Limitations

Last updated by | Subbu Kandhaswamy | Sep 24, 2021 at 2:37 PM PDT

Private Link

Contents

Limitations

- Network/Application Security Groups is not supported on Private Endpoints during preview, only private traffic from connected networks (Peering, on premises) is allowed, limiting access to specific sources is not supported irrespective of the security rules defined on NSG, this limitation will be removed near the time of GA
- Mixing Private Endpoints and Virtual Machines is possible by disabling “NetworkPolicies” on the subnet, this setting disables NSG enforcement on the private endpoints only, VMs will still be under the restrictions defined on the security rules.
- Traffic coming from on premises will use ER/VPN Gateways, depending on the workload, latency depends on the performance assigned to those Gateways based on Sku
- Accessing Private Endpoints from specialized injected workloads is not supported, this impacts App Service VNet Integration Plan and Azure Container Instances

1. Regions added after creating private endpoint are not accessible immediately by client. Customer need to go thorough steps in Section 4.4 ‘Add/ Remove Region’ to make it work end to end. We’re actively working on improvement to make it a 1-click fully-automated experience.

2. Direct connection mode for SQL and Table are not supported. We’re actively working on it.

3. For mongo customers with endpoints xxx.documents.azure.com, having ‘replicaSet=globaldb’ in the connection string doesn’t work. We’re working on the fix. A work-around is to migrate the database account to xxx.mongo.cosmos.azure.com. For mongo customers with endpoints xxx.mongo.cosmos.azure.com, having ‘replicaSet=globaldb’ in the connection string works if ‘appName=<account name>’ parameter is specified. For example, ‘replicaSet=globaldb&appName=@mydbaccountname@’.

4. VNET is not allowed to be moved or deleted if there’s private endpoint under it.

5. Cosmos database account is not allowed to be deleted if there’s private endpoint for it.

6. Cosmos database account is not allowed to fail over to a region which is not mapped by all approved endpoints of this database account. This issue only happens with incomplete Add/ Remove region workflow. Long as steps in Section 4.4 ‘Add/ Remove Region’ are strictly followed, this issue won’t happen. We’re actively working on improvement to make add/ remove region a 1-click fully-automated experience.

7. Network admin who doesn't have sufficient permission on cosmos database account has to be granted '*/PrivateEndpointConnectionsApproval' permission minimally at database account scope by cosmos admin in order to create a private endpoint. We're actively working on manual approval support, so that unprivileged network admin initiates approval request to create private endpoint and cosmos admin can approve or reject.

8. This is common to any firewall related configuration change: Configuration change takes effect within 15 minutes.

How good have you found this content?