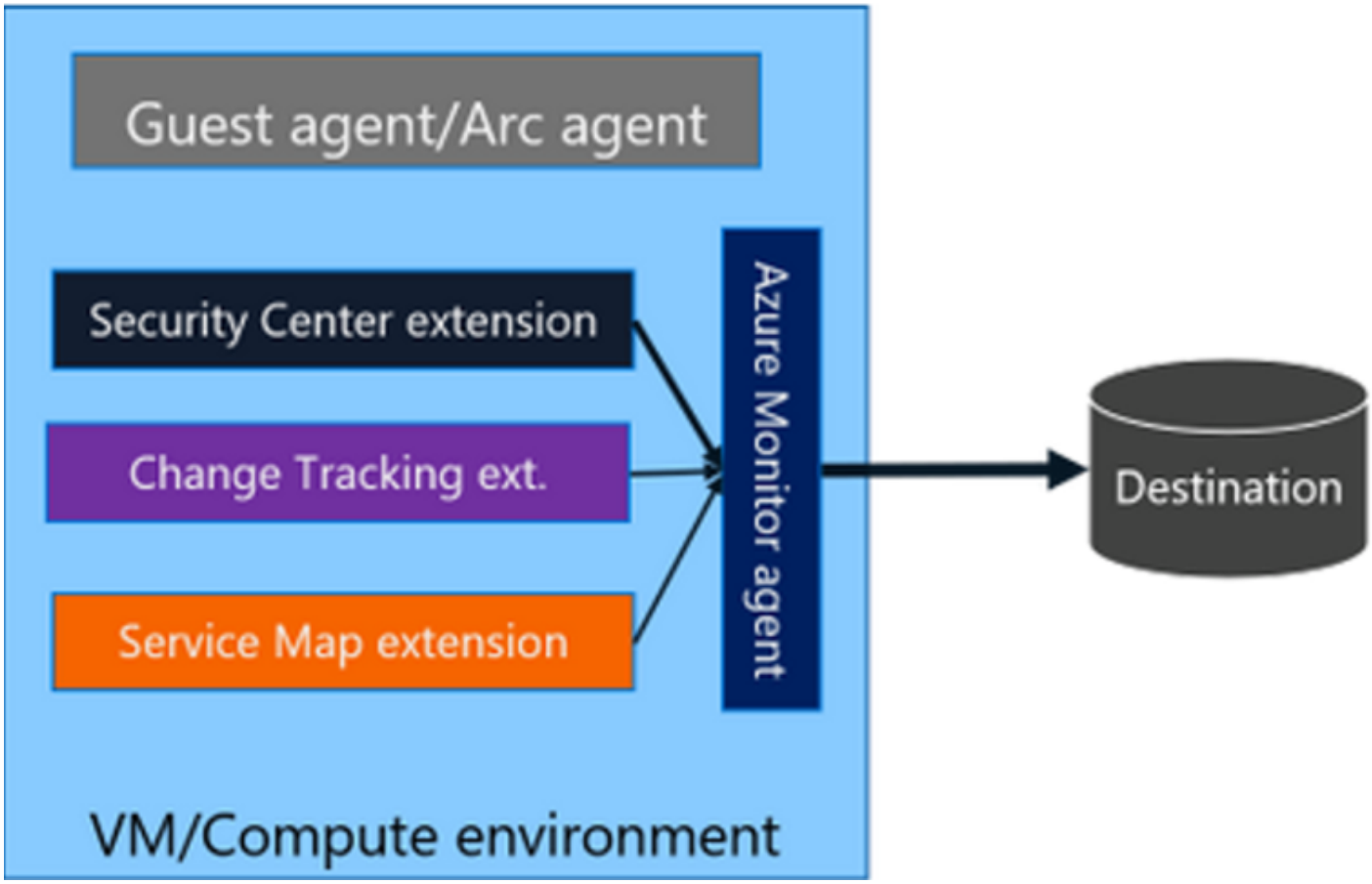
Windows DNS AMA Connector TSG

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

General Context

The DNS connector is a VM extension that collects DNS events from ETW (Event Tracing for Windows) stream in windows and sends the data to Ama that sends the data to NS pipeline and then LA.

The Extension is only supported in Windows environments because the events are read from the ETW mechanism which is a windows feature. more specificity the extension is only supported from windows server 2012 R2 and forward.



The DNS extension is like the SecurityCenter/ChangeTracking extensions. data flows from the extension to ama and then to the cloud(for more info.

Sentinel Contacts

Eng: Yotam Ziv, Ido Klotz , Noam Landress.

Product: Shirley Kochavi.

Data Flow

For DNS Data to flow those things need to work together:

0. A domain controller machine.

1. Azure monitor agent / Arc Agent is installed and running on the machine and reporting healthy.
2. A DCR with the DNS stream (example below) downloaded to the machine.(for more info on DCR here)
3. DNS agent installed + and reporting healthy
4. The VM / on Prem Machine is a DNS server and creates events that can be seen in the windows event viewer.

Extension versioning

It is always recommended to update to the latest version, for a list of versions you can use this: Virtual Machine Extension Images - List Versions, you use the customer info for the location and subscription. the publisher name for our extension is: "*Microsoft.Sentinel.AzureMonitorAgentExtensions*" and the type is "*MicrosoftDnsAgent*". To get the customer version use this with VmExtensionName "*MicrosoftDnsAgent*", you can also the version in the VM blade in the portal under extensions. if you see that the customer has an outdated version you can use Virtual Machine Extensions - Create Or Update call to update his agent with the same VmExtensionName as before and this is a sample body:

```
{
    "name": "MicrosoftDnsAgent",
    "type": "Microsoft.Compute/virtualMachines/extensions",
    "properties": {
        "autoUpgradeMinorVersion": true,
        "publisher": "Microsoft.Sentinel.AzureMonitorAgentExtensions",
        "type": "MicrosoftDnsAgent",
        "typeHandlerVersion": "<Version>"
    }
}
```

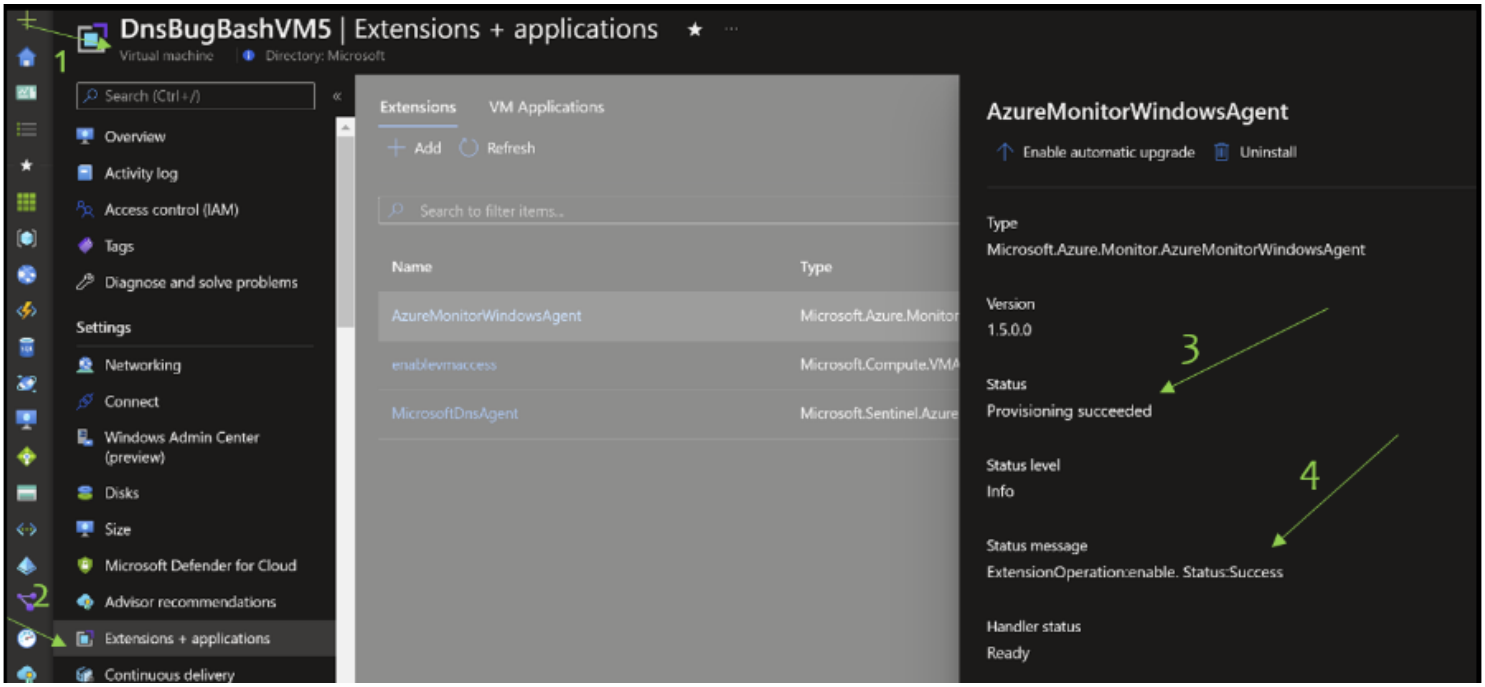
make sure you update the type handler version to the correct version.

Troubleshooting stages

1. If 1 or 2 in the data flow section in the flow are problematic check out the windows AMA connectors TSG for help.

    Things to validate

    1. Ama is sending heartbeat for that machine in the heartbeat table in LA.
    2. Check that the DCR was successfully downloaded and applied to the machine and formatted correctly (explanation here).
    3. Check that Ama is healthy in the vm extension section (only works for non arc machines) - the user needs to open the vm blade and follow the steps with the arrows.



(if the customer is using ARC skip steps 2-3 because the health indicator for vm extensions is not available in ARC)

2. In the same extension window check the Microsoft Dns Agent, if the status isn't "Provisioning succeeded ", there should be a message saying what is incorrect.

You can use this query to check the info without the customer:

Execute in [Web] [Desktop] (only works for non arc machines) other clouds cluster info available here

```
GuestAgentExtensionEvents
| where TIMESTAMP >ago(14d)
| where Name == "Microsoft.Sentinel.AzureMonitorAgentExtensions.MicrosoftDnsAgent"
| project TIMESTAMP,Region,Version,RoleName,Name,Operation,OperationSuccess,Duration,Message,Su
| where OperationSuccess  !="True"
```

3. The status message is supposed to be "Extension is running..". If it isn`t, use the below section to understand each error message:
    1. **"FailedToConnectToPipe"** – there was a problem connecting to the ama agent, this mostly happens because of problems mentioned in step 1 related to connecting to ama for example The DCR might be formatted badly and the ama didn`t open the named pipe needed to move the data.
    2. **"FailedToGetConfiguration"** – the configuration received from ama indicated that there was a failure in getting the configuration, check the internal logs for more info (explained in step 6).
    3. **"ConfigurationFormatError"** – there was a problem (JSON sterilization) reading the configuration sent by ama most likely caused by the extension setting section written wrongly.
    4. **"UnknownConfigurationError"** – an unknown error occurred in getting the configuration message, check the internal logs for more info (explained in step 6).

5. **"UnknownStreamInConfiguration"** – the DCR contained a stream not recognized by the agent , it will ignore it, and the extension should run normally , remove the unknown stream from the DCR to remove this message.
6. **"MissingStreamInConfiguration"**- the extension was expecting a stream in the DCR that was included in the DCR stream section, Currently the extension is only expecting and supporting one stream: "**Microsoft-ASimDnsActivityLogs**"
7. **"MissingDnsManifestFile"** – the manifest needed to read the events from the ETW stream in windows is missing, the manifest is a file that comes with the extension when it is downloaded with the agent, try to resend the put request to install the extension again(without uninstall) or uninstalling and installing again.
8. **"EventsListenerStopped"** – there was a problem with event listener that listens to the ETW events in the agents, read the internal logs to understand more,the logs should be in "C:\WindowsAzure\Logs\Plugins\Microsoft.Sentinel.AzureMonitorAgentExtensions.MicrosoftDnsAgent\ <**version**>". only restarting the agent can solve this problem.

If all the above looks good and there is no indication from the outside that the extension should be problematic, these next steps need access to the machine itself, either in a session with the customer or asking for information.

4. Check that the machine is indeed a DNS machine and is sending DNS events in the ETW stream. To do that use this guide to log DNS events in the event viewer. If you don't see any events then the machine is not a DNS machine or isn't sending events in the normal way and the windows server team should be approached for support.
5. Go to "C:\WindowsAzure\Logs\Plugins\Microsoft.Sentinel.AzureMonitorAgentExtensions.MicrosoftDnsAgent\ <**version**>" there should be logs for the execution of the install\update\enable etc.. commands and also a file called like the agent with the agent logs , look inside and see if you see any exception.
6. Check if events are passing to the ama agent successfully, use the table2csv.exe tool with this guide to check the MaQosEvent.tf file to see if dns events are reaching the ama. You can also see the specific table for dns to see the contents of the events received by ama, the table name is similar to the event name you found before.

If none of the above work , reach out to Yotam or Ido 😊

example DCR

```
{
    "properties": {
        "immutableId": "",
        "dataSources": {
            "extensions": [
               {
                    "streams": [
                        "Microsoft-ASimDnsActivityLogs"
                    ],
                    "extensionName": "MicrosoftDnsAgent",
                    "extensionSettings": {
                        "Filters": [
                            {
                                "FilterName": "SampleFilter",
                                "Rules": [
                                    {
                                        "Field": "DnsQuery",
                                        "FieldValues": [
                                            "ynet.co.il"
                                        ]
                                    }
                                ]
                            }
                        ]
                    },
                    "name": "DnsAgent"
                }
            ]
        },
        "destinations": {
            "logAnalytics": [
                {
                    "workspaceResourceId": "/subscriptions/3c1bb38c-82e3-4f8d-a115-a7110ba70d
                    "workspaceId": "04a763d0-9efd-4391-9bbe-b1a06408c3eb",
                    "name": "DataCollectionEvent"
                }
            ]
        },
        "dataFlows": [
            {
                "streams": [
                    "Microsoft-ASimDnsActivityLogs"
                ],
                "destinations": [
                    "DataCollectionEvent"
```

```
                ]
            }
        ],
    },
    "location": "eastus2euap",
    "kind": "Windows",
    "id": "/subscriptions/3c1bb38c-82e3-4f8d-a115-a7110ba70d05/resourceGroups/DnsBugBash77/pr
    "name": "dnsbugbashws-microsoft-sentinel-asimdnsactivitylogs",
    "type": "Microsoft.Insights/dataCollectionRules",
}
```