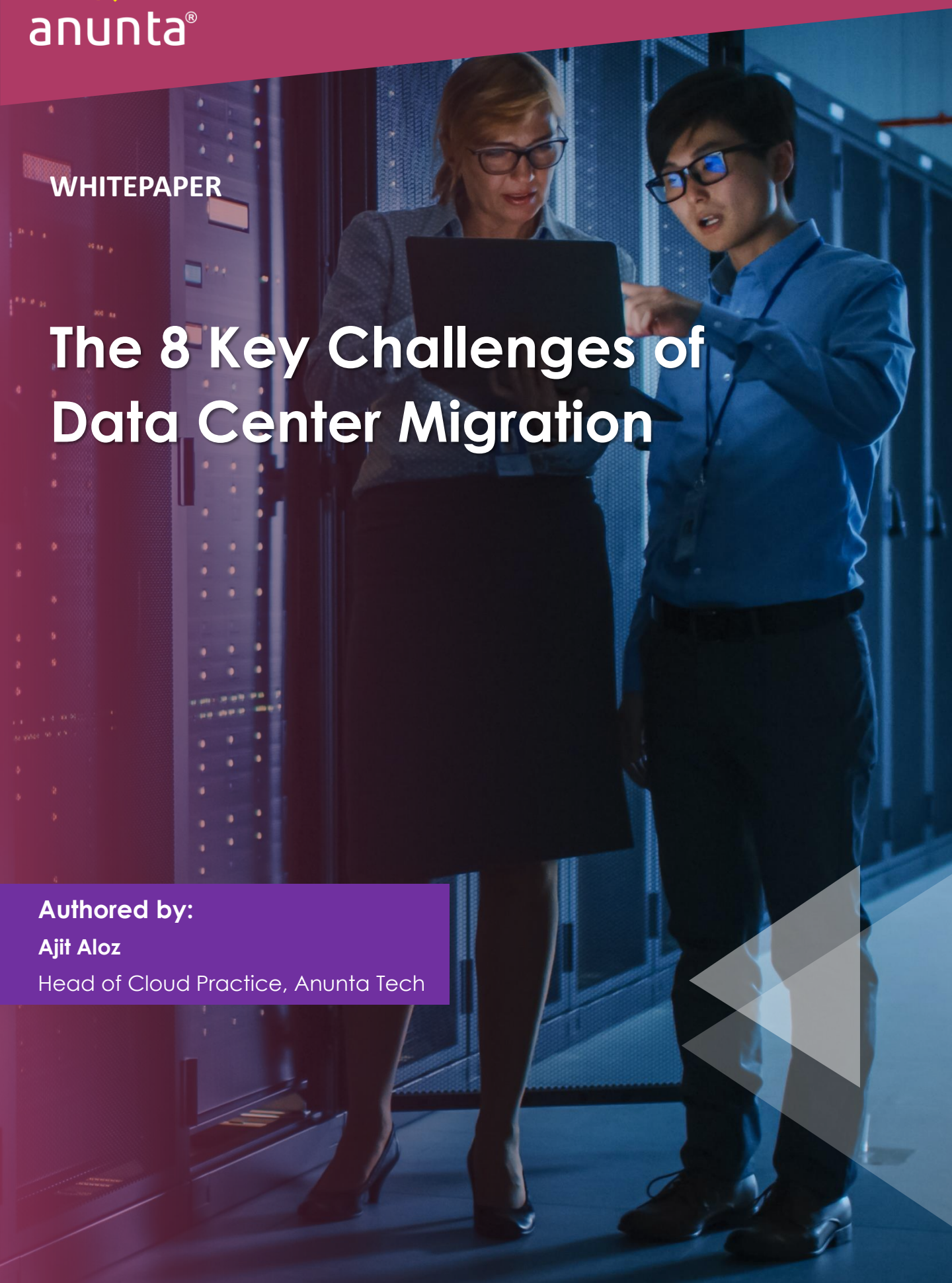
anunta®



WHITEPAPER

The 8 Key Challenges of Data Center Migration

Authored by:

Ajit Aloz

Head of Cloud Practice, Anunta Tech

Introduction

It's no secret that businesses face enormous pressure to move workloads from on-prem data centers to the cloud. More than 90 percent of businesses already use the cloud, which offers unparalleled scalability and cost-efficiency, for at least some of their workloads.

Yet moving data and applications smoothly from on-prem environments into the cloud remains a major challenge. Although public cloud platforms offer the same core types of resources -- such as virtual machines, data storage, firewalls and identity management services -- as companies typically deploy on-premises, moving workloads into the cloud is rarely a lift-and-shift affair.

Instead, migrating data centers into the cloud requires careful evaluation of current workloads and validation of plans for moving them to the public cloud. Organizations must also take care to execute the migration in a way that guards against data loss and business discontinuity.

Before planning a data center migration, then, businesses must consider how they will address the various challenges that are inherent in the migration process. To help with that task, this whitepaper identifies the eight major pain-points companies can expect to face during data center migration and explains how to address them in order to ensure a smooth, efficient and effective migration into the cloud.

Challenge 1: Migrating Virtual Machines

You may assume that, if your on-prem workloads are already hosted inside virtual machines (VMs), moving them to the cloud will be a relatively simple affair. After all, VMs are a standard resource in public clouds. It's easy to launch as many VMs as you need on a public cloud platform.

However, in many cases VMs from a private data center can't simply be dragged-and-dropped into a cloud environment, for several reasons:

- **VM resource requirements:** On-prem VMs may have higher or lower virtual resource requirements than those that will run in the cloud. You must carefully evaluate the VM instance types available in the cloud to determine which one is the best fit for each on-prem virtual machine.
- **VM platform differences:** When you move to the cloud, you may wish to migrate to a different platform -- from VMware ESX to Microsoft Hyper V, for instance -- in order to take advantage of integrations or features that are available on one platform but not another. When you switch platforms, seamless migration along with application integration and non stop business continuity is of utmost importance.
- **Configuration requirements:** If you change a VM type, you may also need to change the operating system configuration on that VM to match new virtual hardware settings.
- **Bare-metal options:** Sometimes, you may wish to take advantage of bare-metal instance types in the cloud rather than running all of your workloads in VMs. This is yet another complex option to assess.

If your VM configurations are very basic, it may be possible simply to clone on-prem VMs and launch new VMs in the cloud based on those cloned images. In many cases, however, the VM migration process requires in-depth evaluation of what the business needs to achieve from its cloud VMs, followed by a VM conversion process that entails rebuilding some or all VMs from scratch.

Challenge 2: Migrating Applications

Applications fall into two main categories: Line-of-business apps that businesses build and maintain in-house, and third-party applications (like office or accounting software) that they obtain from vendors.

Both types of applications typically require at least some configuration changes in order to move smoothly into the cloud. In-house applications that were designed to run on-prem may need to be refactored significantly to integrate with cloud storage, networking and other services.

Third-party apps are more likely to be able to move relatively easily into the cloud, provided that the app vendor designs the apps to be cloud-friendly. But even in that case, third-party apps may require changes to networking, storage and other settings in order to support the new cloud environment.

These application changes can be managed. But here again, businesses must carefully assess the state of their on-prem applications, determine the extent to which they are compatible with cloud environments and implement the changes necessary to make applications work reliably in the cloud.

Challenge 3: Data Migration

Moving large volumes of data from a local data center into the cloud can be challenging for two reasons: The time it takes to move data across the Internet, and the danger of data loss or corruption that could occur during the migration process.

The first challenge can be addressed by strategically evaluating which data needs to move to the cloud and which techniques (such as data compression) can be used to minimize the time it takes to move that data over the network. Simply attempting to copy all data in wholesale fashion from the data center to the cloud is rarely the best approach.

At the same time, it's critical to perform data migration in a way that minimizes the risk of data problems. The ideal approach is to keep all local data intact while the migration process is being carried out. Then, the cloud-based and on-prem copies of the data must be carefully compared to ensure that they are identical. In addition, any changes to the on-prem data that may have occurred since the migration process began must be addressed to ensure that both copies of data remain in sync.

Only after cloud data has been fully validated and synced can the on-prem data be disconnected and production operations moved to the cloud.

Challenge 4: Network Migration

On-prem data center networks and cloud networks tend to look quite different. In a data center, businesses have full control over physical network infrastructure. Resources are not exposed by default to the public Internet.

In the cloud, physical networking devices are replaced by software-defined constructs like cloud firewalls. Segmenting workloads from the Internet requires the setup of Virtual Public Clouds (VPCs) and firewall rules that manage traffic appropriately between VPCs. Cloud VPNs may need to be deployed to allow resources that remain on-prem to connect securely with those running in the cloud. Cloud load balancers must be configured to ensure reliable routing of traffic within the cloud environment.

In short, migrating network configurations from a data center to the cloud typically requires a major overhaul of network setup. Businesses need to determine how their cloud networks should be designed in order to meet the performance and security requirements of their workloads using the network services that public clouds provide, which in many respects look very different from those you would find in your own data center.

Challenge 5: License Management

The software licenses that businesses use in their own data centers may or may not be applicable to the cloud. Although in general the same operating system and application licenses can be used both on-prem and in the cloud, licenses associated with VM platforms, SaaS applications or applications that use a site-license model to make software available on a local network may need to be updated or replaced when companies move to the cloud.

Reviewing existing license configurations and determining where changes are required is therefore a crucial step in moving seamlessly to the cloud. You don't want to migrate your workloads only to discover that licensing issues disrupt your productivity.

Challenge 6: Identity Management

Most businesses use a directory service like Active Directory to manage user accounts and roles across their IT environments. In most cases, Active Directory can be used to govern resources in the cloud as well.

However, Active Directory configurations that were designed only for a local data center typically must be updated to ensure compatibility with cloud services. Businesses may also need to extend their Active Directory architecture so that it includes multiple databases, one for their resources that remain on-prem and another for their public cloud environment.

On top of this, companies must ensure that any applications or services that they deploy in the cloud, and that rely on a directory service to authenticate and authorize their users, are properly integrated with their Active Directory databases. Otherwise, employees may not be able to access the cloud-based resources they need.

Challenge 7: Compliance

Compliance is a complex and fast-evolving domain. Moving to the cloud makes it even more complicated.

In some cases, businesses may face data residency requirements that mandate that they select certain cloud regions for storing data and applications. They may also be subject to security rules that require certain network security policies to protect their workloads. They may need to implement cloud data loss prevention (DLP) services to meet data privacy compliance rules.

Compliance is thus another context in which it's critical to review business needs, determine how the data center migration will impact them and then take steps to ensure a migration that addresses compliance requirements.

Challenge 8: Cost Optimization

The cloud holds great potential for saving businesses money by allowing them to pay for only the resources they need. But achieving the full cost-savings potential of the cloud requires careful preparation.

Companies must determine which data storage tiers -- hot, cold or archive -- are the best fit for their cloud storage requirements, based on the performance and cost implications of these options. They must ensure that they select VM instances that deliver the performance their workloads require, but that don't waste resources and lead to unnecessary costs. They must plan cloud architectures that minimize data egress fees.

In short, businesses must carefully assess the cloud services and configurations available to them to determine which ones are the best fit for their cost requirements.

Anunta: Your data center migration partner

Data center migration is a tremendously complex process. When performed without proper planning, validation and risk-management, moving workloads to the cloud may cause more problems than it solves for the business.

Overcome these challenges by choosing Anunta as your data center migration partner. For more than ten years, Anunta has been helping companies across a variety of industries move their workloads to the cloud. Anunta's team boasts extensive expertise with a variety of cloud platforms -- Amazon Web Services, Azure, Google Cloud and more -- as well as different VM platforms.

When Anunta manages your data center migration, you'll benefit from a strategy that focuses not just on the fastest way to migrate your workloads to the cloud, but also an approach that will deliver the most cost-effective cloud setup in the long run. At the same time, Anunta strives to ensure that migration has minimal impact on your employees and customers: They won't even know that your systems have moved to the cloud because service disruption is minimal.

What's more, Anunta's services don't stop with planning and executing data center migration. Anunta also delivers ongoing support to help businesses manage and grow their cloud environments over time as needs and opportunities change.

About the Author

Ajit Aloz is Head of Cloud Practice at Anunta. He has over two decades of experience in the IT/ITes industry. His expertise lies in cloud computing technologies.

anunta®

About Anunta

Anunta is an industry-recognized Managed Desktop as a Service provider focused on Enterprise DaaS, Packaged DaaS, and Digital Workspace technology. We have successfully migrated 500,000+ remote desktop users to the cloud for enhanced workforce productivity and superior end-user experience.

For more information about Anunta, visit www.anuntatech.com

For sales inquiry, reach out to us at: sales@anuntatech.com

Follow us on: