# Windows Server OS Solution

Windows Server OS is an OMS (Operations Management Suite) management solution which aims at providing monitoring, trends and visibility for your Windows Servers.

With easy to use dashboards and queries you will be able to identify issues for the Windows Servers in your environment. The solution ingests windows event logs and performance counters to detect issues and assess the performance of Windows Servers.

## Connected sources

The following table describes the connected sources that are supported by this solution.

|  |  |  |
| --- | --- | --- |
| Connected Source | Support | Description |
| [Windows agents](https://azure.microsoft.com/en-us/documentation/articles/log-analytics-windows-agents/) | Yes | Direct Windows agents ingest windows event logs and performance counters. |
| [Linux agents](https://azure.microsoft.com/en-us/documentation/articles/log-analytics-limux-agents/) | No | Direct Linux agents do not ingest Windows event logs and performance counters. |
| [SCOM management group](https://azure.microsoft.com/en-us/documentation/articles/log-analytics-om-agents/) | Yes | SCOM agents ingest windows event logs and performance counters.  Windows event logs are forwarded to the management group and then to OMS. Windows Performance counters data is send directly to OMS from the SCOM agents. A direct connection from the SCOM agent to OMS is required. |
| [Azure storage account](https://azure.microsoft.com/en-us/documentation/articles/log-analytics-azure-storage/) | No | No data is ingested from Azure storage for this solution. |

## Prerequisites

Before deploying the solution please remove the following data sources from OMS Portal:

* Windows Event Logs
  + System
  + Application
* Windows Performance Counters
  + Memory(\*)\Available MBytes
  + Memory(\*)\Free System Page Table Entries
  + Memory(\*)\Pages/sec
  + Processor(\_Total)\% Processor Time
  + System(\*)\Processor Queue Length
  + Memory(\*)\% Committed Bytes In Use
  + LogicalDisk(\*)\% Free Space
  + LogicalDisk(\*)\Current Disk Queue Length
  + LogicalDisk(\*)\Disk Transfers/sec
  + LogicalDisk(\*)\Avg. Disk sec/Transfer

This step will ensure successful deployment of the solution. The data sources will be added once the solution is deployed successfully.

Supported Operating Systems:

* Windows Server 2008 R2 SP1 and above

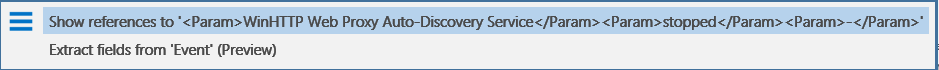
## Configuration

After first deployment of the Windows Server OS Solution please wait 15-20 minutes until data from Windows Servers is being ingested into your OMS workspace. After that custom fields with the following name needs to be created:

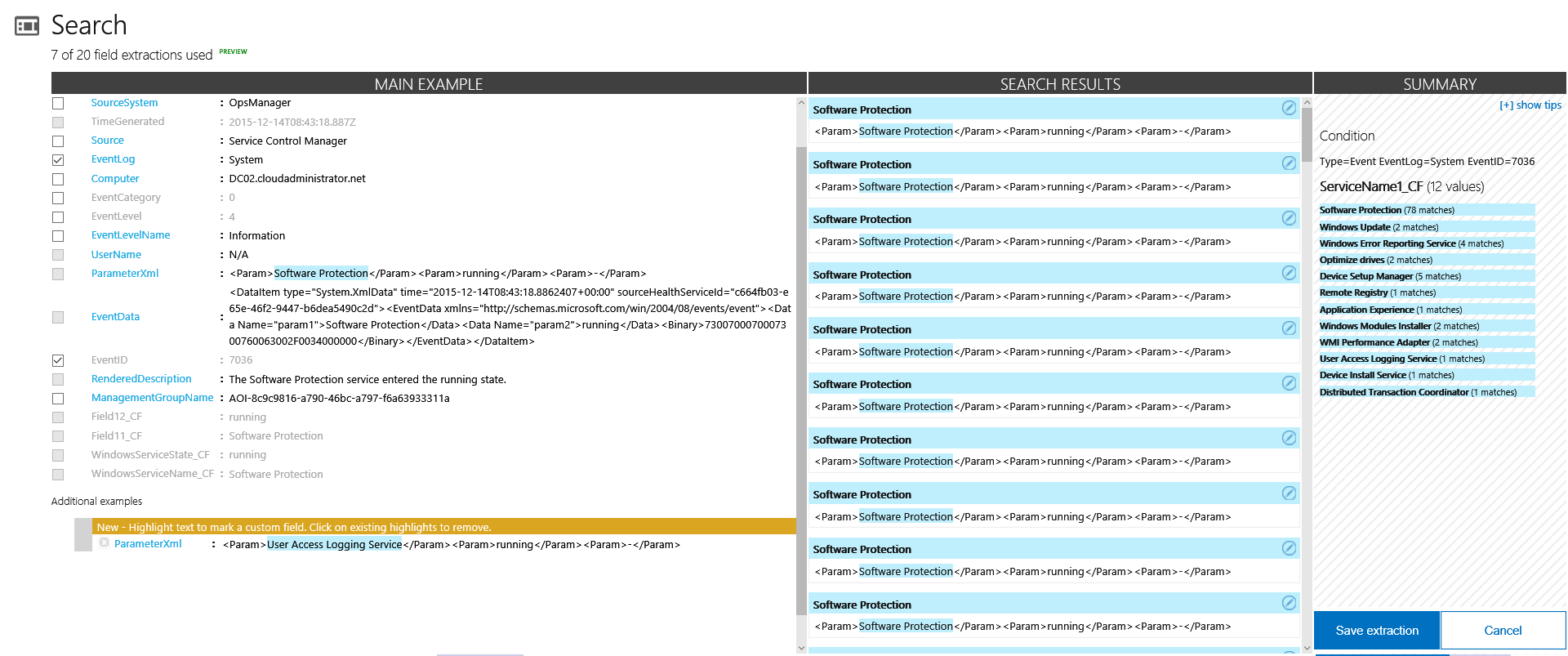
* WindowsServiceName\_CF
* WindowsServiceState\_CF

Execute the following steps to create them:

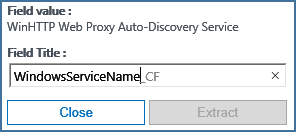
1. Login to OMS Portal.
2. Click on Log Search tile.
3. Execute the following query: *(Type=Event) (EventID=7036) Source="Service Control Manager"* and make sure results appear.
4. Expand all fields of the first result by clicking show more beneath it.
5. Click on the hamburger menu next to **ParameterXML** field and click on **Extract** fields from 'Event'.



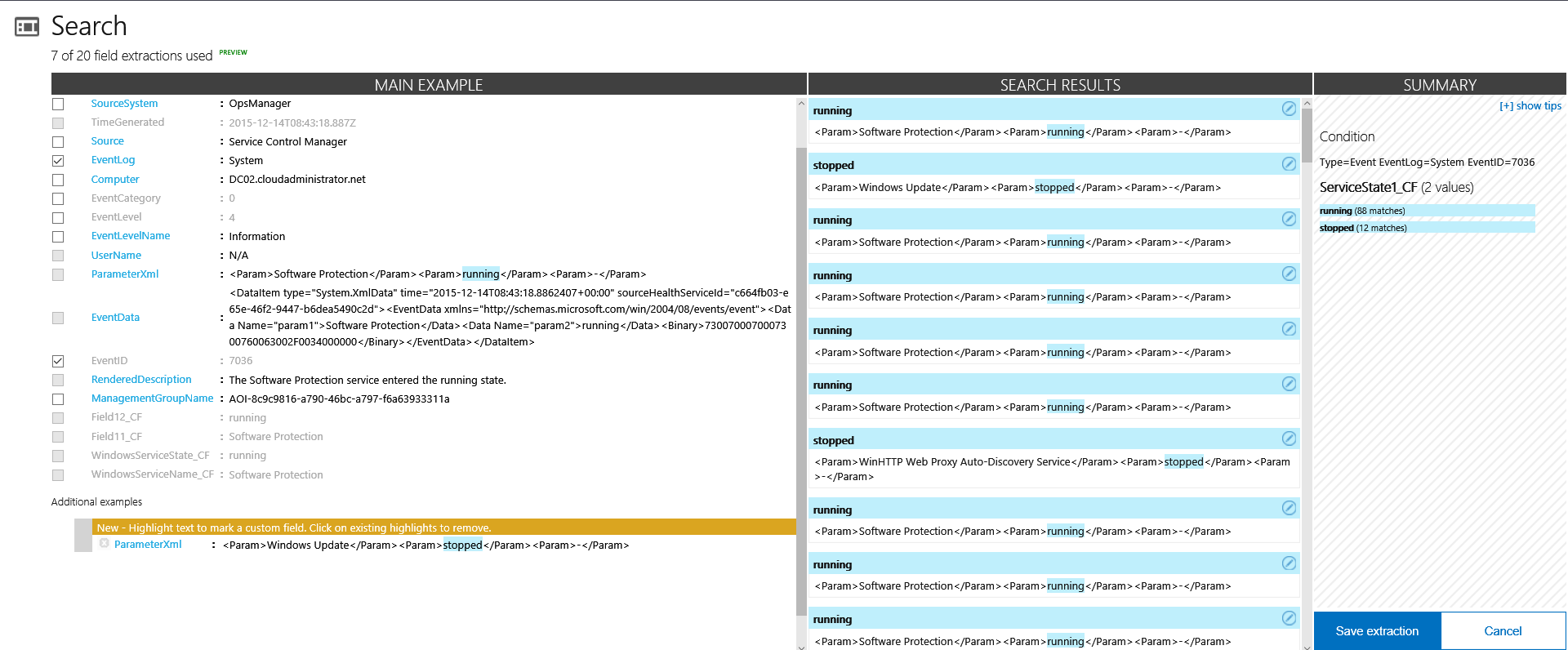
1. From Extract Field page in the Main Example section select service name from **ParameterXML** field as shown in the example. Make sure to select the full name of the service that is located between **<Param>** and **</Param>** tags.



1. Enter **'WindowsServiceName\_CF'** in Field Title and click Extract.



1. Make sure that all service names are correctly shown in Search Results and Summary sections. If some of the results is incorrect click on the edit icon right of the results and correct it.
2. When done click Save extraction.
3. Repeat the same steps to extract service state from **ParameterXML** field. For Field title use **'WindowsServiceState\_CF'.**



## Management packs

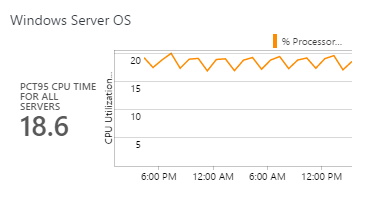
If your SCOM management group is connected to your OMS workspace, then the following management packs will be installed in SCOM when you add this solution. There is no configuration or maintenance of these management packs required.

* Microsoft System Center Advisor Log Management Collection (Microsoft.IntelligencePack.LogManagement.Collection)
* Microsoft System Center Advisor Performance collection library (Microsoft.IntelligencePacks.Performance)

For more information on how solution management packs are updated, see [Connect Operations Manager to Log Analytics](https://azure.microsoft.com/en-us/documentation/articles/log-analytics-om-agents/).

## Using the solution

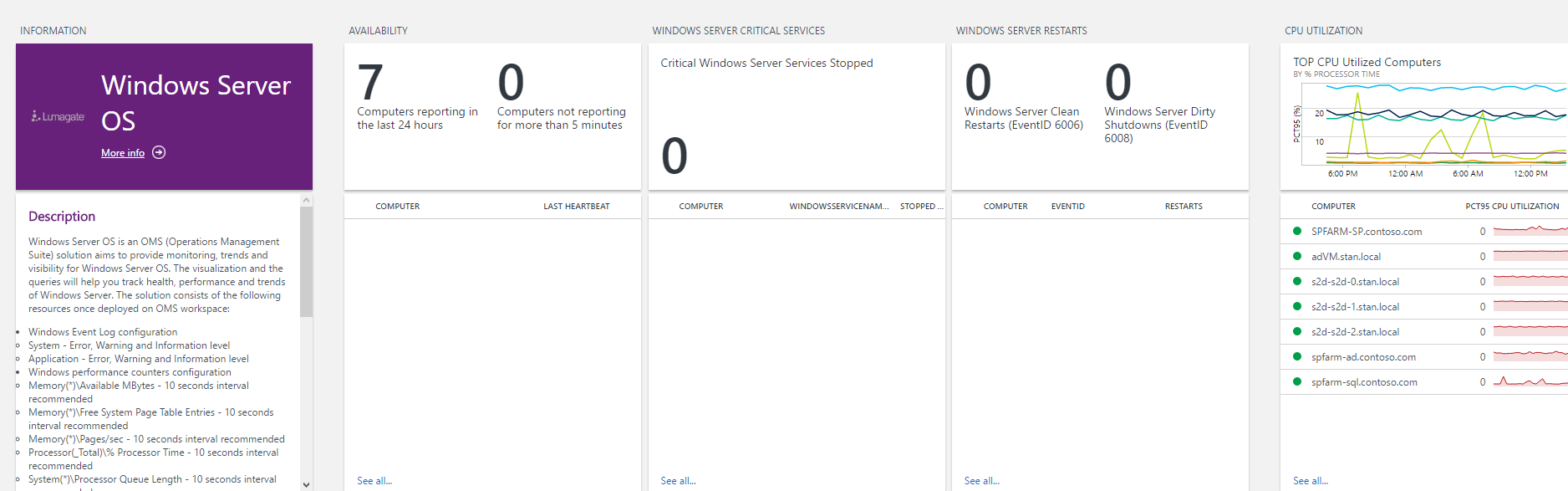
When you add the Windows Server OS solution to your OMS workspace, the **Windows Server OS** tile will be added to your OMS dashboard. This tile displays percentile 95 CPU Time on all Windows Servers in your OMS workspace and graphical representation of it within the last 24 hours. You cannot change this time range.

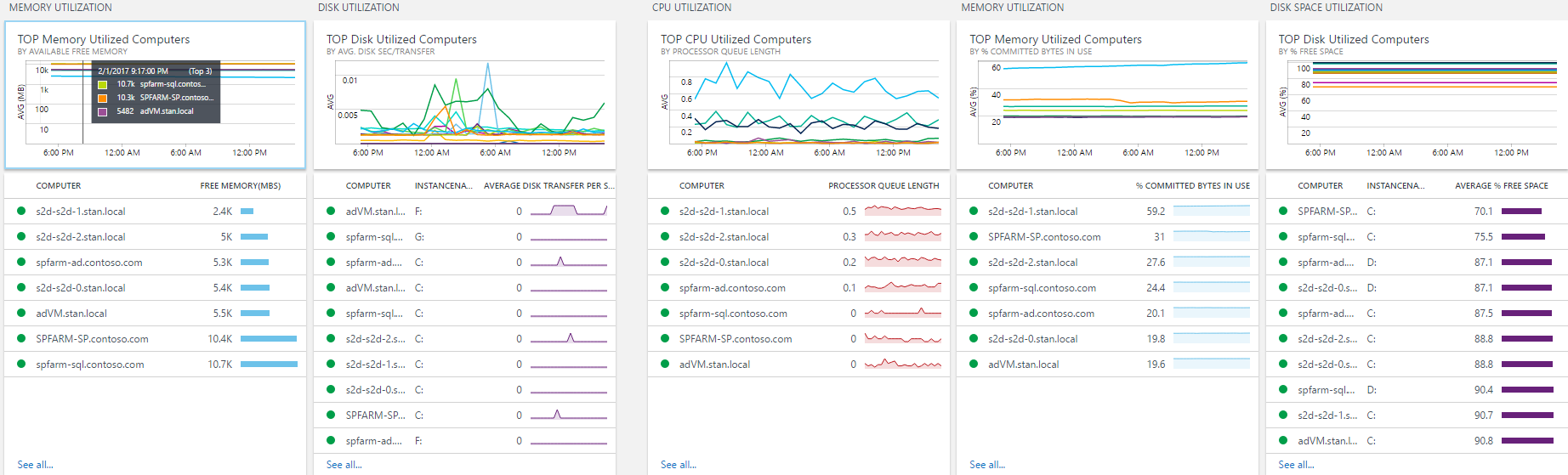


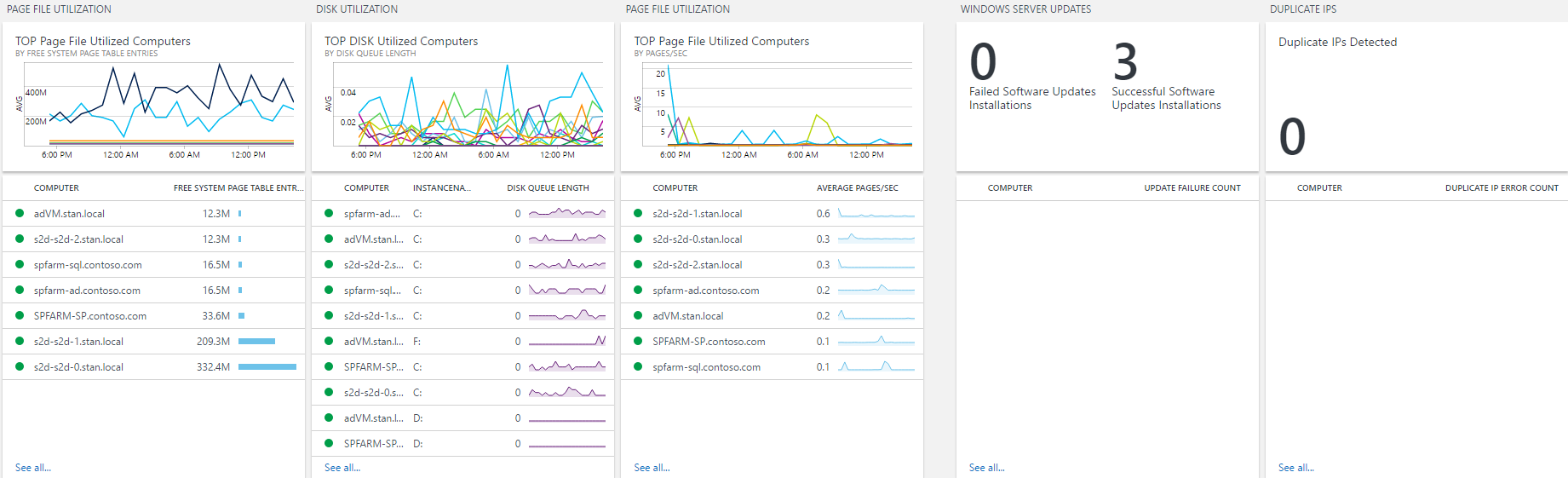
Click on the **Windows Server OS** tile to open the **Windows Server OS** dashboard. The dashboard includes the columns in the following table.

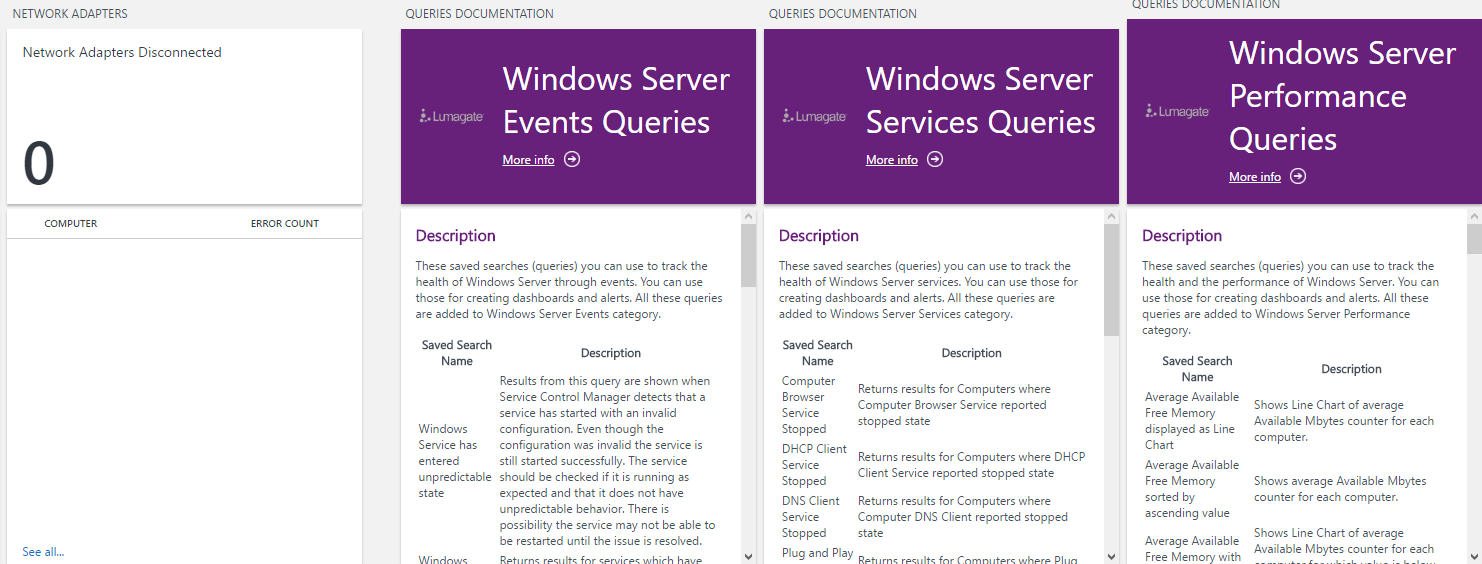
|  |  |
| --- | --- |
| Column | Description |
| Information | Short decrepitation of the solution. |
| Availability | Lists number of Windows Servers reporting to OMS and number of Windows Servers not reporting to OMS for the last 5 minutes. Any non-reporting Windows Server will be listed along with last heartbeat time. |
| Windows Server Critical Services | Lists any critical windows server service stopped for the selected time frame. It does not indicate the current status of the service just if there was stop event. The following services are being tracked: "Windows Remote Management (WS-Management)", "Windows Firewall", "Workstation", "Windows Event Log", "TCP/IP NetBIOS Helper", "Server", "Plug and Play", "DNS Client", "DHCP Client" and "Computer Browser". |
| Windows Server Restarts | Lists any restart events that happened on Windows servers. EventID 6006 is for clean restarts and EventID 6008 is for dirty restarts (BSOD and etc.) |
| CPU Utilization – Top CPU Utilized Computers by % Processor Time | Shows percentile 95 for % processor time for each server. Lists top 10 servers with highest value. In the table the last value for % Processor Time is shown for each server. If value exceeds 80% threshold reaches Warning level, if it exceeds 90 % it reaches Critical level. |
| Memory Utilization – Top Memory Utilized Computers by Available Free Memory | Shows top ten servers with lowest available free memory. Values are in MBs. If value is below 300 Warning threshold is reached, if value is below 200 Critical threshold is reached. |
| Disk Utilization – Top Disk Utilized Computers by Avg. Disk Sec/Transfer | Shows average value for Avg. Disk Sec/Transfer counter on each server and disk. Top ten servers with highest value are listed in the table. In that table, last value for that counter is listed. If value is above 0.03 threshold reaches Warning, if value is above 0.0.4 it reaches Critical level. |
| CPU Utilization – Top CPU Utilized Computers by Processor Queue Length | Shows top ten servers with highest average Processor Queue Length value. If value is above 15 Critical threshold is reached. |
| Memory Utilization – Top Memory Utilized Computers by % Committed Bytes in Use | Shows top ten servers with highest average % Committed Bytes in Use. If value is above 80% critical threshold is reached. |
| Disk Space Utilization – Top Disk Utilized Computers by % Free space | Shows top ten servers and drives with lowest % free disk space. If drive is below 15 % warning threshold is reached, if drive is below 10% critical threshold is reached. |
| Page File Utilization – Top Page File Utilized Computers by Free System Page Table Entries | Shows top ten servers with lowest average value for Free System Page Table Entries. If value is below 5000 critical threshold is reached. |
| Disk Utilization – Top Disk Utilized Computers by Disk Queue Length | Shows top ten servers and drives with highest average disk queue length value. If value is above 2 Critical threshold is reached. |
| Page File Utilization – Top Page File Utilized Computers by Pages/sec | Shows top ten servers with highest average value for Pages/sec. If value is above 5000 critical threshold is reached. |
| Windows Server Updates | Shows count of failed and successful Windows Updates on all windows server for the time frame selected. In the table servers with failed updates installations are listed along with the count of failed updates. |
| Duplicate IPs | Shows count of duplicate IP errors detected. In the table lists the servers with duplicate IP errors and their count. |
| Network Adapters | Shows network adapters disconnected errors detected count. The table lists the servers with network adapters disconnect errors and their count. |
| Queries Documentation – Windows Server Events Queries | Provides documentation for all saved searches deployed within Windows Server Events query category. These queries can be used for additional troubleshooting and alert creation. |
| Queries Documentation – Windows Server Services Queries | Provides documentation for all saved searches deployed within Windows Server Services query category. These queries can be used for additional troubleshooting and alert creation. |
| Queries Documentation – Windows Server Performance Queries | Provides documentation for all saved searches deployed within Windows Server Performance query category. These queries can be used for additional troubleshooting and alert creation. |

If you scroll to the right, to walk through all columns.









## Input data

The Alert Management solution analyzes records in the OMS repository with a type of **Event** and **Perf**. These are populated by the windows event logs and windows performance counters ingested by the solution. The interval for windows performance counters is chosen during the solution deployment. Default value is 10 seconds.

## Output data

The solution uses the standard types **Event** and **Perf** and their properties. Additional properties **WindowsServiceName\_CF** and **WindowsServiceState\_CF** are created for type **Event** as descried in Configuration section. These custom records properties are described the following table.

|  |  |
| --- | --- |
| Property | Description |
| Type | *Event* |
| Windows ServiceName\_CF | Name of a Windows Service as listed in services.msc |
| WindowsServiceState\_CF | Registered state for Windows Service. Can be either running or stopped. |

## Sample log searches

The following table provides sample log searches for alert records collected by this solution.

|  |  |
| --- | --- |
| Query | Description |
| Type=Event (EventLog=Application) (Source="Wininit") (EventID=101) | CHKDSK Operation Occurred on Startup |
| Type=Event (EventLog=System) (Source="DISK" OR Source="Ntfs") (EventID=41 OR EventID=55) | NTFS File System Corrupt |
| Type:Perf (ObjectName=Memory) (CounterName="Available Mbytes") Computer IN {Type=Heartbeat OSType=Windows | Distinct Computer} | Measure Avg(CounterValue) as AVGAvailableFreeMemoryInMBs by Computer | display LineChart | Average Available Free Memory displayed as Line Chart |
| Type:Perf (ObjectName=Memory) (CounterName="Available Mbytes") Computer IN {Type=Heartbeat OSType=Windows | Distinct Computer} | sort TimeGenerated DESC | Dedup Computer | EXTEND if(map(CounterValue,0,200,1,0),"Critical","Normal") as AvailableFreeMemoryLevel | Last value for Available Free Memory marked with Critical for less than 200 MBs and with Normal for greater than 200 MBs per computer |
| Type:Perf (ObjectName=LogicalDisk) (CounterName="% Free Space") CounterPath!=\*\_Total\* InstanceName!=HarddiskVol\* Computer IN {Type=Heartbeat OSType=Windows | Distinct Computer} | sort TimeGenerated DESC | Dedup CounterPath | EXTEND if(map(CounterValue,0,10,1,0),"Critical","Normal") as FreeDiskSpaceLevel | Last value for Free Disk Space marked with Critical for less than 10 Percent and with Normal for greater than 10 Percent per drive |
| Type:Perf (ObjectName=Memory) (CounterName="Available Mbytes") Computer IN {Type=Heartbeat OSType=Windows | Distinct Computer} | Measure Avg(CounterValue) as AVGAvailableFreeMemoryInMBs by Computer | Sort AVGAvailableFreeMemoryInMBs ASC | Average Available Free Memory sorted by ascending value |