nerdio | Manager for MSP

HOW TO

Lift and Shift Migration Strategy for Managed Service Providers (MSPs)

Find more:
getnerdio.com/nmm

Introduction

As a quick overview and definition of terms, a "lift and shift" is where existing resources are migrated from the on-premises environment into Azure. A close cousin of this is a Greenfield deployment where new VMs are provisioned in Azure and only the data is moved from on-premises. In this white paper, we will use lift and shift (L&S) to reference both since in most cases, partners will be doing a little bit of each when migrating their on-premises environment to Azure.

Before we get too deep into the L&S strategy, let's also discuss its counterpart which is known as a Hybrid Active Directory configuration. Hybrid AD is the process of extending an on-premises internal domain into the Azure environment, allowing you to keep existing infrastructure in place, as well as providing new resources in Azure under the on-premises internal domain.

In some cases when we bring up the idea of migrating the on-premises environment into Azure, our partners become a little overwhelmed at the prospect of moving everything. They say something like "we've spent a lot of time and energy building the existing environment, we don't want to go through the headache of migrating everything or starting over." This is definitely a valid argument, however, when we break down the process and go over exactly what's included, most partners actually get excited about the L&S Azure migration option and elect to go this route.

Lift and Shift Concerns

In order to do this topic justice, let's begin by bringing up the top three concerns we hear partners raise when considering the L&S strategy, and we'll break down exactly why those concerns are largely unfounded.

Concern #1: Changing the Active Directory management from on-premisesises to Azure

"Transferring user data sounds like more work than it's worth, plus it could cause major disruptions for the end user."

To address this effectively, we'll break down both concerns in turn.

Active Directory

The process of severing the user's connections with the on-premisesises AD and transferring ownership of those users to the AD in Azure is pretty straightforward. What's, even more, is that the process of transferring ownership shouldn't cause any disruptions to the end-user. Nothing is physically migrated (i.e.. email, contacts, calendar appointments, etc.); you're only changing who has the rights to manage those user objects.

Transferring User Data

Since users will be moving to the cloud anyway, we see the process of transferring user data as the first step to get users thinking in that direction. Although there are several options for this, we normally see partners leverage something like SharePoint or OneDrive to easily backup the user's data, and then copy that to the AVD environment. We've even seen this as something the end users appreciate because it gives them the option to do some house cleaning on their local session. Our partners will hand this task over to the end-user and have them decide what's important to bring over to the cloud environment, and what on their computer is old or redundant data that can be cleaned up or left on the old environment. Once the users have synced their data with an application like OneDrive, the data migration phase is essentially over since the users will simply authenticate to OneDrive in Azure and have all their critical data ready and accessible.

As you can see, when we break down both of these concerns, the actual transition for the users won't cause much disruption at all and can take place during standard work hours if

necessary. The process of severing the user's connections with the on-premisesises AD and transferring ownership of those users to the AD in Azure is pretty straightforward. What's even more is that the process of transferring ownership shouldn't cause any disruptions to the end-user. Nothing is physically migrated (i.e.. email, contacts, calendar appointments, etc.); you're only changing who has the rights to manage those user objects.

Concern #2: Group Policy/On-premisesises Domain

"Our group policy and on-premisesises internal domain have been in place for years. It would be too difficult to start over in Azure."

Since both the GPOs and the internal domain have sometimes existed for over a decade, it's understandable why partners are initially hesitant to transition away. What makes matters worse is that most MSPs have inherited the domain and GPO from a previous provider, which adds another layer of uncertainty. In these situations, there are two options we see most often utilized by partners.

Option 1: Export/Import

The first option is to simply export the GPOs from the on-premisesises environment into Azure. This can be a good option, but one thing to keep in mind is that both the good and the bad get migrated over when going this route. If this environment had been operating for over a decade, it's likely a mess and you're bringing that mess into the Cloud with you. As a result, partners will frequently decide to go with option two.

Option 2: Clean Start with a Reference

The other option is to start over clean and fresh in the cloud but use the existing on-premises GPO as a template to build out the GPO in Azure. Although this sounds intimidating at first, once our partners really think about it, they actually start to like the idea of having full control and intentionality behind every rule and policy that's in place in the environment.

Tied into this conversation is the idea of moving away from the internal domain on-premises. This would be something like contoso.local. After working with many partners in similar

scenarios, we've found that since they are moving all the infrastructure and users to the cloud, there isn't a great reason to keep the on-premises internal domain. All the on-premises servers will be in the cloud and the users and their AVD desktops will be managed by AD and GPO in the cloud. The only thing left on-premises are the users' physical workstations which, to a degree, become irrelevant. What I mean by this is that technically, the users could log in from any computer in the world, as long as they have their phone nearby to verify 2- factor authentication. They could be at home, in the office, at the local library, etc.

In addition, given that AVD is now streamed to their local session, they could use something as simple as a Microsoft Surface Pro, Chrome Book, or some other low-level laptop. Once the connection is established, they're then placed in the cloud with all the controls and restrictions that have been set via GPO. So again, being tied to an on-premisesises internal domain is really not necessary since there won't really be anything left on-premisesises other than a few workstations.

Concern #3: Migration

"It's going to be too much of a headache to migrate all the On-premisesises infrastructure into Azure"

The final concern we see partners raise is related to the migration process of moving their on-premises infrastructure into Azure. This is especially true when they've spent an extended period of time configuring their Servers with applications and customizations that would take 8 to 12 hours to reconfigure from scratch in Azure. In these situations, we see them leverage Azure native tools like Azure migrate or Azure Site Recovery to lift their servers and place them into Azure. This allows for a transition of the entire server without going through the headache of reconfiguring it. They can then place it on the new internal domain in Azure and move forward as if nothing changed. The other option is to use something like our Nerdio built in data mirroring tool. This is effective when the on-premises server is end-of-life and has an outdated operating system. In this case partners don't typically want to move, for example, a server 2008 R2, or 2012 machine into Azure. Instead, they'll migrate individual files/folders using our data mirroring tool, and provision a brand-new server in Azure as the new host.

As you can see, if we break down the top three concerns and talk about the details of what's

included, then the L&S option becomes far more appealing, and the vast majority of our partners choose to go this Azure migration route.

Advantages of L&S

Now that we've addressed the top three concerns, let's talk about the top three advantages of going the L&S route.

Advantage #1: Reduces Overhead and Increases Security

As you can imagine, not having the on-premises infrastructure will immediately reduce costs when compared to the Hybrid AD setup. With the L&S strategy, you don't have to worry about refreshing end-of-life servers or keeping them backed up. The other benefit is that the L&S option requires less infrastructure to run than the Hybrid AD setup. Hybrid AD out of the box includes an additional DC to manage the Domain Trust between on-premises and Azure.

In addition to the reduced overhead, the L&S option is far more secure as there are less opportunities for security breaches. With everything sitting in Azure the only thing left on-premises are the physical workstations used to establish a connection to user's virtual desktops, and those are usually secured with 2-factor. The actual infrastructure in Azure and the security protecting it is backed my Microsoft's trillion-dollar budget, which makes it infinitely more secure than anything the average MSP could create, both physical and virtual.

Advantage #2: Run LOB Applications in Parallel

One of the advantages of a L&S deployment is the ability to test and verify the cloud infrastructure before providing access for end-users. This is especially true with Database applications such as SQL. You can restore the on-premises database in the cloud and run it for a few weeks or for however long is necessary to ensure everything is working as it should. Then as the last step just take one final backup of the SQL database, migrate it into the cloud environment over the weekend, and then use the Cloud environment as the authority starting the next week. This provides ample opportunity for testing and helps to ensure an outstanding end-user experience once the environment goes live.

Advantage #3: Clean Start

Going the L&S route provides for a good refresh of the entire environment. You're getting a new internal domain, fresh GPOs, new infrastructure, and a clean AD forest. In addition, you'll be running all servers on the latest OS and user desktops will be running Windows 10 natively, rather than a Server OS built to look like Win10.

In summary, going the L&S route can be a good way of bringing a client who was running on a legacy environment into the modern age of technology.

Migration Path

Now let's look at the practical order and steps we usually see these Azure migrations take. In order to provide the least amount of disruption to end-users, the Infrastructure & GPOs are typically pulled over to the new Azure environment first. After that's been thoroughly tested and confirmed to work, the end-users are then migrated over to the new environment and everything on-premises is done away with.

Step #1: Infrastructure

The first step when migrating the infrastructure is to select which servers will be migrated as a whole and which server will get built new in Azure. After this you'll migrate the servers specified to get lifted into Azure by leveraging the Azure Migrate tool. The servers you selected to build new in Azure, you'll use the Nerdio native Data Mirroring tool to transfer the data from the older server onto the new server in Azure. During this phase, you'll also configure the AVD pools and any dedicated desktops that will get provisioned for new users.

Step #2: GPO

Migrating the policies from on-premises into Azure is pretty straightforward. You can either export them from on-premises and import them into the Azure environment or use the on-premises GPOs as a template and build them new in Azure manually.

After migrating both the infrastructure & GPOs to Azure, the on-premises environment should still be fully functional. This means that from a quality assurance standpoint you'll be able to setup and configure everything in the cloud before moving to the user import phase. This allows you to test LOB applications, ensure GPOs are applying, and overall thoroughly test the environment to ensure that end-users have a great first impression. Once this is complete, you're ready to move to the User migration phase.

Step #3: Users

The final piece in the migration is to import users over into Azure. This includes breaking their connection with the current on-premises AD and adjusting the management piece to the AD in Azure. One thing to keep in mind is that the migration will require a password reset for each user and can take sometimes 72 hours to enable dirsync. We recommend initiating the process EOD Thursday or Friday (if doing it over the weekend) to provide enough time for the resync to conclude and users to get fully configured for the workday on Monday.

One important thing to note is that the process of breaking the user's connection with the current on-premisesises AD does not cause any disruption, but that's the piece that can take around 72 hours to complete. That timeframe is subjective and is something only Microsoft

can speed up, however starting this on Thursday or Friday during work hours won't cause any disruptions for the end-user. The only thing that will change is general user administration tasks such as password resets and user adjustments will need to be executed from the Office portal, rather than on-premises AD.

Once users are syncing with the AD in Azure the final step is to import their user data over. If you had each user backup their data to OneDrive, then this piece will be quite easy. The only thing required is to have users authenticate to OneDrive in their AVD session and their data will be ready and accessible.

That's it! At this point you've configured the infrastructure in the environment, you have it managed by the appropriate GPOs, and users have been migrated over and are operating smoothly in the new environment. Everything has been fully tested and it's all backed up and totally secure.

Helpful Tools

As the final section, I thought it would be beneficial to highlight a few Nerdio native tools that are quite helpful when transitioning from on-premises to the cloud.

Bulk Add/Update Tools

One of the most underutilized Nerdio tools is the Bulk Add/Update tools. These are used most effectively during the import/configuration phase and for bulk changes after the fact. Our bulk add/update tools provide a comprehensive Excel spreadsheet to populate with various changes including new resource assignments, password resets, and adjusting Office licensing. You can make all these changes on one sheet, then upload that to the Nerdio Admin Portal and our script will run through the list and make all the changes in an automated fashion.

AVD Pool Templates

If you have an existing deployment with Nerdio then you realize how valuable our pool templates are for making bulk application/software changes for whole groups of users in a quick and automated fashion.

Data Mirroring Tool

I've mentioned this several times already, but it's worth mentioning again here because it makes the data migration piece of deployments so simple and easy. It can be located under the "Onboarding" tab in the Nerdio Admin portal.

Final Thoughts

As we've seen, the L&S strategy for environment migrations is less expensive, more secure, and provides a more dynamic and flexible work environment than a Hybrid AD solution. When at all possible, we recommend utilizing this Azure migration strategy. .

Interested in learning more? Contact us to chat more about your L&S migration questions.

About Nerdio

Nerdio Manager for MSP is an Azure managed application that empowers Managed Service Providers to build successful Microsoft Azure cloud practices. Automatically provision a complete Azure Virtual Desktop (AVD) environment in under an hour, connect to an existing deployment in minutes, manage all your clients in a single pane of glass admin portal, and optimize their AVD environment with powerful autoscaling. For more information, visit www.getnerdio.com/nmm.

Contact Us:

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