you are technically renting those resources from Microsoft. Once you decommission the VM, those resources become available again in the Azure datacenter and are provided to the next person who needs those resources. The benefit to you is that you are only responsible to cover the cost of resources while they are in use. This is a major shift from on-prem environments where you pay a large lump sum for a device and then that device is owned by you. With Azure, you can rent a super powerful GPU-enabled VM and provide multiple users access to that VM and its resources all at the same time. In this case, the endpoints they connect from are almost inconsequential and could be a simple low-end device. You no longer have to worry about providing super expensive machines for each user, and when an employee leaves the company, their data and the resources they consume are immediately available again. You can grant other users access to the data, and the physical resources on the Azure side can be decommissioned until a new employee is hired to replace the old one. This level of flexibility allows companies to have an incredibly effective and cost-efficient environment.

To add to the flexibility conversation is the ability to assign multiple resources to the same user. Let's say your environment contains three primary pools: 1) general session desktop pool, 2) published application pool, and 3) GPU-enabled pool. Now, let's say there are groups of users who will be assigned to each resource, but you then have managers within the organization who need access to several of these resources to help manage projects and access the various applications on each. With AVD, you can actually assign a

single user to any or all of the resources. The best part is that with auto-scale configured, you won't pay triple for that user. Instead, the pools will scale-out to accommodate the workload only when that user connects to access the resources. This can be an incredibly powerful and effective way to ensure that every user in the organization has direct access to all the necessary resources without paying the full on-prem price to purchase physical resources for each user capable of running each application and workload required.

The last thing we will discuss around Flexibility and cost savings has to do with hardware refresh in the cloud. With AVD, resizing resources and upgrading to the latest and greatest is a simple matter of assigning a new VM size or series to the AVD pool. This typically takes anywhere from 10-30 minutes depending on the number of current VMs in the pool. After the task is complete, all users get the benefit of the upgraded hardware. Contrast this with an on-prem environment and you're talking dozens of man-hours and thousands of dollars to order new hardware, unpackage them all, deploy all the various applications and software (hopefully with some type of automation), and then ship them to each user. Given how difficult this can be, most companies wait on the hardware refreshes much longer than they should and this can have a significant negative impact on productivity. By using AVD, you've condensed a very costly and time-consuming project down to just 30 minutes or less. End users can now work on the same low-end devices for years while always having the latest and greatest VMs to run their programs and critical LOB software.takes a lot of time; automation and DevOps can be tricky to maintain, and it's definably not for everybody.

Better Performance

When considering the modern dynamic office with users working around the country or around the globe, it can be challenging to ensure great end-user performance. This is especially true when users are attempting to access data or applications stored on company servers. To better clarify I'll use an example. Let's say you have an on-prem QuickBooks server that you need to grant 5 people access to, but each of these users are currently working from home and are separated by hundreds of miles. A standard approach for this might be to establish a P2S VPN connection from the main office to each of the 5 users to give them access to the various QB company files they are working on. However, we all know that QB has notoriously spotty performance over VPN connections. In AVD environments,

this becomes a non-issue as the QB server and the AVD pools are all in the same VNet and communication is handled on the Microsoft backbone. As a result, granting access is simply a matter of configuring permissions and performance for the end-users should be excellent since all the resources are housed in Azure datacenters.

When it comes to AVD pools and the resources user sessions are run on, you have an incredible ability (using tools like Azure Resource Monitor) to gather time-of-day data on when users are most active and what standard work patterns look like. This allows you to configure the environment to size up appropriately when users are working, and then size down when they have signed out for the day. Knowing exactly when users are active and architecting the environment to accommodate for that helps to ensure a fantastic end-user experience while also allowing you to capture great cost savings. eggs into one basket" comes to mind.

5. Why Nerdio?

Now that we've talked about Azure, AVD, and how amazing this solution can be for you and your clients, let's talk for a moment about Nerdio Manager for AVD and where we fit into the equation. To address this we must take a moment and consider Microsoft's approach to Azure and AVD as a whole. Microsoft was presented with the incredible challenge of providing a solution that can accommodate the huge variety of environment needs and use cases in the market. This includes everything from massive 100,000+ user environments, all the way down to that 2-user startup that just launched last month. With this amount of variability comes a huge degree of complexity… which makes sense. However, as an organization that is just migrating to the cloud due to the recent pandemic, it can be quite difficult to keep highly skilled Azure employees who are trained and knowledgeable in Azure to continuously deploy and manage these complex environments. Not to mention, the payroll starts to add up as your engineers get more and more Azure certifications. Nerdio Manager for Enterprise is an automation tool that simplifies the vast majority of tasks you'll want to complete in Azure down to 3-clicks or less. Using our tool, even inexperienced tier 1 technicians can manage complex environments, configuring advanced auto-scale settings, manage custom Images, and rollout changes in just a few clicks and with very little Azure experience. In a nutshell, Nerdio Manager for Enterprise allows you to enter the cloud space with confidence knowing that you have an automation tool that will propel you ahead in productivity, security, ease of use, and cost savings.

Good news – You can try Nerdio Manager for Enterprise free for 30 days. Download it straight from the Azure Marketplace and get started today.

nerdio | Manager for Enterprise

About Nerdio

Nerdio empowers IT Professionals to deploy, manage, and auto-scale Azure Virtual Desktop. Created to address the technical and security requirements of enterprise customers, Nerdio Manager for Enterprise is ideal for IT Professionals looking to deploy and manage large AVD environments and can be connected to an existing AVD setup or used to stand up a new AVD deployment. Nerdio Manager is an all-PaaS Azure application that runs in a customer's own Azure subscription, making it one of the most secure and compliant solutions on the market.

Contact Us:

Email: hello@getnerdio.com
Website: getnerdio.com/nme
Find Nerdio in the Azure Marketplace: nerdio.co/nme