Azure Database for PostgreSQL Flex – Resilience Reference Architecture

Private Link:
Private links are available only for servers that have public access networking. They can't be created for servers that have private access (virtual network integration).

Private links can be configured only for servers that were created after the release of this feature. Any server that existed before the release of the feature can't be set with private links.

Private Link and DNS
Private endpoint Private DNS zone configurations automatically generates only if you use the recommended naming scheme: privatelink.postgres.database.azure.com. On newly provisioned public access (non-virtual network injected) servers, there's a temporary DNS layout change. The server's FQDN now becomes a CName, resolving to a record, in the format servername.privatelink.postgres.database.azure.com. In the near future, this format will apply only when private endpoints are created on the server.

Virtual Endpoint:
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone

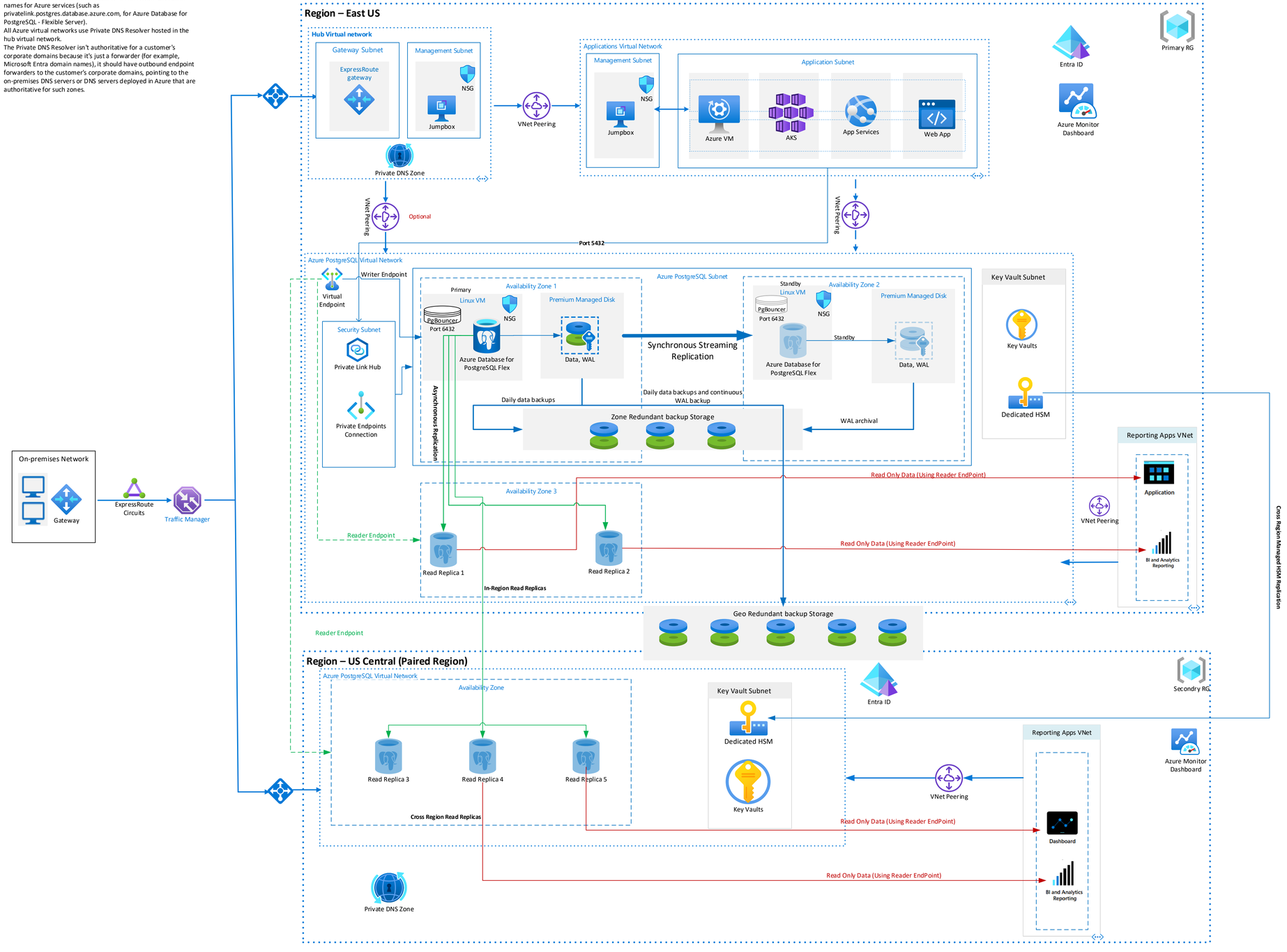
TLS/SSL is enforced on the server by default

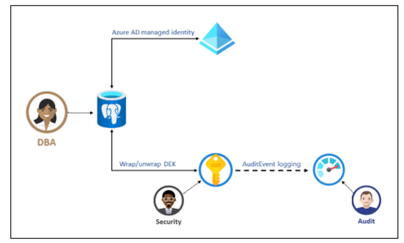
Read Replica
The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the primary. Read replicas can also be deployed in a different region and can be promoted to a read-write server if disaster recovery is needed.

Private Link and DNS integration:
Private DNS zones are typically hosted centrally in the same Azure subscription where the hub virtual network deploys. This central hosting practice is driven by cross-premises DNS name resolution and other needs for central DNS resolution, such as Microsoft Entra. In most cases, only networking and identity administrators have permissions to manage DNS records in the zones.

In such architecture, the following components are configured:

On-premises DNS servers have conditional forwarders configured for each private endpoint public DNS zone, pointing to the Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver hosted in the hub virtual network uses the Azure-provided DNS (168.63.129.16) as a forwarder.
The hub virtual network must be linked to the Private DNS zone names for Azure services (such as privatelink.postgres.database.azure.com, for Azure Database for PostgreSQL - Flexible Server).
All Azure virtual networks use Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver isn't authoritative for a customer's corporate domains because it's just a forwarder (for example, Microsoft Entra domain names), it should have outbound endpoint forwarders to the customer's corporate domains, pointing to the on-premises DNS servers or DNS servers deployed in Azure that are authoritative for such zones.





Azure Database for PostgreSQL flexible server uses Azure Storage encryption to encrypt data at rest by default, by using Microsoft-managed keys. For users of Azure Database for PostgreSQL flexible server, it's similar to transparent data encryption in other databases such as SQL Server.

Feature	Azure Key Vault Standard	Azure Key Vault Premium	Azure Key Vault Managed HSM
Tenancy	Multi-Tenant	Multi-Tenant	Single-Tenant
Compliance	FIPS 140-2 level 1	FIPS 140-2 level 2	FIPS 140-2 level 3
High Availability	Automatic	Automatic	Automatic
Use cases	Encryption at Rest	Encryption at Rest	Encryption at Rest
Key Controls	Customer	Customer	Customer
Root of trust control	Microsoft	Microsoft	Customer

Microsoft Azure

Azure Database for PostgreSQL Flex – Resilience Reference Architecture

Private Link:
Private links are available only for servers that have public access networking. They can't be created for servers that have private access (virtual network integration).

Private links can be configured only for servers that were created after the release of this feature. Any server that existed before the release of the feature can't be set with private links.

Private Link and DNS
Private endpoint Private DNS zone configurations automatically generates only if you use the recommended naming scheme: privatelink.postgres.database.azure.com. On newly provisioned public access (non-virtual network injected) servers, there's a temporary DNS layout change. The server's FQDN now becomes a CName, resolving to a record, in the format servername.privatelink.postgres.database.azure.com. In the near future, this format will apply only when private endpoints are created on the server.

Virtual Endpoint:
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone

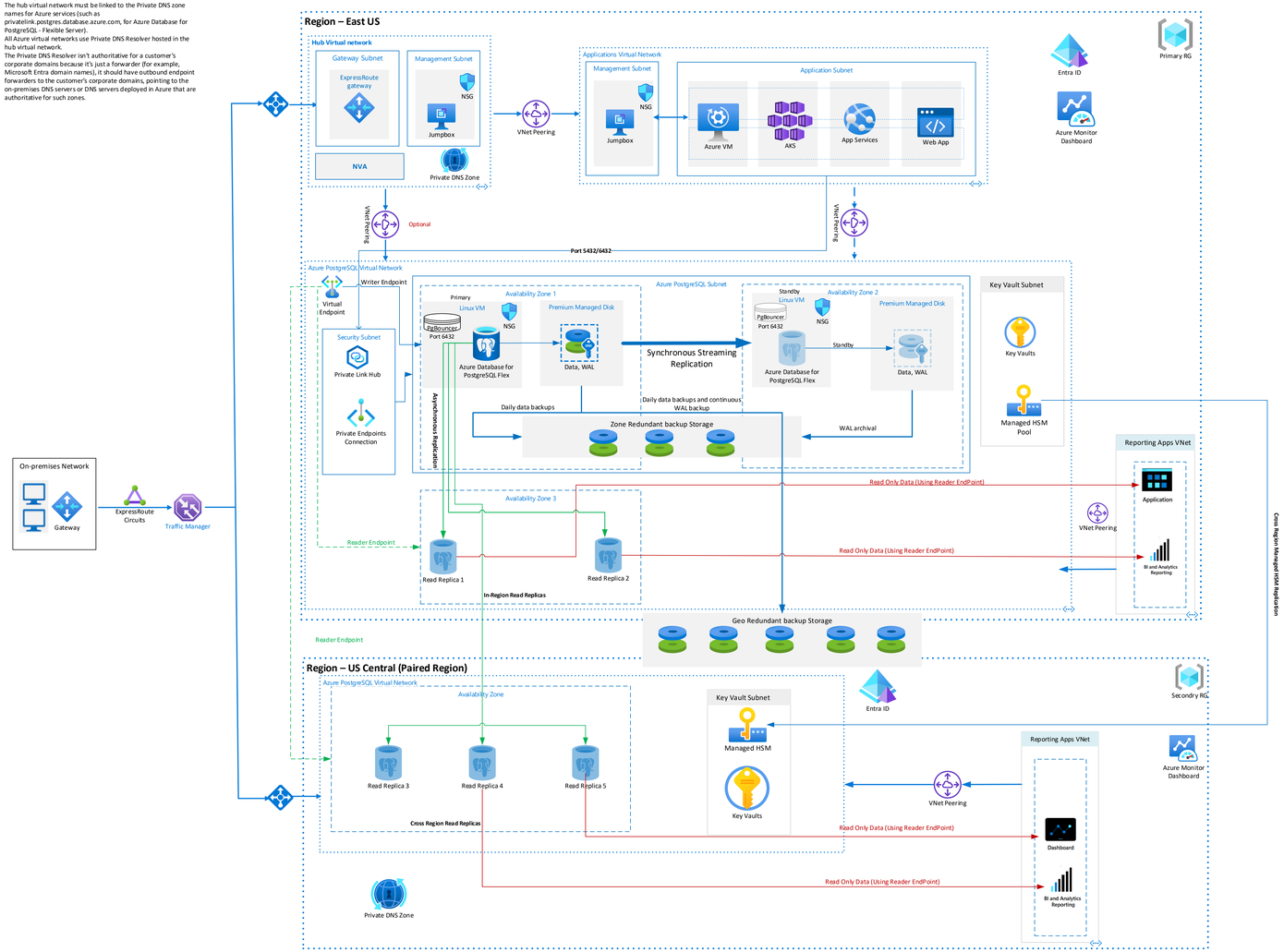
TLS/SSL is enforced on the server by default

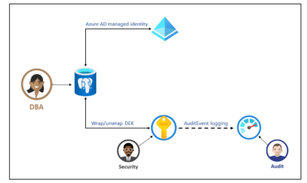
Read Replica
The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the primary. Read replicas can also be deployed in a different region and can be promoted to a read-write server if disaster recovery is needed.

Private Link and DNS integration:
Private DNS zones are typically hosted centrally in the same Azure subscription where the hub virtual network deploys. This central hosting practice is driven by cross-premises DNS name resolution and other needs for central DNS resolution, such as Microsoft Entra. In most cases, only networking and identity administrators have permissions to manage DNS records in the zones.

In such architecture, the following components are configured:

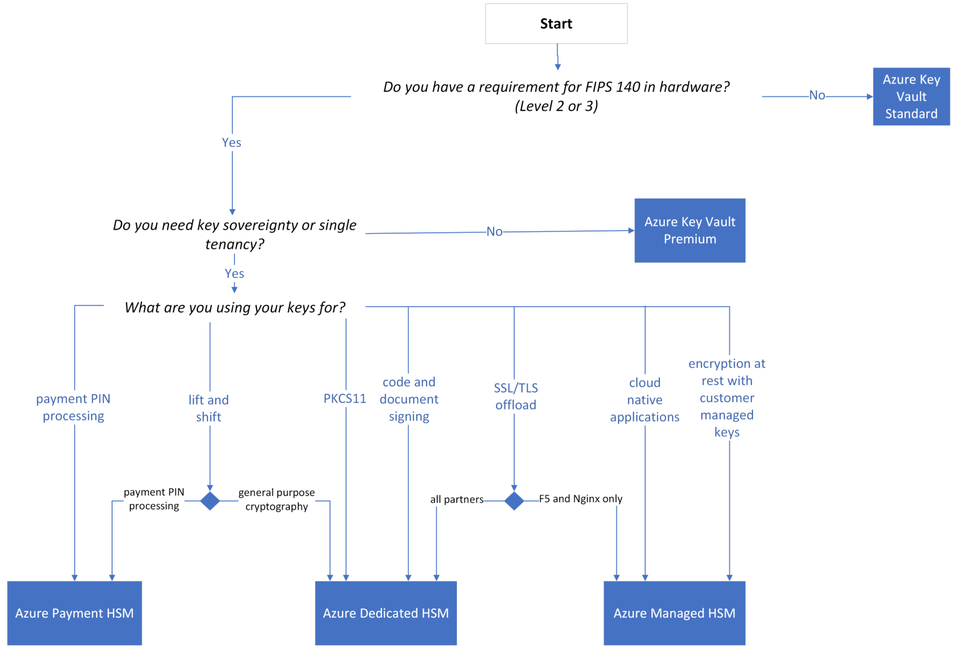
On-premises DNS servers have conditional forwarders configured for each private endpoint public DNS zone, pointing to the Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver hosted in the hub virtual network uses the Azure-provided DNS (168.63.129.16) as a forwarder.
The hub virtual network must be linked to the Private DNS zone names for Azure services (such as privatelink.postgres.database.azure.com, for Azure Database for PostgreSQL - Flexible Server).
All Azure virtual networks use Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver isn't authoritative for a customer's corporate domains because it's just a forwarder (for example, Microsoft Entra domain names), it should have outbound endpoint forwarders to the customer's corporate domains, pointing to the on-premises DNS servers or DNS servers deployed in Azure that are authoritative for such zones.





Azure Database for PostgreSQL flexible server uses Azure Storage encryption to encrypt data at rest by default, by using Microsoft-managed keys. For users of Azure Database for PostgreSQL flexible server, it's similar to transparent data encryption in other databases such as SQL Server.

Feature	Azure Key Vault Standard	Azure Key Vault Premium	Azure Key Vault Managed HSM
Tenancy	Multi-Tenant	Multi-Tenant	Single-Tenant
Compliance	FIPS 140-2 level 1	FIPS 140-2 level 2	FIPS 140-2 level 3
High Availability	Automatic	Automatic	Automatic
Use cases	Encryption at Rest	Encryption at Rest	Encryption at Rest
Key Controls	Customer	Customer	Customer
Root of trust control	Microsoft	Microsoft	Customer



- How Failover works in Read Replica scenario Azure PostgreSQL Flex? Internal Mechanism – DNS, CNAME, Endpoint, Promotion etc.
- How the Encryption works in case of cross region failover - Database Encryption Key (DEK) using Azure Key Vault
- How the Private Endpoint will behave in case of cross region DR scenrio?
- Should we have HSM or AKV for keys
- In case customers don't use Entra ID – What is the most resilient way to store user name and password using linked server?

- No Virtual Endpoint
- Keep Private Link separate
- Control plane will be separate from the data layer – Portal will be available
-
- Site Swap – Prod to DR and DR -> Prod – Need to add in the diagram
- Read Replica – Fail over
- HA and DR scenarios should be separate
- Add Log Analytics as well – No SQL DB for Logs – Time Series DB – They are seprate from the system – Data
-
-
-

Microsoft Azure

Azure Database for PostgreSQL Flex – Hi Availability (HA) - Resilience Reference Architecture

Private Link:
Private links are available only for servers that have public access networking. They can't be created for servers that have private access (virtual network integration).

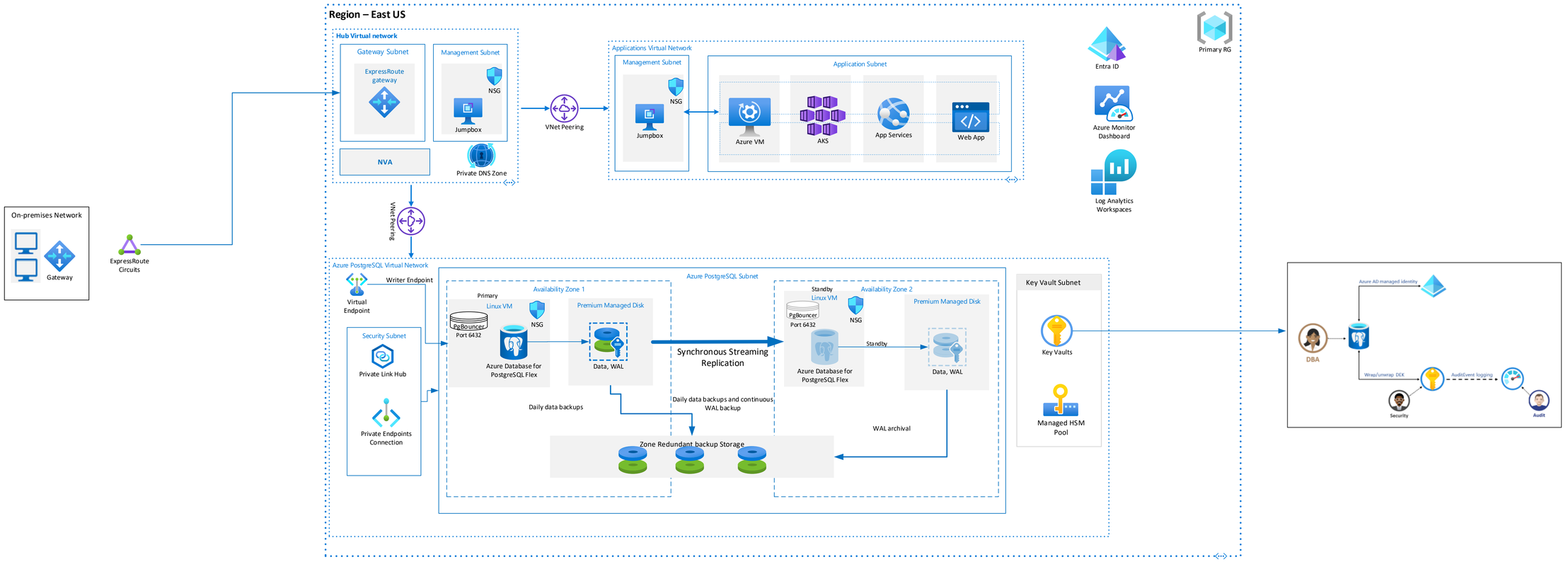
Private links can be configured only for servers that were created after the release of this feature. Any server that existed before the release of the feature can't be set with private links.

Private Link and DNS
Private endpoint Private DNS zone configurations automatically generates only if you use the recommended naming scheme: privatelink.postgres.database.azure.com. On newly provisioned public access (non-virtual network injected) servers, there's a temporary DNS layout change. The server's FQDN now becomes a CName, resolving to a record, in the format servername.privatelink.postgres.database.azure.com. In the near future, this format will apply only when private endpoints are created on the server.

Virtual Endpoint:
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone

TLS/SSL is enforced on the server by default

Read Replica
The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the primary. Read replicas can also be deployed in a different region and can be promoted to a read-write server if disaster recovery is needed.



Microsoft Azure

Azure Database for PostgreSQL Flex – High Availability (HA) with Read Replica in the same Region - Resilience Reference Architecture

Private Link:
Private links are available only for servers that have public access networking. They can't be created for servers that have private access (virtual network integration).

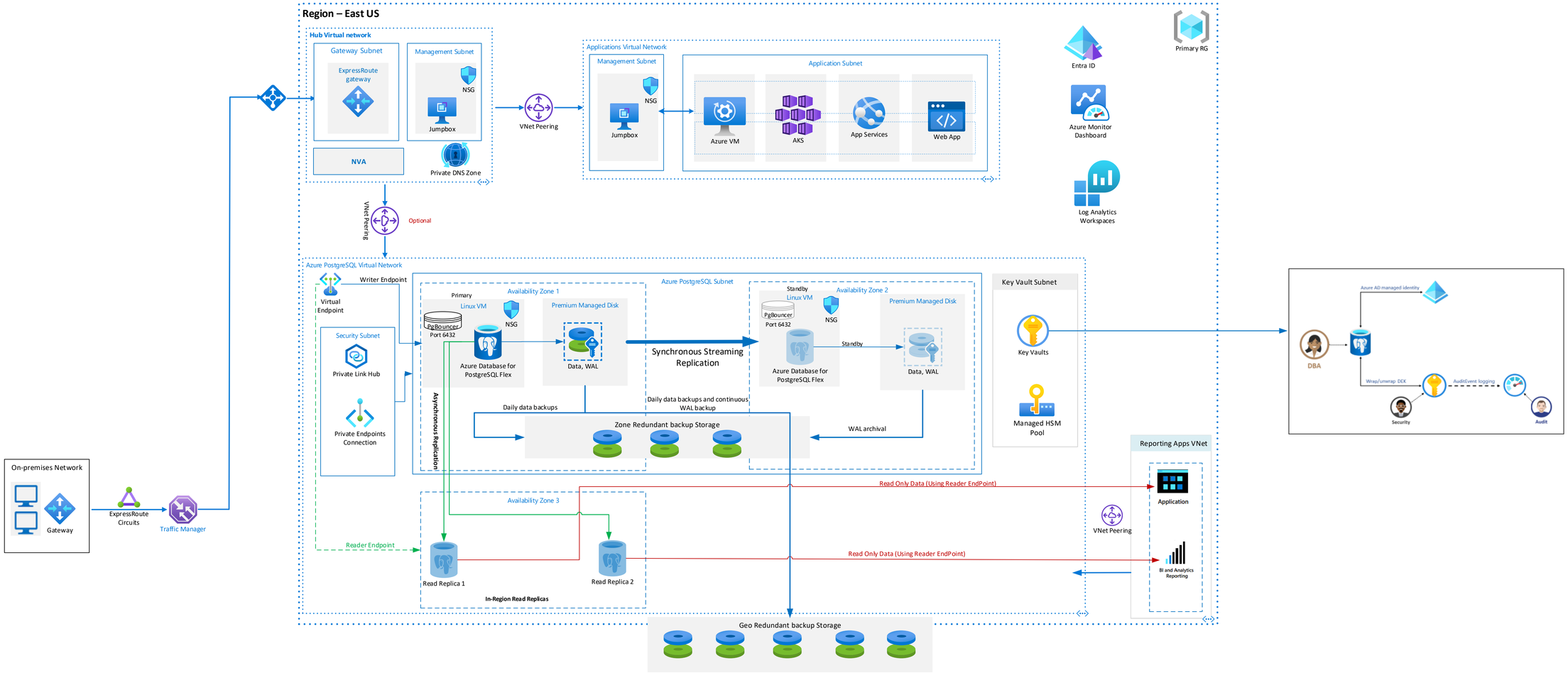
Private links can be configured only for servers that were created after the release of this feature. Any server that existed before the release of the feature can't be set with private links.

Private Link and DNS
Private endpoint Private DNS zone configurations automatically generates only if you use the recommended naming scheme: privatelink.postgres.database.azure.com. On newly provisioned public access (non-virtual network injected) servers, there's a temporary DNS layout change. The server's FQDN now becomes a CName, resolving to a record, in the format servername.privatelink.postgres.database.azure.com. In the near future, this format will apply only when private endpoints are created on the server.

Virtual Endpoint:
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone

TLS/SSL is enforced on the server by default

Read Replica
The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the primary. Read replicas can also be deployed in a different region and can be promoted to a read-write server if disaster recovery is needed.



Azure Database for PostgreSQL Flex – Resilience Reference Architecture

Private Link:
Private links are available only for servers that have public access networking. They can't be created for servers that have private access (virtual network integration).

Private links can be configured only for servers that were created after the release of this feature. Any server that existed before the release of the feature can't be set with private links.

Private Link and DNS
Private endpoint Private DNS zone configurations automatically generates only if you use the recommended naming scheme: privatelink.postgres.database.azure.com. On newly provisioned public access (non-virtual network injected) servers, there's a temporary DNS layout change. The server's FQDN now becomes a CName, resolving to a record, in the format servername.privatelink.postgres.database.azure.com. In the near future, this format will apply only when private endpoints are created on the server.

Virtual Endpoint:
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone

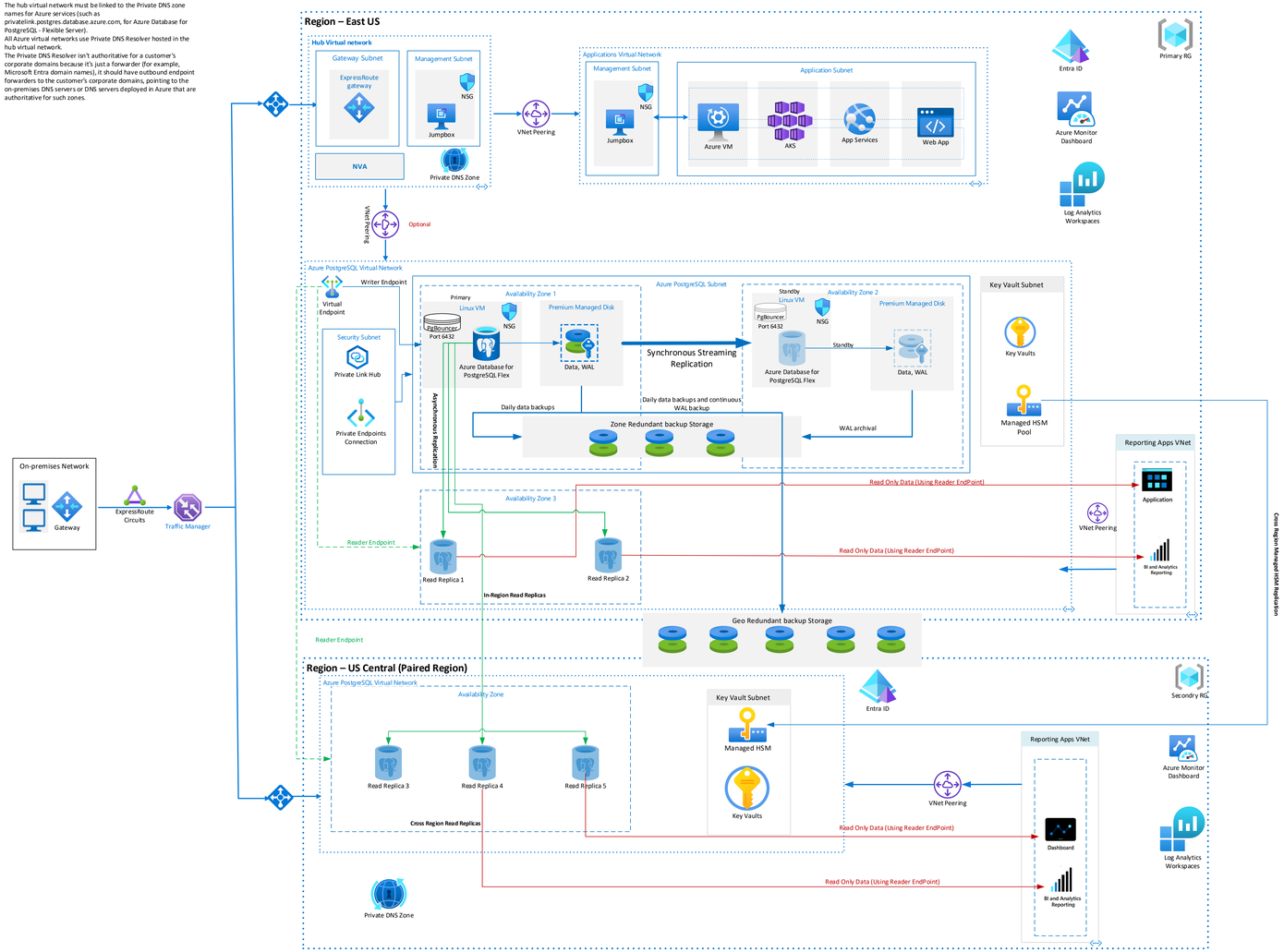
TLS/SSL is enforced on the server by default

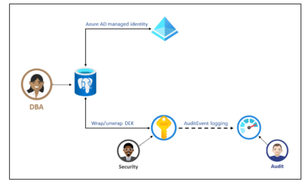
Read Replica
The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the primary. Read replicas can also be deployed in a different region and can be promoted to a read-write server if disaster recovery is needed.

Private Link and DNS integration:
Private DNS zones are typically hosted centrally in the same Azure subscription where the hub virtual network deploys. This central hosting practice is driven by cross-premises DNS name resolution and other needs for central DNS resolution, such as Microsoft Entra. In most cases, only networking and identity administrators have permissions to manage DNS records in the zones.

In such architecture, the following components are configured:

On-premises DNS servers have conditional forwarders configured for each private endpoint public DNS zone, pointing to the Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver hosted in the hub virtual network uses the Azure-provided DNS (168.63.129.16) as a forwarder.
The hub virtual network must be linked to the Private DNS zone names for Azure services (such as privatelink.postgres.database.azure.com, for Azure Database for PostgreSQL - Flexible Server).
All Azure virtual networks use Private DNS Resolver hosted in the hub virtual network.
The Private DNS Resolver isn't authoritative for a customer's corporate domains because it's just a forwarder (for example, Microsoft Entra domain names), it should have outbound endpoint forwarders to the customer's corporate domains, pointing to the on-premises DNS servers or DNS servers deployed in Azure that are authoritative for such zones.





Azure Database for PostgreSQL flexible server uses Azure Storage encryption to encrypt data at rest by default, by using Microsoft-managed keys. For users of Azure Database for PostgreSQL flexible server, it's similar to transparent data encryption in other databases such as SQL Server.

Feature	Azure Key Vault Standard	Azure Key Vault Premium	Azure Key Vault Managed HSM
Tenancy	Multi-Tenant	Multi-Tenant	Single-Tenant
Compliance	FIPS 140-2 level 1	FIPS 140-2 level 2	FIPS 140-2 level 3
High Availability	Automatic	Automatic	Automatic
Use cases	Encryption at Rest	Encryption at Rest	Encryption at Rest
Key Controls	Customer	Customer	Customer
Root of trust control	Microsoft	Microsoft	Customer

- How Failover works in Read Replica scenario Azure PostgreSQL Flex? Internal Mechanism – DNS, CNAME, Endpoint, Promotion etc.
- How the Encryption works in case of cross region failover - Database Encryption Key (DEK) using Azure Key Vault
- How the Private Endpoint will behave in case of cross region DR scenrio?
- Should we have HSM or AKV for keys
- In case customers don't use Entra ID – What is the most resilient way to store user name and password using linked server?

- No Virtual Endpoint
- Keep Private Link separate
- Control plane will be separate from the data layer – Portal will be available
-
- Site Swap – Prod to DR and DR -> Prod – Need to add in the diagram
- Read Replica – Fail over
- HA and DR scenarios should be separate
- Add Log Analytics as well – No SQL DB for Logs – Time Series DB – They are seprate from the system – Data
-
-
-

Microsoft Azure

Azure PostgreSQL Flexible Server is designed to handle failover scenarios both within a region and across regions, ensuring high availability and resilience for your databases. Here's a detailed look at how failover is managed and the considerations involving Azure Key Vault (AKV) with private endpoints:

Within-Region Failover
High Availability Configuration: Azure PostgreSQL Flex allows you to configure a standby replica of your primary server within the same region but in a different availability zone. This setup ensures that in the event of a zone failure, the standby can automatically take over with minimal downtime.

Automatic Failover: The service automatically handles failover to the standby server if the primary server becomes unavailable due to maintenance or outages.

DNS Caching: When using private endpoints, DNS caching can affect how quickly applications can reconnect to the database post-failover. It’s crucial to configure your DNS settings properly to handle the updated pointers that direct to the new primary server.

Cross-Region Failover
Geo-Redundancy: Cross-region failover can be facilitated by setting up a geo-redundant standby server in a different region. This is particularly important for disaster recovery scenarios where regional continuity is at risk.

Manual Failover: Typically, cross-region failover is not automatic and requires manual intervention to promote a standby server in another region to become the new primary server.

DNS and Endpoint Configuration:

Using AKV with private endpoints complicates cross-region failover due to the need for proper DNS management. Since AKV uses regional DNS zones, you need to ensure that your DNS setup can handle the change in regions without significant delays.
Consider implementing traffic manager profiles or using Azure DNS to manage DNS failover and health checks, ensuring that the DNS can quickly resolve to the new primary server’s location.
Integration with Azure Key Vault
When integrating Azure PostgreSQL Flex with AKV for managing encryption keys and secrets, consider the following:

AKV Resilience: Rely on AKV’s built-in high availability and redundancy features to ensure that it remains accessible even during regional outages.

DNS Requirements: For AKV, especially when accessed via private endpoints, ensure that your DNS setup aligns with AKV's failover mechanism to maintain connectivity during and after failovers. This might involve configuring DNS settings to support rapid changes in endpoint addresses.

Cross-Region Considerations: If your DR strategy includes cross-region failover, ensure that your AKV setup can replicate secrets and keys across regions or that you have equivalent key vaults in multiple regions with synchronized data.

By addressing these considerations, you can enhance the resilience and availability of your Azure PostgreSQL Flexible Server deployments, ensuring they remain robust even in complex scenarios involving regional outages and failovers.