How to Pull Alerts from SCOM DataBase/DataWare

Here in this I have written and modified some SQL and PowerShell quires to fetch SCOM alerts

First let's talk about a very (within 7 days) recent alert for a particular server since Db has store recent data so we can this from DB and for this we need to run below given query on **DB: -**

```sql
select * from dbo.Alert where AlertParams like '%servername%'
order by TimeRaised desc
```

Here in the above query we have given a parameter with server name so it will only look for alert with this server. But what if we need all alerts from **DB** then we need to remove this parameter and the query will look like this: - (This will give all alerts stored in DB)

```sql
select * from dbo.Alert order by TimeRaised desc
```

To fetch all alerts from DW: -

```sql
select * FROM Alert.vAlert
```

To fetch all alert of last month from DW: -

```sql
select * FROM Alert.vAlert where RaisedDateTime >= DATEADD(day,-30, GETDATE())
```

To fetch all critical alert for last one month from DW:-

```sql
select * from alert.vAlert where Severity=2 and RaisedDateTime >= DATEADD(day,-30,
GETDATE())
```

To fetch alert for particular alert name (Monitor/Rule) from DW: -

```sql
select * FROM Alert.vAlert WHERE AlertName='Percentage Logical Disk Free Space is low'
AND RaisedDateTime >= DATEADD(day,-30, GETDATE())
```

Now suppose we want alert for **disk** only then we can create a filter for Alert description and alert name: - **You can modify it as per your needs** (*Run this on DW)*

```sql
select * FROM Alert.vAlert WHERE Severity=2 and AlertName like '%disk%'and
AlertDescription like '%disk%' and RaisedDateTime >= DATEADD(day,-30, GETDATE())
```

Now we have a question if we want alert older than 7 days then what we can do so for this we need to dig into Dataware since it has the responsibility to store older data.

The below query will fetch alerts from DW which has server name in description field or Server Name in server Name field why we need this coz sometimes in Monitor/Rule settings server name would be alert name so to overcome this issue we have taken 2 fields.

```
Select alert.AlertName, alert.AlertDescription,VME.DisplayName as
ServerName,Alert.RaisedDateTime from
Alert.vAlertResolutionState as ARS INNER JOIN
Alert.vAlertDetail as AD on ARS.AlertGuid = AD.AlertGuid INNER JOIN
Alert.vAlert as alert ON ARS.AlertGuid=alert.AlertGuid INNER JOIN
vManagedEntity as VME ON alert.ManagedEntityRowId=VME.ManagedEntityRowId
WHERE
((path like '%servername%') or (displayname like '%servername%'))
and ARS.ResolutionState = '0'
and RaisedDateTime  between '2018-03-01' and '2018-03-31'
Order by RaisedDateTime Desc
```

After running the above query what I have just noticed that there are some more fields which needs to be added to fetch all alerts (But this is not the best practice to add more and more fields) so I came up with this query, the below query will give all alerts related to server name.

```
SELECT AlertName, AlertDescription, RaisedDateTime
FROM [OperationsManagerDW].[Alert].[vAlert] where ManagedEntityRowId IN
(SELECT  [ManagedEntityRowId]
FROM [OperationsManagerDW].[dbo].[vManagedEntity] where FullName  like
'%servername%' and RaisedDateTime between '2018-03-01 06:09:15.027' and '2018-03-31
13:09:15.027')
```

“Now coming to PowerShell”

To fetch alert from Powershell

We need to follow below steps: -

First open elevated PS on any MS and import operations manager module in it.

To import module, we need to run below command on it.

Import-module operationsmanager

Once we have imported SCOM module we can run any cmdlets related to SCOM

Our main goal is to get alerts from SCOM, so cmdlets to for alerts is as follows: -

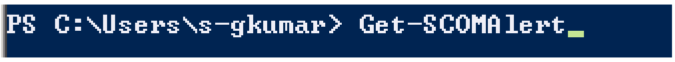
You can check all cmdlets related alert keyword by typing **get-command *alert***

```
PS C:\Users\s-gkumar> get-command *alert*
```

```
Name
 ----
 Add-SCOMAlertResolutionState
 Get-SCOMAlert
 Get-SCOMAlertHistory
 Get-SCOMAlertResolutionSetting
 Get-SCOMAlertResolutionState
 Remove-SCOMAlertResolutionState
 Resolve-SCOMAlert
 Set-SCOMAlert
 Set-SCOMAlertResolutionSetting
```

- To fetch all alerts, we can run command on PS: -

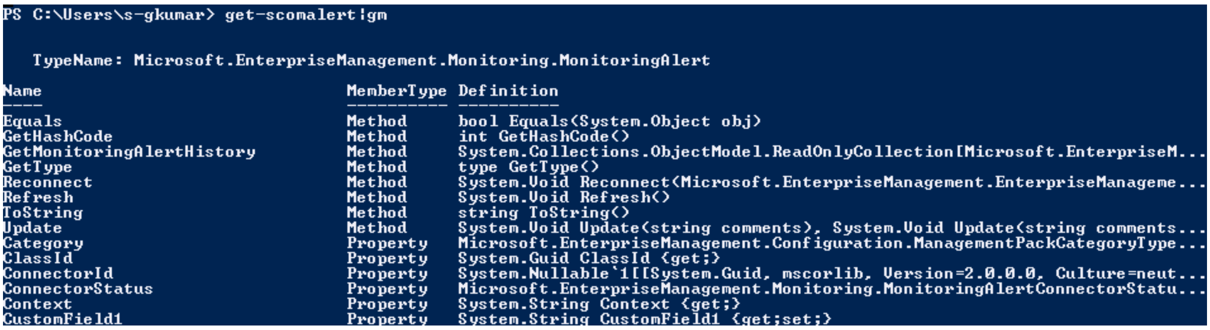
Get-scomalert



```
PS C:\Users\s-gkumar> Get-SCOMAlert_
```

- To fetch all attributes/parameters related to alerts, we can use below command

Get-scomalert|gm



```
PS C:\Users\s-gkumar> get-scomalert|gm


   TypeName: Microsoft.EnterpriseManagement.Monitoring.MonitoringAlert

Name                              MemberType Definition
----                              ---------- ----------
Equals                            Method     bool Equals(System.Object obj)
GetHashCode                       Method     int GetHashCode()
GetMonitoringAlertHistory         Method     System.Collections.ObjectModel.ReadOnlyCollection[Microsoft.EnterpriseM...
GetType                           Method     type GetType()
Reconnect                         Method     System.Void Reconnect(Microsoft.EnterpriseManagement.EnterpriseManageme...
Refresh                           Method     System.Void Refresh()
ToString                          Method     string ToString()
Update                            Method     System.Void Update(string comments), System.Void Update(string comments...
Category                          Property   Microsoft.EnterpriseManagement.Configuration.ManagementPackCategoryType...
ClassId                           Property   System.Guid ClassId {get;}
ConnectorId                       Property   System.Nullable`1[[System.Guid, mscorlib, Version=2.0.0.0, Culture=neut...
ConnectorStatus                   Property   Microsoft.EnterpriseManagement.Monitoring.MonitoringAlertConnectorStatu...
Context                           Property   System.String Context {get;}
CustomField1                      Property   System.String CustomField1 {get;set;}
```

- To fetch all critical alerts

get-scomalert -criteria ‘Severity>=2’

- To fetch all New alerts

get-scomalert -criteria ‘ResolutionState=0’

- Closed Critical Alerts

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=2’

- New Critical Alerts

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=2’

- Closed Warning Alerts

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=1’

- New Warning Alerts

get-scomalert -criteria ‘ResolutionState=0 AND Severity>=1’

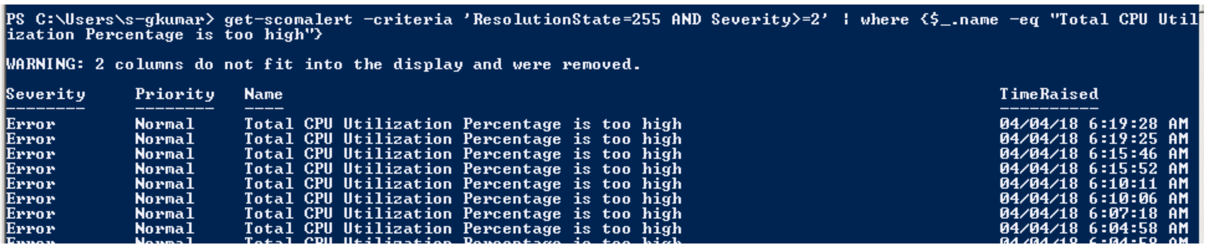
- Now fetching alert with particular name and particular time

Get-SCOMAlert | where{($_.name -like "alertname") -and ($_.timeraised -gt (datefrom)) -and ($_.timeraised -lt (dateto))

Now merging quires and creation of filter

- Now we are going to fetch all **closed, critical** alert for **CPU Utilization** so the query would be as follows: -

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=2’ | where {$_.name -eq "Total CPU Utilization Percentage is too high"}



```
PS C:\Users\s-gkumar> get-scomalert -criteria 'ResolutionState=255 AND Severity>=2' | where {$_.name -eq "Total CPU Util
ization Percentage is too high"}

WARNING: 2 columns do not fit into the display and were removed.

Severity     Priority    Name                                                      TimeRaised
--------     --------    ----                                                      ----------
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:19:28 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:19:25 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:15:46 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:15:52 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:10:11 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:10:06 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:07:18 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:04:58 AM
Error        Normal      Total CPU Utilization Percentage is too high              04/04/18 6:04:58 AM
```

- Now we are going to add some parameters which we are required

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=2’ | where {$_.name -eq "Total CPU Utilization Percentage is too high"} | select MonitoringObjectDisplayName,Name,Severity,ResolutionState,TimeRaised,Parameters,NetBiosComputerName

- Now we if need to export them into sheet, so we can run below command

get-scomalert -criteria ‘ResolutionState=255 AND Severity>=2’ | where {$_.name -eq "Total CPU Utilization Percentage is too high"} | select MonitoringObjectDisplayName,Name,Severity,ResolutionState,TimeRaised,Parameters,NetBiosComputerName | export-csv c:\CPUAlertall.csv

Hope this all will help you to fulfil your requirements, you can modify these queries as per your requirements.

Note: - in SQL query server name would be only server name not FQDN.

For any assistance you can write me to gouravrathore23@gmail.com **or** can reach me on below channels.

Author: - Gourav Kumar

Professional & Social Channels: -

https://www.facebook.com/gourabunpredictable

https://www.linkedin.com/in/gouravrathore/

https://social.technet.microsoft.com/profile/gouravin/