


Multiple geographic regions

04/04/2019 • 12 minutes to read • Contributors 

In this article

- [General scope expansion](#)
- [Implementing the general approach](#)
- [Suggested prerequisites](#)
- [Assess process changes](#)
- [Migrate process changes](#)
- [Optimize and promote process changes](#)
- [Next steps](#)

When businesses operate in multiple geographic regions, additional complexity can be introduced into cloud migration efforts. These complexities manifest in three primary forms: asset distribution, user access profiles, and compliance requirements. Before addressing complexities related to multiple regions, it's important to understand the extent of the potential complexity.

General scope expansion

The following approach can help assess the potential challenges and establish a general course of action:

- Consider a more robust readiness and governance implementation.
- Inventory the affected geographies. Compile a list of the regions and countries that are affected by the cloud migration.
- Document data sovereignty requirements: Do the countries identified have compliance requirements that govern data sovereignty?
- Document the user base: Will employees, partners, or customers in the identified country be affected by the cloud migration?
- Document datacenters and assets: Are there assets in the identified country that might be included in the migration effort?

Align changes across the migration process to address the initial inventory.

Documenting complexity

The following table can aid in documenting the findings from the steps above:

Region	Country	Local Employees	Local External Users	Local Datacenters or Assets	Data Sovereignty Requirements
North America	USA	Yes	Partners and customers	Yes	No
North America	Canada	No	Customers	Yes	Yes
Europe	Germany	Yes	Partners and customers	No - Network only	Yes
Asia Pacific	South Korea	Yes	Partners	Yes	No

Why is data sovereignty relevant?

Around the world, government organizations have begun establishing data sovereignty requirements, like General Data Protection Regulation (GDPR). Compliance requirements of this nature often require localization within a specific region or even within a specific country to protect their citizens. In some cases, data pertaining to customers, employees, or partners must be stored on a cloud platform within the same region as the end user.

Addressing this challenge has been a significant motivation for cloud migrations for companies that operate on a global scale. To maintain compliance requirements, some companies have chosen to deploy duplicate IT assets to cloud providers within the region. In the example table above, Germany would be a good example of this scenario. In this example, there are customer, partners, and employees in Germany, but no existing IT assets. This company may choose to deploy some assets to a datacenter within the GDPR area, potentially even using the German Azure datacenters. An understanding of the data affected by GDPR would help the Cloud Adoption team understand the best migration approach in this case.

Why is the location of end users relevant?

Companies that support end users in multiple countries have developed technical solutions for addressing end user traffic. In some cases, this involves localization of assets. In other scenarios, the company may choose instead to implement global WAN solutions to address disparate user bases via network focused solutions. In either case, the migration strategy could be affected by the usage profiles of those disparate end users.

Since the company supports employees, partners, and customers in Germany but there are no datacenters currently in that country, it's very likely that this company has implemented some form of leased-line solution to route that traffic to datacenters in other countries. This existing routing presents a significant risk to the perceived performance of migrated applications. Injecting additional hops in an established and tuned global WAN can create the perception of underperforming applications after migration. Finding and fixing those issues can add significant delays to a project. In each of the processes below, guidance for addressing this complexity is included across prerequisites, assess, migrate, and optimize processes. Understanding user profiles in each country is critical to properly manage this complexity.

Why is the location of datacenters relevant?

The location of existing datacenters can affect a migration strategy. The following are a few of the most common impacts:

Architecture decisions: Target region/location is one of the first steps in migration strategy design. This is often influenced by the location of the existing assets. Additionally, the available of cloud services and the unit cost of those services can vary from one region to the next. As such, understanding the current and future location of assets affects the architecture decisions and can also affect budget estimates.

Datacenter dependencies: Based on the data in the table above, there is a high likelihood of dependencies existing between the various datacenters around the globe. In many organizations which operate on this type of scale, those dependencies may not be documented or well understood. The approaches used to evaluate user profiles will help identify some of these dependencies. However, additional steps are suggested during the assess process to mitigate risks associated with this complexity.

Implementing the general approach

This approach is driven by quantifiable information. As such, the following approach will follow a data-driven model for addressing the global migration complexities.

Suggested prerequisites

It is suggested that the Cloud Adoption team begin with the migration of a simple workload using the [Azure migration guide](#), before attempting to address global scale. This will ensure the team is familiar with the general process of cloud migration prior to attempting a more complex migration scenario.

When scope for a migration includes multiple regions, the following readiness considerations should be evaluated by the Cloud Adoption team:

- Data sovereignty might require localization of some assets, but there are many assets that may not be governed by those compliance constraints. Things like logging, reporting, network routing, identity, and other central IT services may be eligible to be hosted as a shared services across multiple subscriptions or even multiple regions. It is advised that the cloud adoption team evaluate a share service model to those services, as outlined in the [reference architecture for a hub and spoke topology with shared services](#)
- When deploying multiple instances of similar environments, an environment factory could create consistency, improve governance, and accelerate deployment. The [large enterprise governance journey](#) establishes an approach that creates an environment factory which scales across multiple regions.

Once the team is comfortable with the baseline approach and readiness is aligned, there are a few data-driven prerequisites to consider:

- **General discovery:** Complete the [Documenting complexity](#) table above.
- **Perform a user profile analysis on each affected country:** It is important to understand general end user routing early in the migration process. Changing global lease lines and adding connections like ExpressRoute to a cloud datacenter can require months of networking delays. Address this as early in the process as possible.
- **Initial digital estate rationalization:** Any time complexity is introduced into a migration strategy, an initial digital estate rationalization should be completed. See the guidance on [digital estate rationalization](#) for assistance.
 - **Additional digital estate requirements:** Establish tagging policies to identify any workload affected by data sovereignty requirements. Required tags should begin in the digital estate rationalization and carry through to the migrated assets.
- **Evaluate a hub and spoke model:** Distributed systems often share common dependencies. Those dependencies can often be addressed through the implementation of a hub and spoke model. While such a model is out of scope for the migration process, it should be flagged for consideration during future iterations of the [Ready processes](#).
- **Prioritization of the migration backlog:** When network changes are required to support the production deployment of a workload that supports multiple regions, it is important for the Cloud Strategy team to track and manage escalations regarding those network changes. The higher level of executive support will aid in accelerating the change. However, the more important impact is that it gives the strategy team an ability to reprioritize the backlog to ensure that global workloads aren't roadblocked by network changes. Such workloads should only be prioritized, after the network changes are complete.

These prerequisites will help establish processes that can address this complexity during execution of the migration strategy.

Assess process changes

When dealing with global asset and user base complexities, there are a few key activities that should be added to the assessment of any migration candidate. Each of these changes will bring clarity to the impact on global users and assets, through a data driven approach.

Suggested action during the assess process

Evaluate cross datacenter dependencies: The [dependency visualization tools in Azure Migrate](#) can help pinpoint dependencies. Use of this tool set prior to migration is a good general best practice. However, when dealing with global complexity it becomes a necessary step to the assessment process. Through [dependency grouping](#), the visualization can help identify the IP addresses and ports of any assets required to support the workload.

Important

Two important notes: First, a subject matter expert with an understanding of asset placement and IP address schemas is required to identify assets that reside in a secondary datacenter. Second, it is important to evaluate both downstream dependencies and Clients in the visual to understand bidirectional dependencies.

Identify global user impact: The outputs from the prerequisite user profile analysis should identify any workload affected by global user profiles. When a migration candidate is in the affected workload list, the architect preparing for migration should consult networking and operations subject matter experts to validate network routing and performance expectations. At minimum, the architecture should include an ExpressRoute connection between the closest network operations center (NOC) and Azure. The [reference architecture for ExpressRoute](#) connections can aid in configuration of the necessary connection.

Design for compliance: The outputs from the prerequisite user profile analysis should identify any workload affected by data sovereignty requirements. During the architecture activities of the Assess process, the assigned architect should consult compliance subject matter experts to understand any requirements for migration/deployment across multiple regions. Those requirements will significantly affect design strategies. The reference architectures for [multiregion web applications](#) and [multiregion n-tier applications](#) can aid in design.

Warning

When using either of the reference architectures above, it may be necessary to exclude specific data elements from replication processes to adhere to data sovereignty requirements. This will add an additional step to the promotion process.

Migrate process changes

When migrating an application that must be deployed to multiple regions, there are a few considerations the Cloud Adoption team must take into account. These considerations consist of Azure Site Recovery vault design, configuration/process server design, network bandwidth designs, and data synchronization.

Suggested action during the migrate process

Azure Site Recovery vault design: Azure Site Recovery is the suggested tool for cloud-native replication and synchronization of digital assets to Azure. Site Recovery replicates data about the asset to a Site Recovery vault, which is bound to a specific subscription in a specific region and Azure datacenter. When replicating assets to a second region, a second Site Recovery vault may be required.

Configuration/process server design: Site Recovery works with a local instance of a configuration and process server, which is bound to a single Site Recovery vault. This means that a second instance of these servers may need to be installed in the source datacenter to facilitate replication.

Network bandwidth design: During replication and ongoing synchronization, binary data is moved over the network from the source datacenter to the Site Recovery vault in the target Azure datacenter. This process consumes bandwidth. Duplication of the workload to a second region will double the amount of bandwidth consumed. When bandwidth is limited or a workload involves a large amount of configuration or data drift, it can interfere with the time required to complete the migration. More importantly, it could affect the experience of users or applications that still depend on the bandwidth of the source datacenter.

Data synchronization: Often the largest bandwidth drain comes from synchronization of the data platform. As defined in the reference architectures for [multiregion web applications](#) and [multiregion n-tier applications](#), data synchronization is often required to keep the applications aligned. If this is the desired operational state of the

application, it may be wise to complete a synchronization between the source data platform and each of the cloud platforms before migrating the application and middle tier assets. **Data synchronization:** Often the largest bandwidth drain comes from synchronization of the data platform. As defined in the reference architectures for [multiregion web applications](#) and [multiregion n-tier applications](#), data synchronization is often required to keep the applications aligned. If this is the desired operational state of the application, it may be wise to complete a synchronization between the source data platform and each of the cloud platforms before migrating the application and middle tier assets.

Azure to Azure disaster recovery: There is an alternative option that may reduce complexity further. If timelines and data synchronization approaches approach a two-step deployment, [Azure to Azure disaster recovery](#) could be an acceptable solution. In this scenario, the workload is migrated to the first Azure datacenter using a single Site Recovery vault and configuration or process server design. Once the workload is tested, it can then be recovered to a second Azure datacenter from the migrated assets. This approach reduces the impact to resources in the source datacenter and takes advantage of faster transfer speeds and high bandwidth limits available between Azure datacenters.

ⓘ Note

This approach may increase the short-term cost of migration, because it could result in additional egress bandwidth charges.

Optimize and promote process changes

Addressing global complexity during optimization and promotion could require duplicated efforts in each of the additional regions. When a single deployment is acceptable, duplication of business testing and business change plans may still be required.

Suggested action during the optimize and promote process

Pretest optimization: Initial automation testing can identify potential optimization opportunities, as with any migration effort. In the case of global workloads, it is important to test the workload in each region independently, as minor configuration changes in the network or the target Azure datacenter could affect performance.

Business Change Plans: For any complex migration scenario, it is advised that a business change plan be created to ensure clear communication regarding any changes to business processes, user experiences, and timing of the efforts required to integration the changes. In the case of global migration efforts, the plan should include considerations for end users in each affected geography.

Business testing: In conjunction with the business change plan, business testing may be required in each region to ensure adequate performance and adherence to the modified networking routing patterns.

Promotion flights: Often promotion happens as a single activity, rerouting production traffic to the migrated workloads. In the case of global release efforts it is advised that promotion be delivered in flights (or predefined collections of users). This allows the Cloud Strategy team and Cloud Adoption team to better observe performance and improve support of users in each region. Promotion flights are often controlled at the networking level by changing the routing of specific IP ranges from the source workload assets to the newly migrated assets. After a specified collection of end users have been migrated, the next group can be rerouted.

Flight optimization: One of the benefits of promotion flights, is that it allows for deeper observations and additional optimization of the deployed assets. After a brief period of production usage by the first flight, additional refinement of the migrated assets is suggested, when allowed by IT operation procedures.

Next steps

A separate point of complexity, often related to multiple regions, is the need to prepare for the migration of [multiple datacenters](#). While very similar in nature, this complexity deals with the volume of assets to be migrated when moving multiple datacenters to the cloud.

Migrating multiple datacenters