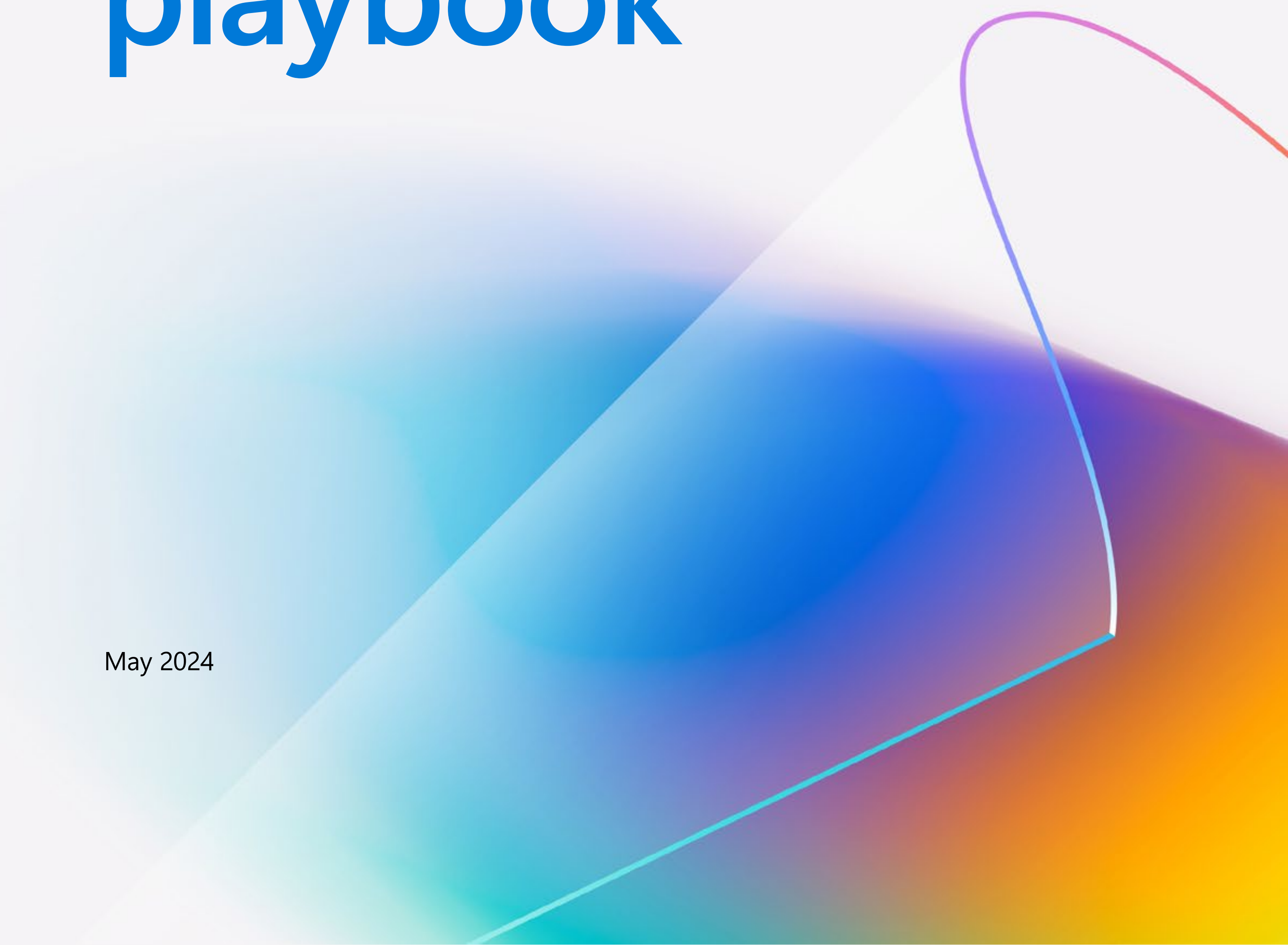
Microsoft Azure

New Zealand cloud region playbook



May 2024

The upcoming launch of the New Zealand cloud region represents a tremendous opportunity. By storing and processing your data on shore, you can meet your data residency and compliance obligations, reduce the latency of your workloads, and meet your sustainability commitments.

This document provides some specific guidance for New Zealand North, which is the name of the New Zealand cloud region.

The guidance is centred around two key parts:

1. Three common scenarios, which collectively represent many of the use cases for New Zealand North.
2. A set of guidance about technical topics to help you to plan your use of the new region.

Table of contents

What is New Zealand North?

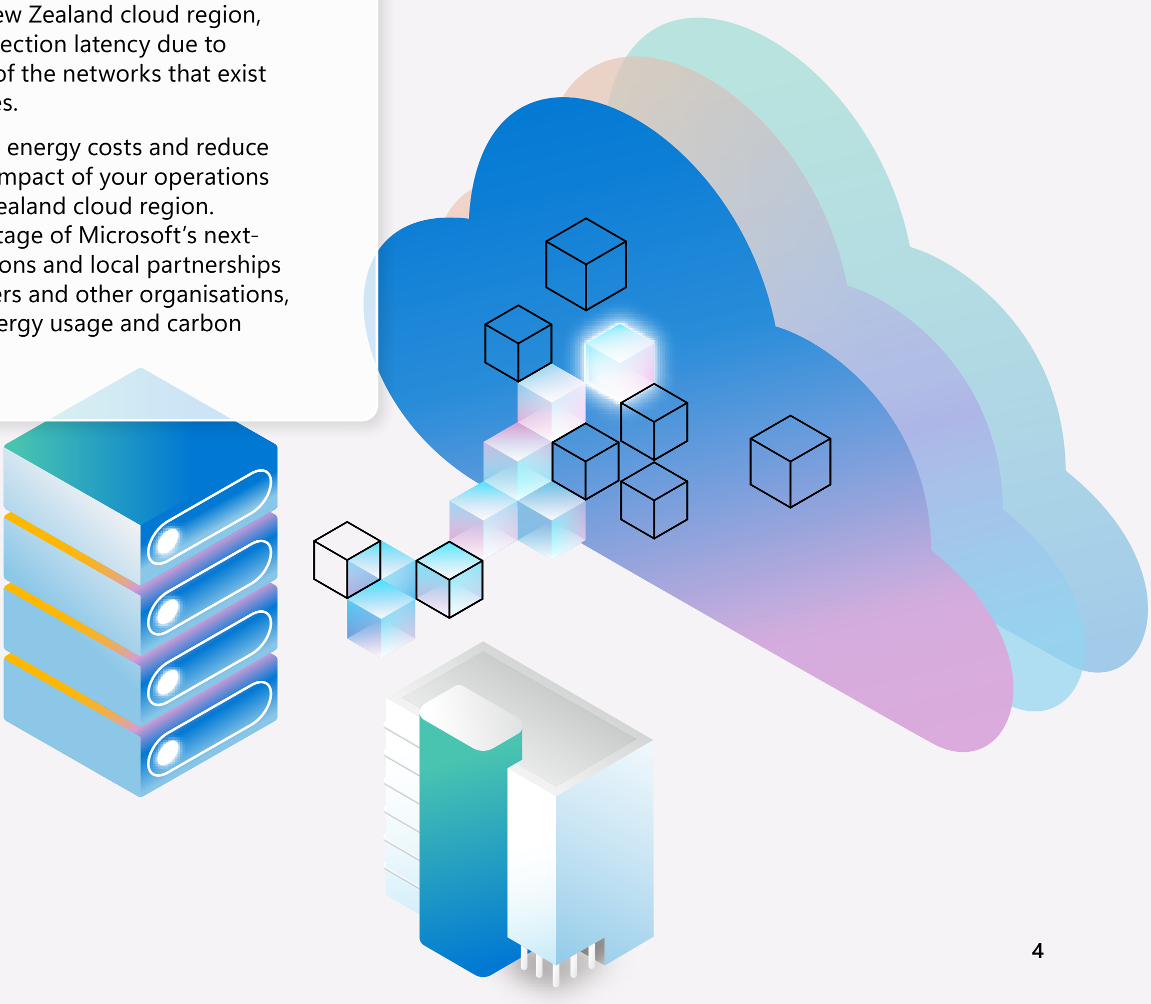
Many Microsoft cloud services will be available from the New Zealand cloud region including Microsoft Azure, as well as most of the Microsoft 365 and Microsoft Dynamics services.

By using the New Zealand cloud region, you gain several benefits:

- **Data residency:** You can honour your data residency commitments by storing and processing data within New Zealand's borders. By using the New Zealand cloud region, you can meet your regulatory and cultural data requirements.
- **Security and compliance:** Protect your business with local, regional, and global security offerings. Additionally, if you work with sensitive data, you are likely to have heightened security and compliance requirements.
- **Latency:** Increase your efficiency with faster network connectivity and lower latency between local datacentres and the cloud. You can choose to build a hybrid environment that includes the New Zealand cloud region, which reduces connection latency due to distance or quality of the networks that exist between datacentres.
- **Sustainability:** Save energy costs and reduce the environmental impact of your operations by using the New Zealand cloud region. You can take advantage of Microsoft's next-generation innovations and local partnerships with energy providers and other organisations, and reduce your energy usage and carbon emissions.

It's important to know that the New Zealand North region is more than just a datacentre. The region includes three *availability zones*, which are distinct physical locations that are close enough to have low-latency connections to other availability zones, but are far enough apart to reduce the likelihood that more than one will be affected by local outages or weather. Availability zones have independent power, cooling, and networking infrastructure. They're designed so that if one zone experiences an outage, then regional services, capacity, and high availability are supported by the remaining zones.

In addition, every region includes extensive networking infrastructure that enables both public and private connectivity from your environments to the Microsoft cloud. The New Zealand cloud region is connected to Microsoft's global wide area network (WAN), which provides high-bandwidth, low-latency connectivity to other Azure regions internationally.



Common scenarios

Scenario 1:
Green field, new deployment

If you're new to Azure, you might consider deploying your workloads directly into New Zealand North.

Key questions to ask

When you're deploying a new Azure estate to New Zealand North, here are some questions that are useful to ask:

- **What are your timelines?** Services in New Zealand North will become available in stages. If you have a hard deadline, you need to ensure that it fits within the launch timelines and allows for contingency. For more information, see Service availability and timelines.
- **Which services will you use?** All foundational and mainstream Azure services will be deployed in New Zealand North. Strategic services will be deployed in NZ based on local demand. As part of your solution planning, you will need to understand service availability and timelines. If your solution uses third-party services from the Azure Marketplace, you will need to clarify with the ISV when it will be available in New Zealand North.
- **How are you likely to grow your use of services within the region?** To plan our capacity for the region, Microsoft needs to track the estimated growth in service usage. Please make sure to discuss your expected use with Microsoft or your key partner.
- **What are your requirements for high availability and disaster recovery?** It's important to understand that New Zealand North has three independent availability zones, and that you've fully considered how to use availability zones in your solution architecture.
- **Are you planning to use multiple regions?** For example, you might plan a global expansion of your business, or to support international employees or business partners. Such a strategy might result in the use of other Azure regions in addition to New Zealand North.

Key actions

- **Understand the services and SKUs** that you intend to use, and verify they are supported in the region. For more information, see Service availability and timelines.
- **Plan the HA and DR strategy,** and confirm your team is comfortable architecting with availability zones. For more information, see Availability zones, zone redundancy, and zonal services.
- **Decide on a connectivity approach.** For more information, see Connectivity to on-premises environments.
- **Establish a landing zone and use New Zealand North for regional components.** For more information, see Landing zones.

Scenario 2:
Brown field, multi-region

You might have an existing Azure estate that uses other regions. When you plan a new component or workload, you can deploy it to New Zealand North.

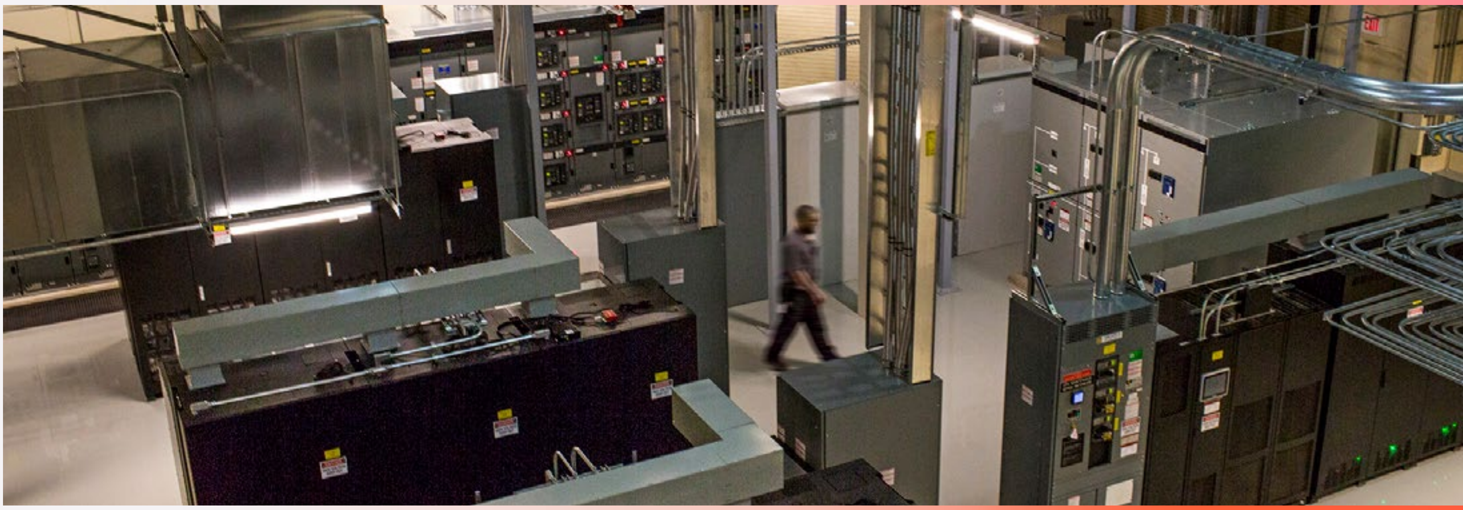
Key questions to ask

If you have an Azure estate in another region and are thinking about deploying a new Azure workload to New Zealand North, here are some questions that are useful to ask:

- **What are your timelines?** Services in New Zealand North will become available in stages. If you have a hard deadline, you need to ensure that it fits within the launch timelines and allows for contingency. For more information, see Service availability and timelines.
- **Which services will you use?** All foundational and mainstream Azure services will be deployed in New Zealand North. Strategic services will be deployed in NZ based on local demand. As part of your solution planning, you will need to understand service availability and timelines. If your solution uses third-party services from the Azure Marketplace, you will need to clarify with the ISV when it will be available in New Zealand North.
- **What are your requirements for high availability and disaster recovery?** Confirm that you understand how New Zealand North's availability zone-based architecture works, and that you've in the solution architecture and that they've fully considered how to use availability zones in their solution architecture.

Key actions

- **Understand the services and SKUs** that you intend to use, and verify they are supported in the region. For more information, see Service availability and timelines.
- **Plan the HA and DR strategy,** and confirm that your team is comfortable architecting with availability zones. For more information, see Availability zones, zone redundancy, and zonal services.
- **Plan how connectivity to the new region will work.** For example, you might deploy additional ExpressRoute circuits, upgrade an existing circuit, or deploy a new site-to-site VPN. For more information, see Connectivity to on-premises environments. You might also need to plan cross-region connectivity.
- **Plan how the your landing zone will be extended to the new region.** For more information, see Landing zones.



Scenario 3: Brown field, repatriation

If you already have workloads in another region, you might be interested in repatriating those workloads to New Zealand North when it's available. Generally, the workloads are deployed to Australia East or Australia Southeast, but they might be deployed to other regions and the same considerations apply.

Key questions to ask

When you consider repatriating some or all of your Azure estate to New Zealand North, here are some questions that are useful to ask:

- **What's your motivation?** You might be interested in service availability, legal/regulatory compliance, data residency, performance optimisation, or potentially simply a feel-good factor of having your workloads running locally. Understanding the motivation helps to ensure that you get the right guidance.
- **What's the timeline?** If your relocation isn't time-critical, consider whether you can perform the relocation alongside other changes to the solution, which might reduce the overall effort involved.
- **What's the scope of the workload to be repatriated?** Are you aiming to move all of your Azure resources, those resources related to a specific workload/solution, or just a single resource?
- **Have you considered other alternatives to repatriation?** Other alternatives might include the following:
    - Build a multi-region solution by keeping existing resources and deploying to a new region, or (where supported) adding a new region to the existing resource. While this might not fit all situations it can be a good strategy for SaaS and eCommerce solutions, which need to expand globally.
    - Use global routing. Keep the application in its current region, and use Azure Front Door or a global layer 4 load balancer to route requests across the Microsoft global network for global performance acceleration and security. For more information, see Network secure ingress implementation.
    - **How will the migration be sequenced?** You might decide to move everything together, or to move sets of resources together (such as an entire tier of a solution), or to move individual components. If you plan to migrate in stages, will you have resources that need to be accessed from both regions? How will the latency affect the application performance during the period when you run across two regions?
- **Are there components that can't be migrated?** For example, Log Analytics and Azure Backup data can't be moved across regions. If you need to retain logs or backups for a specific duration, you might have to keep the resources in the old region until that duration has passed. This might, in turn, introduce operational complexity if those logs or backups need to be accessed.
- **When will they have landing zone components established in New Zealand North?** Consider the landing zone components that you need to deploy before migrating a workload.
- **Who will do the migration activities?** Will a partner be engaged? Will you migrate resources yourselves, or use the partner's skills to execute the migration?
- **Can the migration be rehearsed?** It is always ideal, when possible, to conduct a rehearsal of a migration. Ideally using a region with 3 Availability Zones which will mirror what we have in New Zealand.
- **Is the migration a good opportunity to resolve any outstanding technical debt or to make other improvements?** Common examples include:
    - Improvements to monitoring: Can you ensure they have monitoring enabled for your important resources, and that your team understands the telemetry as well as how to respond to alerts?
    - Testing: If you're building a test environment to validate the migration, can you make the same scripts/processes available for other tests in the future?
    - Automation: If you are rebuilding the environment anyway, can you follow best practices and deploy the infrastructure as code, use modern DevOps practices, and automate their deployment and management as much as practicable?
    - Availability zones: Can you make use of availability zones in their solution, if you don't already? Many resources must be configured for availability zones when they're first created, so a migration presents a great opportunity to remediate any configuration that needs to be adjusted.
    - Disaster Recovery or DR: Can you take lessons from the migration process and apply them to your disaster recovery plan?

Understand how cross-region moves work

There isn't a single approach to moving resources across regions. Some Azure resource types provide built-in support for cross-region moves, while others need to be recreated or migrated by using a tool like Azure Migrate. To execute a move, you'll need to make a plan that considers each resource type that you use. Azure Region Mover can help to move some types of Azure resources between regions. We provide guidance for moving many common Azure resource types. In general, stateful resources are more complex to move than stateless resources.

Key actions

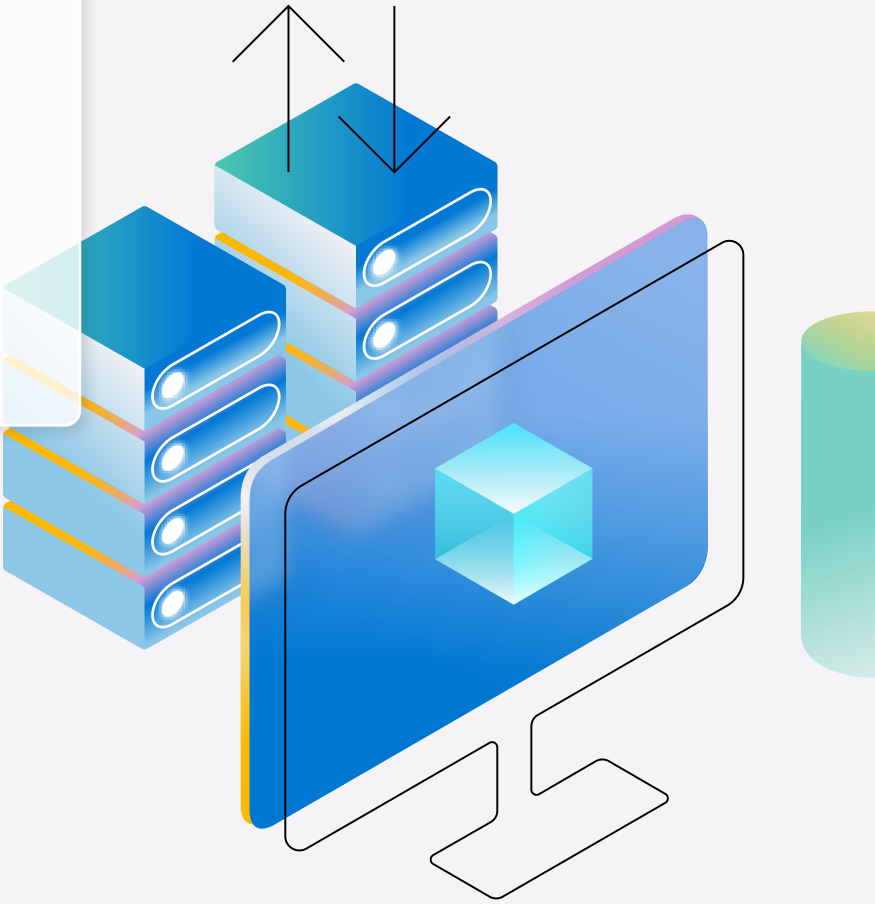
- **Understand the services and SKUs** that you intend to use, and verify they are supported in the region. For more information, see Service availability and timelines.
- **Plan the HA and DR strategy,** and confirm you are comfortable architecting with availability zones. For more information, see Availability zones, zone redundancy, and zonal services.
- **Ensure that you have a support contract** with an appropriate SLA, and that your team knows how to open support cases. During a migration of a production solution, you need to be able to quickly reach Azure Support.
- **Verify the permissions in the Azure environment,** including who can create subscriptions, who can set up peerings between virtual networks, and so forth.
- **Plan how your landing zone will be moved to the new region.** For more information, see Landing zones.
- **Plan how connectivity to the new region will work.** For example, you might deploy additional ExpressRoute circuits, upgrade an existing circuit, or deploy a new site-to-site VPN. For more information, see Connectivity to on-premises environments.

Considerations

- Consider latency, and whether the application is sensitive to latency. This might influence the strategy and process.
- For many Azure services, DNS names and IP addresses might change when you move across regions.
- Resource names and resource IDs are very likely to change. Verify whether you have any automation that depends on finding resources with a specific name or resource ID.
- Azure Reservations are regionally scoped, but can be exchanged for new reservations in another region.

Resources

- Cloud Adoption Framework relocation guidance
- Migrating Azure services to new regions
- Azure Region Mover can help to move some types of Azure resources between regions.
- We provide guidance for moving many common Azure resource types.



Key technical areas

Service availability and timelines

Key points:

- Services will be released to New Zealand North progressively, over a period of several months. Ensure you understand which services you use, and plan based on availability timeframes.
- You might need to plan workarounds if you need to use services that aren't available immediately upon region launch.

If you plan for a deployment into New Zealand North, you should be aware of the service availability and sequencing.

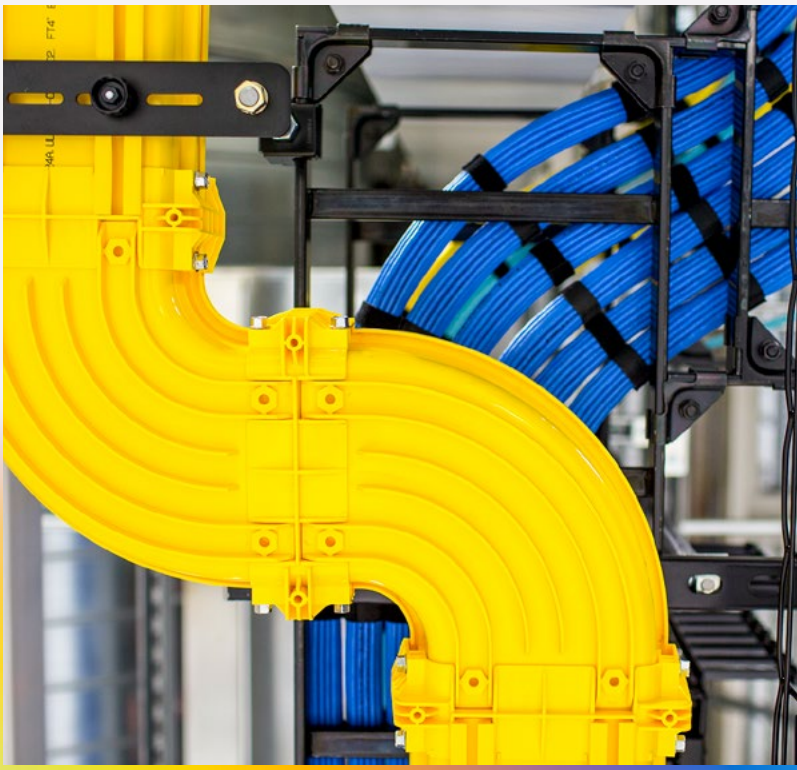
Azure services are released to new regions on an ongoing basis. Azure assigns service categories as foundational, mainstream, and strategic. For a list of the services in each category, see Available services by region types and categories. It's important to understand the deployment timelines:

- **All foundational services** will be available as soon as the region is publicly available.
- **All mainstream services** will be deployed to the region, but might not be available immediately. Check with your Microsoft team on when services become available.
- **Strategic services** are deployed individually based on demand. Please discuss this process with your Microsoft team.

If you plan to use New Zealand North, it's critical that you evaluate the services and SKUs that you intend to use to ensure they will be available. If your project timelines require you to have access to services at a certain time contact your Microsoft account team. They can advise you on timelines, scope, and potential workarounds.

If you need to use services that aren't yet available, then you should make contingency plans. These plans might include:

- **Wait until your chosen set of services are available** in New Zealand North before they begin to deploy their workload. If you're building a new workload, consider whether you can deploy nonproduction environments in another region, and then plan to deploy your production services in New Zealand North when their services are ready.
- **Temporarily deploy your workload to another region** with the intention to repatriate it when your chosen services are ready. You might need to accept latency and cross-region traffic cost during the period of time you run across regions. If you follow this approach, review the guidance for repatriation for some important considerations.
- **Use a different service or SKU** that is available in New Zealand North, and then migrate to the desired service or SKU later.
- **Use a partner service,** such as a network virtual appliance (NVA), while waiting for an Azure-native service to become available. There are tradeoffs with each type of contingency plan. You, along with your partner, need to make an informed decision on the tradeoffs that are right for your scenario.



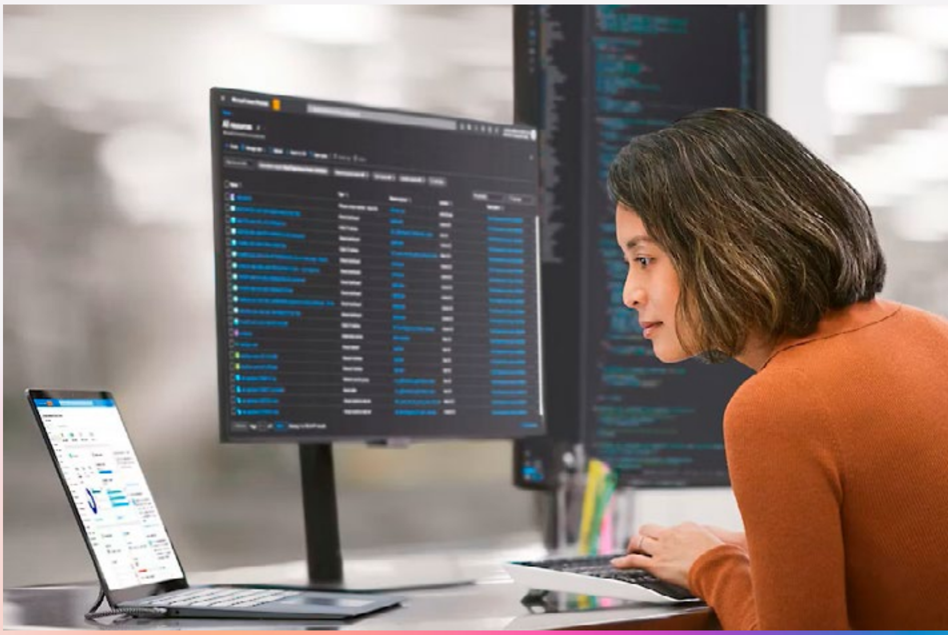
Service	Example Contingency Plan
Azure Cache for Redis	Deploy your own Redis cache on a virtual machine temporarily, and migrate to Azure Cache for Redis when it's available.
Azure Functions	Deploy your function app to Australia East, and then redeploy to New Zealand North when it's available.
Azure Monitor: Log Analytics	Send your Azure diagnostic and activity logs to a storage account in New Zealand. However, you can't easily query across logs in a storage account.
	Route your logs to a Log Analytics workspace in another region. However, you will pay cross-region traffic.
Azure Virtual WAN	Deploy a hub-and-spoke VNet in New Zealand North, and then migrate to Azure Virtual WAN when it's available.

Please work with your Microsoft account team to ensure that your demand for Azure services is recorded.

Important: Some of the components required by an enterprise-scale landing zone (ESLZ) are considered mainstream services. This means that a full ESLZ might not be deployable immediately upon region launch. You might need to implement workarounds temporarily.

Strategic services

Not all strategic services will be available in New Zealand North, for a variety of reasons. You might need to run some components of your workloads in other regions if there are specific services that aren't available locally. Alternatively, you might be able to redesign your deployments to use services that are supported in New Zealand North.



Availability zones, zone redundancy, and zonal services

Key points:

- Availability zones provide a high degree of redundancy and support resiliency for most workloads' requirements. They are the right choice for most Azure customers.
- Availability zones can be used to support a variety of types of workloads and requirements.
- Multi-region architectures should be considered when a workload has users who are globally distributed, or when you have a mission-critical system that means you are extremely risk averse, and you're prepared to accept the cost and complexity of a multi-region service.

New Zealand North has three independent availability zones. Availability zones are sets of datacentres that are fully isolated from each other. They're physically located far enough apart to reduce likelihood of an issue at one affecting another, but close enough together to allow synchronous replication between zones. For more information about how we design regions with availability zones, see [What are Azure regions and availability zones?]

For New Zealand North, there's no paired secondary region. It's important that you understand how to use availability zones and other approaches to achieve your resiliency requirements.

Zonal and zone-redundant deployments

There are two ways that resources might be configured to use availability zones. The option you use depends on the way the underlying Azure service works as well as your requirements.

- *Zonal resources* (also called *zone pinning*) are deployed into a specific availability zone. This approach doesn't inherently provide any sort of high availability or disaster recovery, but by deploying multiple resources across multiple availability zones you can achieve sophisticated availability requirements. You are responsible for handling data replication and failover, but this approach can work well for latency-sensitive workloads. Virtual machines are an example of a zonal resource.
- *Zone-redundant resources* have multiple instances that are deployed across multiple availability zones. Microsoft handles data replication and failover between zones. Many platform as a service (PaaS) services can be deployed in a zone-redundant configuration, such as App Service and Cosmos DB.

In general, we recommend that most production workloads should use multiple availability zones. If possible, use zone-redundant resources, which often give the best set of tradeoffs between resiliency, cost, and operational complexity.

To learn more about how to design a solution with zonal or zone-redundant deployments, and the tradeoffs in the different approaches, see [Recommendations for using availability zones and regions.]

Disaster recovery with availability zones and regions

A workload's disaster recovery strategy is heavily dependent on your business requirements. It's important you have a clear understanding of the business criticality of the system and the implications of downtime so you can make an informed decision about how they should plan for different types of failure.

Availability zones should play a significant role in your disaster recovery strategy. By spreading their workload across multiple availability zones, you mitigate many risks, such as a datacentre outage, power or network connectivity failure, or local weather events. The *Metro DR* approach is one way to use availability zones for disaster recovery, with zonal deployments that fail over to an alternative zone. Zone-redundant deployments also provide protection against many of these risks.

Occasionally, some workloads might be so critical that you want to consider mitigating the risk of an entire region outage. It's important to remember that region-wide outages are extremely unlikely. If you need to mitigate this kind of risk, you need to be prepared to deal with a more complex multi-region architecture. There are complex tradeoffs to consider involving latency, durability, and cost.

For most customers, availability zones provide the best set of tradeoffs to achieve high resiliency without introducing a lot of extra cost and complexity. We recommend most customers use availability zones as part of their primary resiliency approach, and consider cross-region data backups as an extra layer of protection.

Backups

Every customer's situation is unique, with several methods available for creating backups. The most common approach is utilising any of the three available zones within the New Zealand cloud region or backing up data to another Microsoft cloud region.

Shared responsibility principle

Resiliency is a shared responsibility. Microsoft provides availability zones and numerous other capabilities in the Azure platform to help you to design reliable solutions, but you need to ensure that your applications and workloads are designed to work correctly with the platform's resiliency capabilities.

Resources

- Recommendations for using availability zones and regions
- Availability zone mappings: Each subscription's availability zone order is different. This article describes how subscriptions are mapped to physical availability zones, and how you can safely use availability zones across subscriptions
- Well-Architected Framework reliability pillar, including Design reliable Azure applications
- Availability zone migration guidance overview for Microsoft Azure products and services

Availability zone-based reference architectures

The Azure Architecture Centre is building up a set of reference architectures that use availability zones, including the following:

- High availability enterprise deployment using App Services Environment
- IaaS: Web application with relational database
- Baseline highly available zone-redundant web application
- Azure Spring Apps baseline architecture

Connectivity to on-premises environments

Key points:

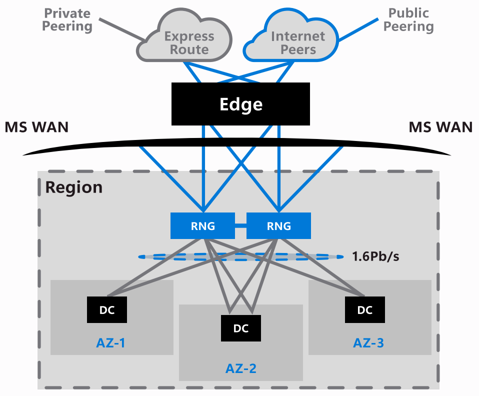
- ExpressRoute is a highly available service, with redundancy in each part of the Microsoft environment, including the Auckland points of presence (PoP). We provide two links for redundancy. You need to ensure that your equipment and configuration is ready for high availability.
- If you have a mission-critical workload and have low risk tolerance, you can mitigate the risk of PoP outages with a variety of approaches. This is not necessary for most customers.

You have multiple choices for how you connect your on-premises environments into Azure, including public internet connectivity, ExpressRoute, VPNs (point-to-site and site-to-site), and SD-WANs.

The Microsoft WAN

Microsoft's wide-area network provides connectivity across our global network of datacenters and edge sites. Each Azure region provides two regional network gateways (RNGs), which are redundant components that enable connectivity between all of the datacenters in the region as well as out to the global Microsoft network.

Traffic enters or leaves the Microsoft network at an edge location. We provide two types of edge locations, which are also called points of presence (PoPs). Public edge locations are used for connectivity across the internet, and private peering locations are used to support private connectivity through ExpressRoute.



ExpressRoute

ExpressRoute is often the preferred solution to connect your networks to Azure. You can use ExpressRoute today to connect to your Azure virtual networks and resources in Australia and beyond. When New Zealand North is launched, you can also use ExpressRoute to connect to resources deployed to that region. For a complete list of ExpressRoute connectivity partners in New Zealand, see Connectivity providers and locations for Azure ExpressRoute. You should contact your ExpressRoute partner to plan how they will create new circuits or move any existing circuits.

Auckland point of presence

Microsoft provides an ExpressRoute point of presence (PoP), also called a Microsoft Enterprise Edge (MSEE) location, in Auckland. The PoP is generally available now and is located at Vocus in Albany. Nothing about the PoP changes when the New Zealand North region is launched.

If you have virtual networks in New Zealand North, you'll be able to set up an ExpressRoute circuit in the region and then migrate to the new circuit. For more information, see How to approach migrating from one ExpressRoute circuit to another ExpressRoute circuit, with a focus on methodical transition of the ExpressRoute Private Peering.

Connectivity models

You can establish ExpressRoute circuits through a partner or by using ExpressRoute Direct. The Auckland ExpressRoute PoP supports partner connectivity and ExpressRoute Direct circuits.

ExpressRoute circuit SKUs

New Zealand and Australia share a geopolitical region, which means that ExpressRoute Standard circuits can connect to resources in either country. You can use global peering to connect virtual networks in Australia with those in New Zealand as required, and ExpressRoute can connect across the VNets.

ExpressRoute Local circuits will become available when the New Zealand North region is generally available. The Local circuit type will provide connectivity to the New Zealand North region only.

For more information about ExpressRoute circuit types, see Azure ExpressRoute pricing.

High availability

ExpressRoute is a highly available service, backed by a 99.95% uptime SLA. Microsoft's largest customers depend on ExpressRoute to connect their on-premises networks to Microsoft resources.

Microsoft builds high availability into each layer of the ExpressRoute connection. We provide two separate links for each circuit, each terminating in different physical hardware inside the PoP. If the primary link is unavailable the secondary link can continue to be used. Further, ExpressRoute PoPs are designed with a high degree of redundancy and resiliency.

High availability is a shared responsibility. You need to use both physical links, and test your configuration and failover regularly. You should deploy your ExpressRoute configuration based on our guidance for high availability. You must also ensure that your side of the connection doesn't have a single point of failure. Customer premises equipment (CPE) must be evaluated by your team, or a partner, to ensure that it supports your high availability requirements. At the application tier, workloads must be able to handle retries correctly, because short, intermittent outages of the ExpressRoute connection are normal and expected within the SLA.

Disaster recovery

Outages of an ExpressRoute PoP are extremely rare, and PoPs are specifically designed to ensure they remain operational even in a variety of failure conditions. Occasionally, some customers deploy mission-critical workloads, and have a lower risk tolerance. As part of a broader disaster recovery plan, they might look to mitigate the risk of an entire PoP failing. **For most customers, the cost-benefit ratio of mitigating this risk doesn't make sense,** and they are better to rely on the built-in resiliency of ExpressRoute as described above.

Customers with mission-critical workloads should have explicit, business-driven requirements that indicate the need to mitigate the risk of a PoP outage. These requirements might include a very low recovery time objective (RTO) or recovery point objective (RPO). In these situations, consider a variety of mitigations, each of which have tradeoffs, and remember that in a disaster scenario it's common to run a degraded experience. Mitigations you might consider include:

- Deploy a second ExpressRoute circuit, which will connect to another PoP in another region (typically Sydney or Melbourne). This option is fully described in the ExpressRoute disaster recovery guidance. Note that this approach will add latency due to cross-region traffic, but in a disaster scenario, added latency is often seen as a reasonable tradeoff.
- Use a site-to-site VPN as a fallback.
- Consider whether a software-defined WAN (SD-WAN) with a partner network virtual appliance (NVA) might provide an alternative connection path.
- Consider other fallback options based on the workload and your requirements, such as:
    - Use a virtual desktop (VDI) solution, which might be appropriate for low-latency workloads.
    - Deploy point-to-site VPN infrastructure, which users can connect to when their primary connectivity is unavailable. This approach can be more cost-effective than a site-to-site VPN.
    - Use a public endpoint and identity-based access controls.

Each mitigation option adds complexity and cost, so it's important to clearly identify whether there's a real need for such a mitigation before commencing. Many of our largest customers rely on a single ExpressRoute circuit.

Calls to action

- **Read our HA and DR guidance.** Specifically, read the ExpressRoute high availability guidance and disaster recovery guidance, and understand the ExpressRoute SLA.
- **Ensure you understand how to configure high availability for ExpressRoute** including using both physical links and using zone redundant gateways where applicable. You should test your configurations regularly.
- **Understand that your equipment (CPE) and application workloads are your responsibility.** If CPE isn't configured for high availability then your overall posture is compromised. Similarly, understand that application workloads that depend on ExpressRoute need to be designed to gracefully retry in the event of occasional connection dropouts.

If you have a mission-critical solution and a low risk tolerance, and the standard high availability PoP architecture is not sufficient:

- Verify that you have concrete, business-based requirements, such as an RTO and RPO. Ensure that your architectural decisions are grounded in these requirements and that you aren't overcomplicating their solution when you don't need to.
- Based on your requirements, if you need to mitigate the risk of a complete PoP outage, consider using the mitigations described above after fully evaluating their costs and benefits.

Resources

Review the following patterns for ExpressRoute high availability and resiliency:

- Connection weighting
- Autonomous system path pre-pending
- iBGP preferences
- iBGP or interior gateway protocols

You should always use bidirectional forwarding detection (BFD) to help to prevent lengthy failovers and unpredictable results when circuits flap.

Landing zones

Key points:

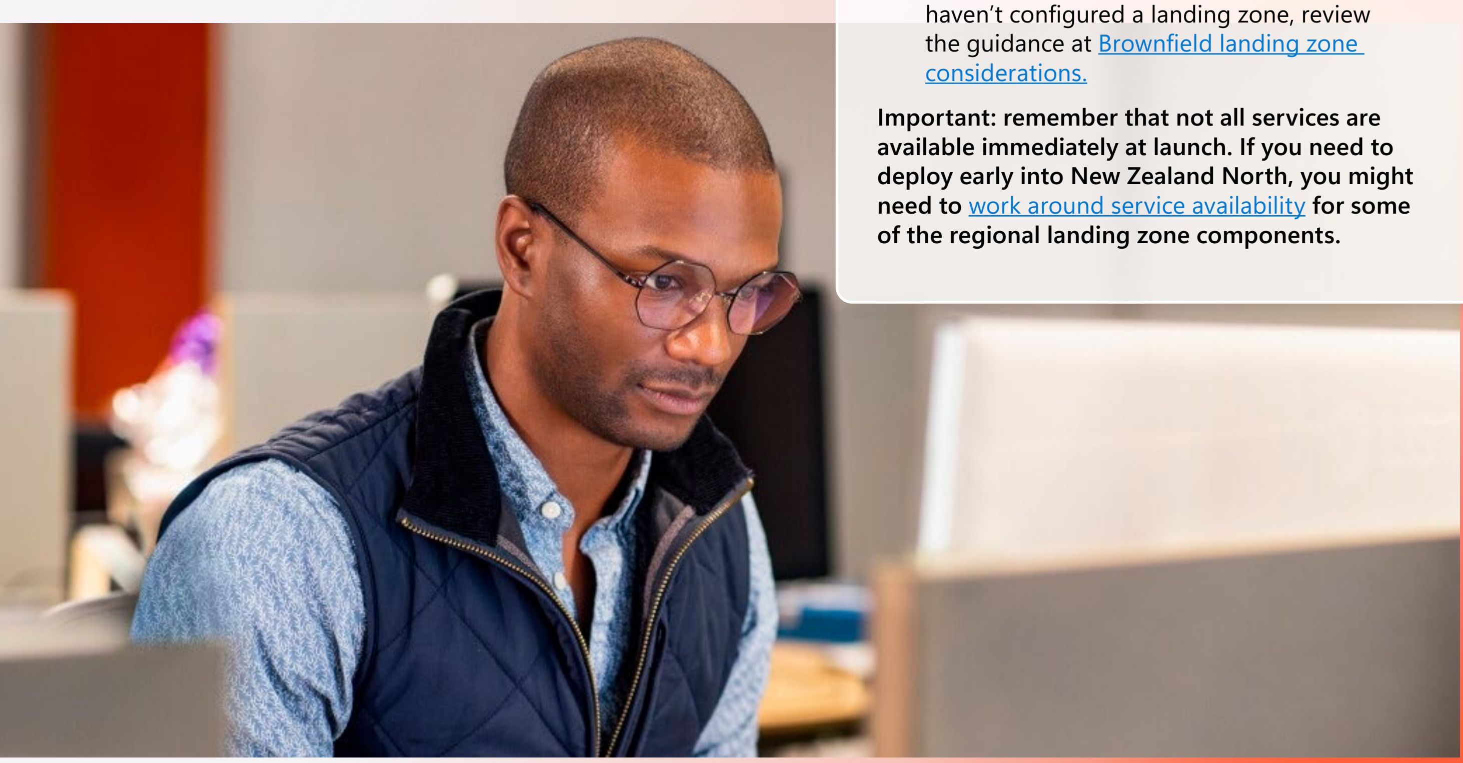
- If you have an established landing zone, you can extend it or move it into New Zealand North when the region is launched and the necessary services are available.

A *landing zone* is a set of resources and configuration that establish the basis for an Azure estate.

It can be helpful to think of Azure landing zones as being like city plans. The architectures of workloads deployed into a landing zone are like plans for buildings in a city. A city's water, gas, electricity, and transport systems all must be in place before buildings can be constructed. Similarly, an Azure landing zone's components, including management groups, policies, subscriptions, and role-based access control (RBAC), all must be in place before any production workloads can be deployed. For more information, see What is an Azure landing zone?

When you deploy a landing zone, many components are not regionally bound. For example, management groups, role assignments, DNS zones, and Microsoft Defender for Cloud configuration are set globally and apply regardless of which Azure regions you use.

There are also some components that *are* regionally bound, especially for components that relate to networking, connectivity to on-premises environments, Log Analytics and monitoring resources, and automation of management. For more information, see How landing zones use Azure regions.



Suggestions

- If you're new to Azure and you're deploying a brand-new landing zone after the New Zealand North region launches, you'll likely deploy the regional landing zone components directly to New Zealand North.
- If you have an existing landing zone and you're extending your Azure estate to New Zealand North, many of your existing landing zone resources will remain in place. However, you will likely need to deploy new resources into New Zealand North. For more information, see Add a new region to an existing landing zone.
- If you have an existing landing zone and you're migrating your entire Azure estate to New Zealand North, you can move the regionally deployed landing zone components. For more information, see Move your Azure estate to a new region.
- If you have an existing Azure estate but you haven't configured a landing zone, review the guidance at Brownfield landing zone considerations.

Important: remember that not all services are available immediately at launch. If you need to deploy early into New Zealand North, you might need to work around service availability **for some of the regional landing zone components.**

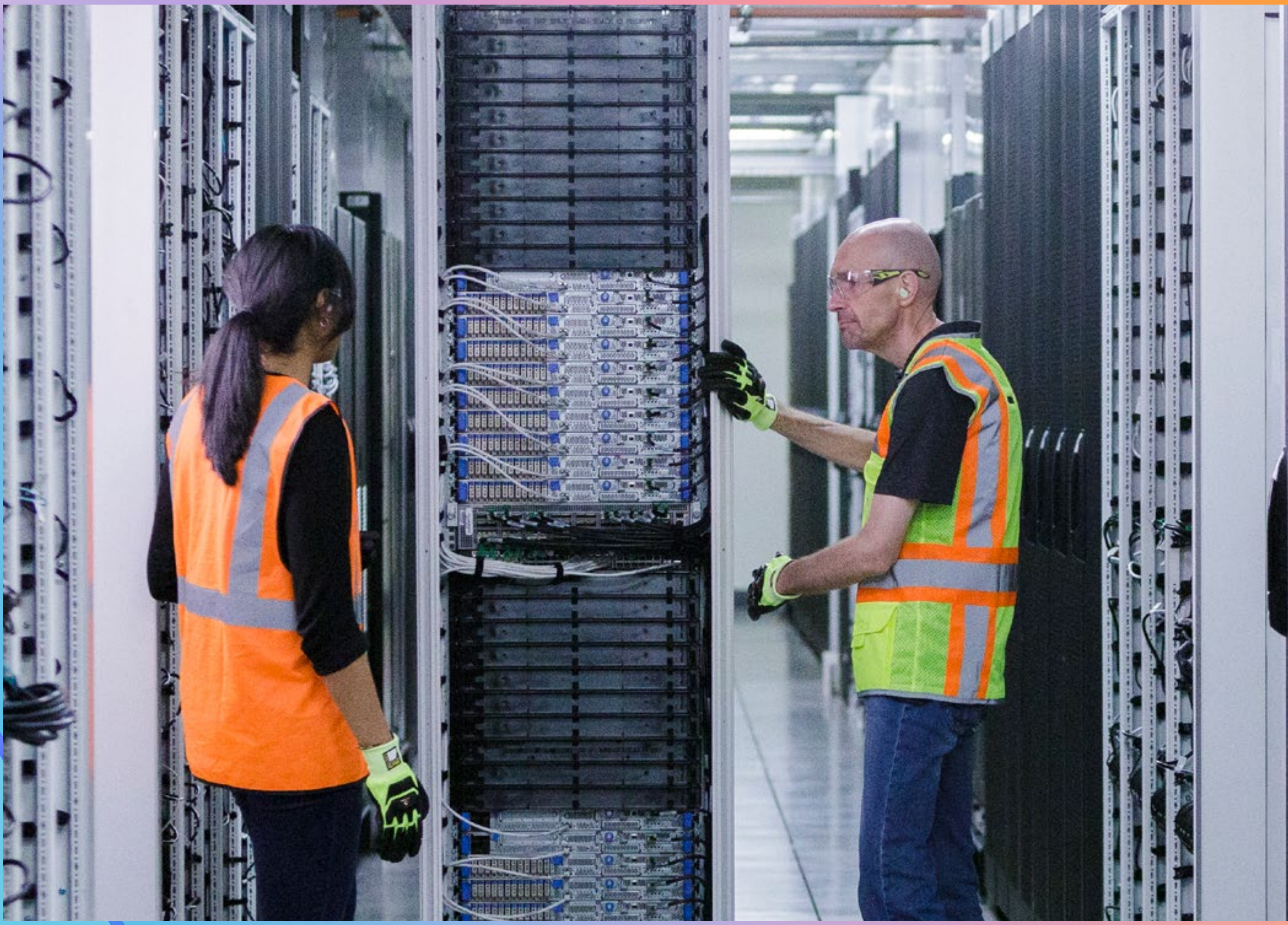
Security considerations for New Zealand North

Key points:

- Security for New Zealand North is the same as other Azure regions.

Azure regions all meet the same stringent security requirements, including physical access to datacenters, network security, and hardware- and software-layer security throughout the entire Azure environment. Whether you use New Zealand North or any other region, there's nothing different from a security perspective.

Ensure that you understand how services are deployed to New Zealand North and to other regions. Strategic services might not be available in New Zealand North at all. If you use specific security products, you might need to consider running those services in other regions, and will need to determine how this approach can meet your data residency requirements.



Data residency

Key points:

- New Zealand North provides in-country data residency. However, there are some situations where your data might leave the geography, and you need to make informed decisions about whether to allow this to happen.
- New Zealand-based customers' Microsoft 365 tenancies can be migrated to the New Zealand North region. You must purchase the Microsoft 365 Advanced Data Residency add-on to have your Microsoft 365 data migrated.

You might choose to use New Zealand North to meet data residency requirements for your workloads in the Microsoft cloud.

It's important to be aware that, in some narrow situations, data might be stored outside of your selected geography. For more information, see Data residency in Azure.

Also, if you use a wide range of Azure services, you might need to use multiple regions because not all services are available in all regions. You should carefully consider whether your services will be available in New Zealand North. For more information, see Service availability and timelines. If you depend on services that aren't available in the region, you should determine which other regions provide a good balance between your data residency requirements, resource cost, and latency.

Microsoft 365 Advanced Data Residency

Microsoft has recently improved its data residency commitments for Microsoft 365 services with the opening of new regions. This enhancement is particularly beneficial for the public sector and regulated industries, which often have stricter data residency requirements than other customers.

If you wish to migrate from Australia to New Zealand North, you need to purchase the Microsoft 365 Advanced Data Residency SKU in addition to your existing licenses (for example, E3 or E5).

When the region reaches general availability, if you have purchased the additional SKU, you can specify the destination for your tenancy migration in the Microsoft 365 portal. This step is crucial to ensure that you, as the tenancy owner, have consciously decided to migrate to the chosen destination.

The migration process is managed by Microsoft. You can monitor the progress of individual service migrations through your portal. After all services have been successfully migrated, you will receive a formal notification. This approach ensures transparency and allows you to stay informed throughout the migration process. For more information, see Advanced data residency in Microsoft 365.

Compliance and regulatory standards

Key points:

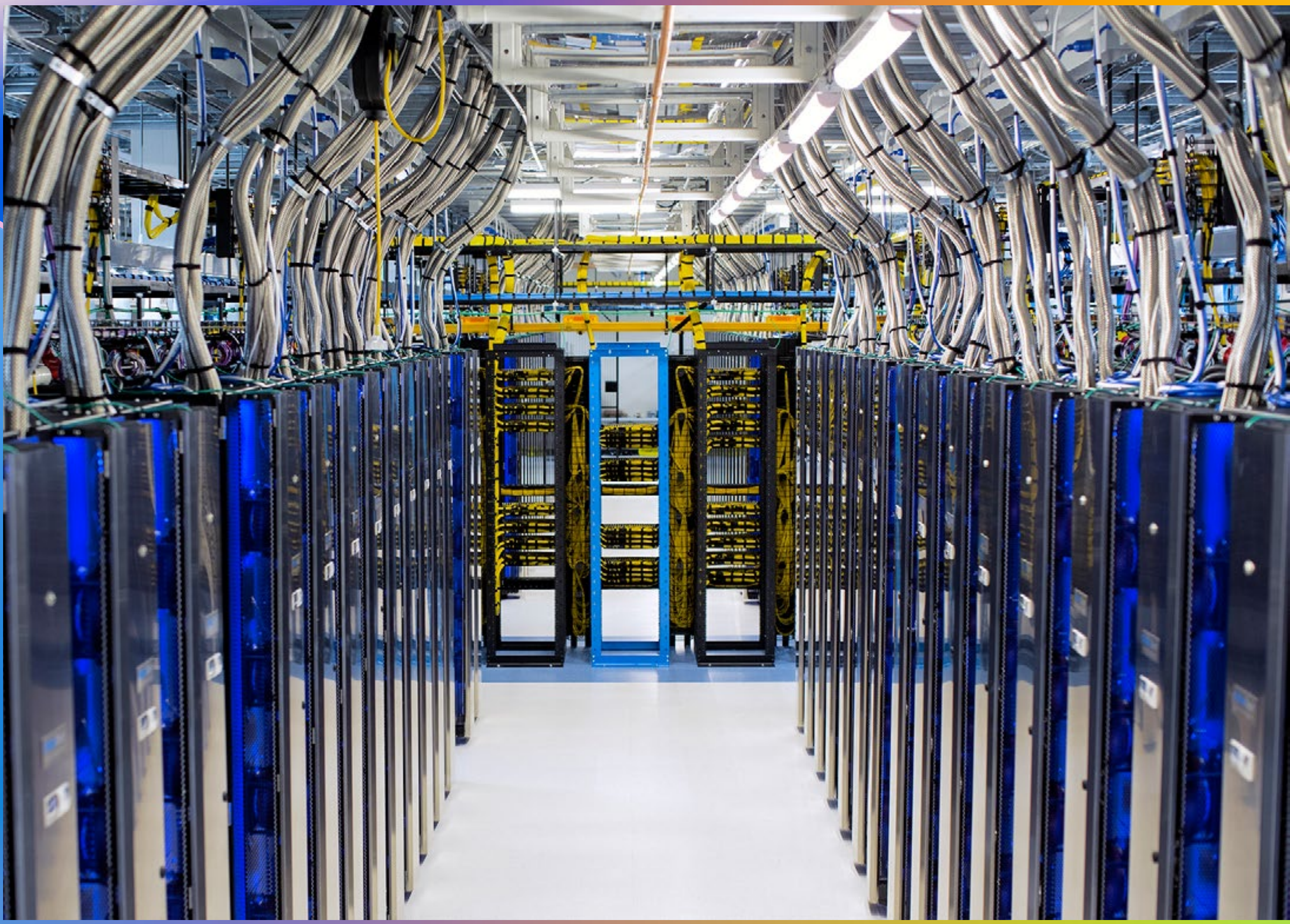
- Microsoft provides New Zealand-specific resources for compliance purposes.

Microsoft Azure and other Microsoft cloud products meet many global and New Zealand compliance and regulatory standards. See New Zealand regional guidance on the Microsoft Service Trust Portal for compliance and regulatory information here https://servicetrust.microsoft.com/ViewPage/RegionalNewZealand.

Also, for the Azure Policy initiative that corresponds to the New Zealand ISM Restricted standard, see the regularly updated download on the GCSB website here https://www.nzism.gcsb.govt.nz/resources/nzism-baseline-security-templates/ or the Azure code repository here https://github.com/Azure/Community-Policy/tree/main/policySetDefinitions/regulatorycompliance-nzism.

If you're a government agency customer, you'll need to use the Cloud Risk Discovery Tool to identify risks and controls for your workload. Microsoft provides information about the Azure platform to support this process which can be found here https://learn.microsoft.com/en-us/compliance/regulatory/offering-nz-cc-framework-nz.

If you require more information, speak to your Microsoft account team.



Microsoft Azure

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.