Win AMA connectors TSG

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Contents

Relevant connector for this help guide are only windows AMA based-

Windows Security events on AMA Windows Forwarded events

Contact list-

For general questions including agent specifications- Noam Landress, Haim Naamati

For UI questions- Lior Gishry

For Agent deep dive questions-

Manish Goel.

Important links-

AMA official documentation- https://docs.microsoft.com/azure/azure-monitor/agents/azure-monitor-agent-overview?tabs=PowerShellWindows ↗

Azure Monitoring AMA TSG

https://dev.azure.com/Supportability/AzureMonitoringAgents/_wiki/wikis/AzureMonitoringAgents/484791/Windows-AMA-TSG

Windows Security Events official documentation- https://docs.microsoft.com/azure/sentinel/connect-windows-security-events?tabs=LAA ↗

DCR limitations docs- https://docs.microsoft.com/azure/azure-monitor/service-limits#data-collection-rules ↗

Data collection rules explained- https://docs.microsoft.com/azure/azure-monitor/agents/data-collection-rule-overview ↗

Dictionary-

AMA = New Log Analytics agent. Also known as One agent and Azure Monitoring Agent.

MMA = Old Log Analytics agent. Also known as Microsot Monitoring agent.

DCR = A short for Data collection rule. An Azure resource that serves as a configuration rule that hold basic details regarind data collection. For example: what data to collect, from where, and where to send it (worksapce).

DCRA= A short for Data collection rule association. It's a resource that connects between DCRs and machines and tells the agent to download the DCR mentioned in the DCR.

Xpath = A filter one can use in his DCR. The xpath has a specific format and can specifiy what exact event to collect. For example: "Security!*[System[Provider[@Name='4622'] and (Level=3)]]"

This means to collect Security events from level 3 (warning) and of ID 4622.

Issues we will cover in this manual:

1. Data flow issues.
2. UI Issues.
3. Capability issues. Feel free to use the following schema to determine the issue and the neccessary course of action:

Data flow issues-

First it's important to determine which of the 3 following topics the customer issue refers to:

Agent is not getting downloaded to the machine.

Diagnosis:

The customer is not seeing heartbeat events in his workspace. The query to run is (You can use the "Query on customer data help guide

https://eng.ms/docs/cloud-ai-platform/security/cloud-security-group/sentinel/microsoft-azure-sentinel/azure-sentinel-operational-guides/helpguides/how-to-query-on-customer-data):

```
Heartbeat
| where Computer == "computer_hostname_here"
// | where ComputerIP == "another option is to put an IP here"
```

- The customer doesn't have the following directories (ask the customer for a snip/to verify): C:\Packages\Plugins\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent (inside there is the agent version for example):
- directory that looks like this C:\WindowsAzure\Resources{some_long_id}._{Machine name}.AMADataStore
- The customer could also verify the agent version running through the portal by going to the extensions tab in his VM as so-
- Use the same to make sure the customer is not also running the old MMA agent by accident. The extension is called "MicrosoftMonitoringAgent".
- You can also run the following GET command to get the extensions running on the customers VM (The agent extension is called "AzureMonitorWindowsAgent") -

GET
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmName}/extensions/{vmExtensionName}?api-version=2021-07-01

For more information look at the following docs- https://docs.microsoft.com/rest/api/compute/virtual-machine-extensions/get

(Use CSS to fill in the missing information needed for the request)

DCR is not getting downloaded to the machine

Diagnosis:

- Customers mcs\configchunks directory is empty or doesn't contain the relevant DCR just created by the customer (ask the customer to provide it's content):

C:\WindowsAzure\Resources{some_number}._WEFCollectorMachine.AMADataStore\mcs\configchunks

- You can also run the following GET request to fetch all the running DCR's:

GET
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Insights/dataCollectionRules/{dataCollectionRuleName}?api-version=2019-11-01-preview

- The full document is - https://docs.microsoft.com/en-us/rest/api/monitor/data-collection-rules/get

(Use CSS to fill in the missing information needed for the request).

- In case the relevant DCR does seem to be created, It's possible that it's not associated to the machine correctly. Use the following GET command to get the associations list for a specified resource-

GET https://management.azure.com/{resourceUri}/providers/Microsoft.Insights/dataCollectionRuleAssociations?api-version=2019-11-01-preview

- The full document is - https://docs.microsoft.com/en-us/rest/api/monitor/data-collection-rule-associations/list-by-resource

- Each DCR is a json file which is pretty easily readable. Using the creation dates and content, one can determine whether the specific DCR was downloaded already or not (can take up to a couple of minutes for new DCR's to appear). A DCR sample: {"dataSources":[{"configuration":{"scheduledTransferPeriod":"PT1M","xPathQueries":["ForwardedEvents!"*]},"id":"eventLogsDataSource","kind":"winEventLog","streams":[{"stream":"SECURITY_WEF_EVENT_BLOB","solution":"SecurityInsights"}],"sendToChannels":["ods-664a3b4f-9b3a-4a48-9470-2b9c28b032bb"]}],"channels":[{"endpoint":"https://664a3b4f-9b3a-4a48-9470-2b9c28b032bb.ods.opinsights.azure.com","id":"ods-664a3b4f-9b3a-4a48-9470-2b9c28b032bb","protocol":"ods"}]} Explanation: Xpath = "ForwardedEvents!*" Data type = "SECURITY_WEF_EVENT_BLOB" workspace id= 664a3b4f-9b3a-4a48-9470-2b9c28b032bb

Agent can't send data/has delays in ingestions

Diagnosis: Steps a, b are fine but there is no data visible in the workspace/data is ingested after more than 15 minutes.

- Sometimes there can be indicative errors in the agent log file- The log files are in the following directory (Ask CSS to attach it to the ICM)- C:\WindowsAzure\Resources{some_number}}._WEFCollectorMachine.AMADataStore\Configuration And also in this file - C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.Monitor.AzureMonitorWindowsAgent{agent version}

- CSS should sort the files by datetime and provide the latest one (the one with the latest number called- MonAgentHost.{some_number} or extension/extensionHealth.{latest_number} Open the file and search for any indicative errors that might point to the error (fault Xpath for example).

How to handle

- Agent is not getting downloaded to the machine: In the case the customer doesn't have a running agent on the machine please verify with him that there is indeed a DCR in the in his workspace pointing to the specific machine in question. It can be seen from the connecros blade UI as so-

- If there isn't- instruct the customer to create one.

- If there is a DCR but the agent is still not loaded, ask the customer to create a dummy DCR and deleting it. That should retrigger the agent download mechanism.

- If the agent is still not downloaded you can suggeset to the customer to install it manually using the RestAPI as so- https://docs.microsoft.com/en-us/rest/api/compute/virtual-machine-extensions/create-or-update The extension name is "AzureMonitorWindowsAgent"

DCR is not getting downloaded to the machine:

In case the customer complains that he created a DCR but doesn't see data flow to the specific workspace he set (but for others there is no issue), it means one of two scenarios is happening.

- The DCR is visiable in the UI, but data doesn't flow.
- If the DCR is visiable in the UI but not downloaded to the machine (not seen in the mcs/configchunks directory- section B diagnosis for more), then please contact the AMA agent team for asistance.
- The DCR is not visiable in the UI and data doesn't flow. If the DCR is not visiable in the UI please proceed to section 2- UI issues for further investigating.

Data missing/delay in data.

In case data is missing and not due to any scenario mentioned above, the issue might be caused due to failure to process the DCR itself. This usually happends because of a fault Xpath. Whenever a DCR is created with a fault Xpath it can cause the agent to mal-function. Look for any indicative message in the agent log file (section C Diagnosis for more). Also ask the customer for the Xpath he is using and try to recreate the issue with the test machine provided below. When creating the DCR you can put the xpath here: If you ae able to reproduce the issue, it probably means the Xpath is wrong (there are many online tools to verify this too). Also it might be that the customer crossed some sort of limit. Take a look at section 3 (capability issues) below. Share the root cause you found with the customer (If needed- contact Noam Landress for further asistance)

If the situation above is not the case though- please follow the following ingestion help guide-

https://eng.ms/docs/cloud-ai-platform/security/cloud-security-group/sentinel/microsoft-azure-sentinel/azure-sentinel-operational-guides/helpguides/gt/workspaceinvestigation

- In case there is delay in data which is larger then 15 minutes, please validate the following with the cutomer-
- The customer is not running MMA as well as AMA. The customer is not sending more then 5K eps in total (including all of his DCR's). For example- 5K for 1 DCR (2.8K for ARC based setups), or 2.5K if he has 2 DCR's, etc. The customers disk is not full and he has at least 8 cores of CPU. The agent is not outputing any failures (look at bullet C1 to validate in the logs) If after fixing all of the above, the customer is still experiencing the delay, please consult with the Agent team. (contacts are about)

UI issues-

Diagnosis: If the customer is complaining about one of the following issues:

Can't create a DCR in the portal. Can't view the DCR's in the portal (may take up to 15 seconds to apear). Can't delete a DCR. Can't attach the DCR to the customers machine or workspace. Any other limit or exception the customer is getting from the UI. You can try using Rest commands to verify a dcr is indeed suppoed to be visiable/deleted. You can find an explanation how in the "DCR is missing"/ "Agent is not downloaded" sections. If you find a mismatch between the RestAPI calles and the UI, please consult with Lior Gishry. We have looked into many edge cases by now but there could only be more and it is possible either the customer found a bug or his configurtion something wrong. In that case it's best to try and recreate the customers set-up (if possible- by creating a dcr in a similar way the customer is trying).

Capability issues-

In the case the customer/CSS reach out with a query related to AMA, the official documentation by the agent team is mentioned in the important links above The official documentation of the Security Events connector can also be found in the important links above.

Some common questions:

What are the best practices? 5K EPS for 1 DCR with at least 8 cores CPU's and 10GB remaining of free disk space. How to set up the WEF infrustructure? It is very complexed and not supported by us. Manuals can be found online. How many Xpath's can you have per DCR? 100 How many LA workspaces can you connect per DCR? 10. For more questions and limits please view the DCR limits doc above. Test machine for investigantions- This machine is running the Windows Security events connector on AMA:

VM- https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/resource/subscriptions/de5fb112-5d5d-42d4-a9ea-5f3b1359c6a6/resourcegroups/Noamlandress-rg/providers/Microsoft.Compute/virtualMachines/Windows-AMA-Investigation-Machine/overview

IP-40.91.243.202

User name and Password- https://cefinvestkeyvault.vault.azure.net/secrets/Windows-AMA-investigation/df648813b1e94614971d0e247d32dec2

Workspace where the events are sent to- https://ms.portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/6/subscriptionId/de5fb112-5d5d-42d4-a9ea-5f3b1359c6a6/resourceGroup/noamlandress-rg/workspaceName/windowsamainvetigationws

If the machine doesn't work please use the following ARM template to deploy a new one: https://noamstorageaccount.blob.core.windows.net/windowsinvestigation/ExportedTemplate-noamlandress-rg.zip