# Subnet Delegation

Last updated by | Vitor Tomaz | Feb 18, 2021 at 3:30 AM PST

## Service-aided subnet configuration

Service-aided subnet configuration provides automated network configuration management for subnets hosting managed instances. With service-aided subnet configuration user stays in full control of access to data (TDS traffic flows) while managed instance takes responsibility to ensure uninterrupted flow of management traffic in order to fulfill SLA.

Automatically configured network security groups and route table rules are visible to customer and annotated with prefix *Microsoft.Sql-managedInstances_UseOnly_*.

Service-aided configuration is enabled automatically once you turn on subnet-delegation for Microsoft.Sql/managedInstances resource provider.

### Important

> Once subnet-delegation is turned on you could not turn it off until you remove last virtual cluster from the subnet. For more details on how to delete virtual cluster see the following article. Note As service-aided subnet configuration is essential feature for maintaining SLA, starting May 1st 2020, it won't be possible to deploy managed instances in subnets that are not delegated to managed instance resource provider. On July 1st 2020 all subnets containing managed instances will be automatically delegated to managed instance resource provider.

### Enforced NSG inbound rules

| Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| management | 9000, 9003, 1438, 1440, 1452 | TCP | SqlManagement | MI SUBNET | Allow |
| | 9000, 9003 | TCP | CorpnetSaw | MI SUBNET | Allow |
| | 9000, 9003 | TCP | CorpnetPublic | MI SUBNET | Allow |
| mi_subnet | Any | Any | MI SUBNET | MI SUBNET | Allow |
| health_probe | Any | Any | AzureLoadBalancer | MI SUBNET | Allow |
| allow_tds_inbound | 1433 | TCP | VirtualNetwork | MI SUBNET | Allow |
| allow_redirect_inbound | 11000-11999 | TCP | VirtualNetwork | MI SUBNET | Allow |
| allow_geodr_inbound | 5022 | TCP | VirtualNetwork | MI SUBNET | Allow |

If you are configure MI using pre-deployed subnet, you need to manually create last three inbound rules "allow_tds_inbound", "allow_redirect_inbound", "allow_geodr_inbound".

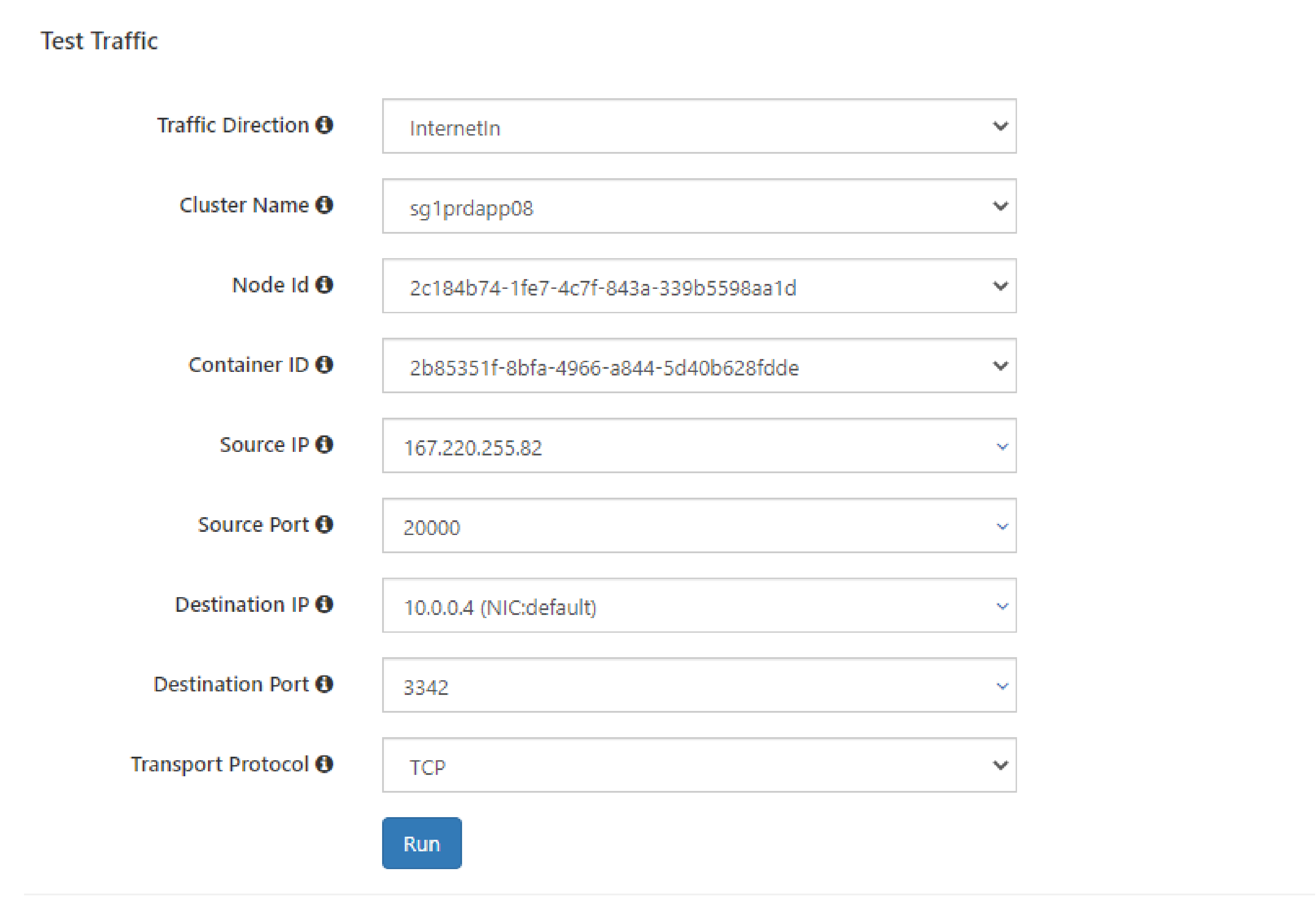
**Enforced NSG outbound rules**

| Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|
| management | 443, 12000 | TCP | MI SUBNET | AzureCloud | Allow |
| mi_subnet | Any | Any | MI SUBNET | MI SUBNET | Allow |
| allow_linkedserver_outbound | 1433 | TCP | MI SUBNET | VirtualNetwork | Allow |
| allow_redirect_outbound | 11000-11999 | TCP | MI SUBNET | VirtualNetwork | Allow |
| allow_geodr_outbound | 5022 | TCP | MI SUBNET | VirtualNetwork | Allow |

If you are configure MI using pre-deployed subnet, you need to manually create last three inbound rules "allow_tds_outbound", "allow_redirect_outbound", "allow_geodr_outbound".

### Check NSG from ASC

You can use network diagnostics from ASC to check NSG, route table settings.



Test Traffic

| | |
|---|---|
| Traffic Direction ℹ | InternetIn |
| Cluster Name ℹ | sg1prdapp08 |
| Node Id ℹ | 2c184b74-1fe7-4c7f-843a-339b5598aa1d |
| Container ID ℹ | 2b85351f-8bfa-4966-a844-5d40b628fdde |
| Source IP ℹ | 167.220.255.82 |
| Source Port ℹ | 20000 |
| Destination IP ℹ | 10.0.0.4 (NIC:default) |
| Destination Port ℹ | 3342 |
| Transport Protocol ℹ | TCP |

## How good have you found this content?