Traffic from MI to AWS

Last updated by | Vitor Tomaz | Nov 24, 2021 at 4:00 AM PST

Contents

Issue

Scenario 1

Customer notes traffic leaving Managed Instance subnet and destined to 52.216/217/218/219.x.x addresses which is listed as belonging to Amazon Web Services (AWS).

Scenario 2

The customer has observed unexpected traffic leaving this Managed Instance subnet (outbound) through his firewall. This connection tries to reach the URL netmon-canary-us-northernvirginia.s3.amazonaws.com. Connection runs every couple of hours.

Mitigation

Scenario 1

Customer is advised to block the NSG rules for suspicious addresses.

RCA Template

Scenario 1

Windows attempts to check revocation status of certificates by sending OCSP (Online Certificate Status Protocol) requests to external endpoints, some of which belong to amazon public IP ranges.

Considering that Sql MI doesn't depend on this external traffic and instead uses internal service for managing certificate revocations SQL MI enforces following NSG rule which allows only outbound calls towards azure IPs, which is why customer sees these calls in there NSG logs.

NSG rule being enforced:

```
{
   "name":"mi-services-out-<subnet_range_placeholder>-v9",
   "properties":{
      "description":"Allow MI services outbound traffic over https",
      "protocol":"Tcp",
      "access":"Allow",
      "direction":"Outbound",
      "sourcePortRanges":[
         "*"
      ],
      "destinationPortRanges":[
         "443",
         "12000"
      ],
      "sourceAddressPrefixes":[
         "<subnet_ip_range>"
      ],
      "destinationAddressPrefixes":[
         "AzureCloud"
      ]
   }
}
```

Scenario 2

"We can confirm that this traffic is a result of activity of Microsoft internal component.

This component is owned by Azure Networking team, and has been deployed for the purpose of monitoring availability of connections going to destinations outside of the Azure.

Monitoring is done in a way that the component is trying to reach selected endpoints from the predefined list every 30s.

We can also confirm that the endpoint customer observed is one of those predefined endpoints."

Internal Reference

Scenario 1

Similar incidents:

- https://servicedesk.microsoft.com/#/customer/cases?caseNumber=120070224003238
- https://servicedesk.microsoft.com/#/customer/cases?caseNumber=120112425001205 ICM: https://portal.microsofticm.com/imp/v3/incidents/details/215696709/home
- https://servicedesk.microsoft.com/#/customer/cases?caseNumber=120092822001176 ICM: https://portal.microsofticm.com/imp/v3/incidents/details/207485999/home

Scenario 2

- https://portal.microsofticm.com/imp/v3/incidents/details/268888693/home

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Azure SQL v3\Security\Other

How good have you found this content?

🙂 🙁