

Troubleshoot common Networking issues

Last updated by | Vitor Tomaz | Nov 16, 2022 at 12:58 PM PST

Contents

- [Common problem scenarios](#)
- [Network Intent Policy \(NIP\)](#)
 - [Network Security Group \(NSG\)](#)
 - [Route Table \(RT\)](#)

Common problem scenarios

Problem: Customer gets [Network Intent Policy \(NIP\)](#) conflict during provisioning of new Managed Instance while using networkconfiguration that worked in the past.





Solution: This means that default [Network Intent Policy \(NIP\)](#) changed in the meantime and customer's older configuration is no longer compatible with it. Check the logs from Kusto: [Getting Network Intent Policy \(NIP\) errors in Kusto](#) Then instruct the customer to make necessary [Network Security Group \(NSG\)](#) / [Route Table \(RT\)](#) changes and try provisioning again.

Problem: Customer gets conflict when adding route that contains public IP space that he owns, with NextHop other than Internet.

Solution: This means that newest Network Intent Policy (NIP) hasn't been applied. Previous NIP contained all public IP ranges (everything except private ones: 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16) which causes conflict when you try putting **NextHop** other than **Internet** for any range that belongs to public IP space. New [NIP](#) will be automatically applied only when customer's configuration (both [NSG](#) and [RT](#)) is compliant with it.

Check customer's configuration and apply the necessary changes (e.g. customer had **Internet** instead of **AzureCloud** in outbound [NSG](#) rule), **wait 1 hour** (this is the NIP auto-update period) and ask the customer to try adding the route again. [Getting Network Intent Policy \(NIP\) errors in Kusto](#) [Check current Network Intent Policy \(NIP\) value in CMS](#)

*Problem:** Customer reports seeing a lot of Create or Update Network Intent Policy Activity Log on portal e.g.

▶  Create or Update Network Intent Policy	Failed	23 min ago	Wed Apr 03...	DS-CloudLifter_jovanc_R&D_60843	Azure SQL Managed Insta...
▶  Create or Update Network Intent Policy	Failed	25 min ago	Wed Apr 03...	DS-CloudLifter_jovanc_R&D_60843	Azure SQL Managed Insta...
▶  Create or Update Network Intent Policy	Failed	26 min ago	Wed Apr 03...	DS-CloudLifter_jovanc_R&D_60843	Azure SQL Managed Insta...
▶  Create or Update Network Intent Policy	Failed	26 min ago	Wed Apr 03...	DS-CloudLifter_jovanc_R&D_60843	Azure SQL Managed Insta...

Solution: This means that newest [NIP](#) cannot be applied because the current network configuration is incompatible with the latest [NIP](#) . Check customer's configuration: [Check current Network Intent Policy \(NIP\) value in CMS](#) and compare with the current default [NIP](#) as presented in this document: [Current global \(default\) NIP](#) Then instruct the customer to make the necessary changes.

Network Intent Policy (NIP)

Current global (default) NIP: [Current intent policy](#)

[Check current Network Intent Policy \(NIP\) value in CMS](#)

NIP purpose: NIP is attached to a subnet and defines what kind of network configuration must be applied to it.

Two important parts are requirements for [Network Security Group \(NSG\)](#) and [Route Table \(RT\)](#) .e

Network Security Group (NSG)

It is possible to have no NSG assigned! But if there is NSG assigned then it must have supporting rules for all 5 mandatory rules.

These are current NSG requirements (3 inbound + 2 outbound rules):

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance-connectivity-architecture#mandatory-inbound-security-rules>

Mandatory inbound security rules

Name	Port	Protocol	Source	Destination	Action
management	9000, 9003, 1438, 1440, 1452	TCP	Any	Any	Allow
mi_subnet	Any	Any	MI SUBNET	Any	Allow
health_probe	Any	Any	AzureLoadBalancer	Any	Allow

Mandatory outbound security rules

Name	Port	Protocol	Source	Destination	Action
management	80, 443, 12000	TCP	Any	AzureCloud	Allow
mi_subnet	Any	Any	Any	MI SUBNET*	Allow

- Please note that rules that contain many ports (management inbound/outbound rules) must be defined **as one rule** in NSG in order to avoid conflicts.
 - e.g. **management** outbound rule cannot be split in 3 rules with ports 80, 443 and 12000).
- All Source/Destination tags are mutually incompatible (except **Any**).
 - e.g. if you put **Internet** as **Destination** in management outbound rule, NIP conflict will happen, while if you put **Any**, there will be no conflicts.

LATEST UPDATE (04/01/2019):

- **Management** outbound rule **Destination** changed from **Internet** to **AzureCloud**. This provides greater protection for customer.

Route Table (RT)

RT must be assigned! Further, it needs to have supporting rule for every RT requirement + no conflicts.

Current RT requirements: [Current intent policy](#) - "routes" section: These are currently routes that define whole Microsoft owned public IP ranges.

Customer doesn't need to have all these 99 routes in RT, as any rule that covers multiple ranges is also valid.

- e.g. 0.0.0.0/0 covers everything from 0.0.0.0 to 255.255.255.255, which contains all of the required ranges.

LATEST UPDATE (04/01/2019):

- 31 ranges (which described whole public IP space) changed to 99 ranges (which describe only MSFT public IP space). This is strict subset of the previous requirements, thus it won't cause conflict for anyone using RT config that worked earlier. Change will help customers who own certain public IP ranges to be able to add proper routes for them.

Tags: NIP, Network Intent Policy, NetworkIntentPolicy, Route Table, RouteTable, RT, NetworkSecurityGroup, Network Security Group, NSG, Networking, Connectivity, Managed Instance

How good have you found this content?



-