

White paper

Integration options for PRIMERGY Servers into Microsoft Operations Management Suite (OMS)

This white paper describes some technical possibilities and the current limitations to extend the available functionality of a Microsoft Azure Operations Management Suite Workspace by collecting performance and health state data for Fujitsu PRIMERGY servers which are monitored by a Microsoft System Center Operation Manager (SCOM) Management Group.



Contents

1.	Introduction	3
1.1.	Purpose and target groups	3
1.2.	Changes since the last edition	3
1.3.	Notational Conventions	4
1.4.	Related Links	4
2.	Integration requirements	6
3.	Installation and setup	7
3.1.	Setting up a Microsoft Operations Management Suite workspace	7
3.2.	Registering a SCOM Management Group to OMS	7
4.	Log Analytics	9
4.1.	Recommended OMS Solutions	9
4.2.	Enabling Data Sources	10
4.3.	SCOM Alert forwarding	10
4.4.	Custom Windows Event Log forwarding	10
4.5.	Performance Data forwarding from Managed Computers	11
4.6.	SCOM Performance Data forwarding with custom rules	12
5.	Custom Views	13
5.1.	Creating and editing custom views	13
5.1.1.	Create a new view	13
5.1.2.	Edit an existing view	13
5.1.3.	Clone an existing view	14
5.1.4.	Delete an existing view	14
5.1.5.	Export an existing view	14
5.1.6.	Import an existing view	14
5.2.	Custom Views for Performance Data	15
5.2.1.	Power Consumption Performance Data of Windows servers	15
5.2.1.1.	Custom View creation	16
5.2.2.	Custom Performance Data of Fujitsu PRIMERGY servers	19
5.2.2.1.	Ambient Temperature Performance Data Monitoring	19
5.2.2.2.	Temperature History' View	21
5.2.2.3.	'Temperature Distribution by Computer' View	22
5.2.3.	Power Consumption Performance Data Monitoring	23
5.2.3.1.	'PRIMERGY Power Consumption by Computer' View	24
5.2.3.2.	'Power Consumption over Time' View	26
5.3.	Health State Monitoring with OMS	26
5.4.	Implementation details	27
5.5.	Defining Custom Health State Views based on the available OMS data	28
5.5.1.	'PRIMERGY Server Health State' View	29
5.5.2.	Number of 'PRIMERGY Server sending Data' View	30
5.5.3.	Number of 'PRIMERGY Server with Warning State' View	31
5.5.4.	Number of 'PRIMERGY Server with Critical State' View	32
5.5.5.	Number of 'PRIMERGY Server in SCOM' View	33
5.5.6.	'List of Queries' View	34
5.6.	Further analyze SCOM Alerts in OMS with Custom Fields	35
5.7.	Create Custom Views with Custom Fields	37
5.7.1.	'iRMC Login and AVR Started' View	37
5.7.2.	'iRMC Traps by Severity' View	38
6.	Appendix	39
6.1.	Management Packs	39
6.1.1.	Fujitsu ServerView Server - Collect Health State to OMS	39
6.1.2.	Collect Performance Data to OMS Management Packs	40
6.2.	iRMC Trap Numbers	41
6.3.	Custom Views	42

1. Introduction

The FUJITSU Software ServerView® suite provides a well proven and comprehensive tool set to manage Fujitsu PRIMERGY and PRIMEQUEST systems throughout their lifecycle. The suite includes several ServerView® integration modules which enable Fujitsu servers to be integrated easily into other enterprise management systems.


Microsoft System Center Operation Manager (SCOM) provides the generic infrastructure to monitor a given local customer datacenter infrastructure including Software or Hardware based entities. Fujitsu PRIMERGY Server Integration Packs for different Operating Systems or even Out-Of-Band monitoring provide detailed modelling, monitoring and performance data collection of the underlying server hardware and software components.

Microsoft Operations Management Suite (OMS) is Microsoft's cloud-based Management Platform that complements a customer's System Center investment to enable new, cloud integrated management scenarios. OMS extends existing System Center capabilities to deliver a full hybrid management experience across any on premise datacenter or cloud.

This white paper focusses on the technical options to extend the existing SCOM to OMS integration and provides various step by step instructions to monitor and visualize different aspects of Fujitsu PRIMERGY Servers in an OMS workspace, extending the classical SCOM based Management into the Microsoft Cloud on top of existing Fujitsu PRIMERGY Server SCOM Integration modules.

The referenced additional Management Packs and Custom View definitions are provided on the latest PRIMERGY ServerView Suite DVD2 from Fujitsu Technology Solutions or under:

http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/

 The queries used as examples of this white paper have been converted to the new 'Azure Log Analytics' language. If you had previously installed any of the provided custom views these will automatically be converted during your workspace upgrade.

1.1. Purpose and target groups




This manual is intended for system administrators, network administrators and service technicians who have a thorough knowledge of hardware and software. Likewise, a sound basic knowledge of the Microsoft System Center Operations Manager 2016 / 2012 R2 and Microsoft Azure or Microsoft Operation Management Suite (OMS) is required.

1.2. Changes since the last edition

- Change the custom log name from SVTEST into SVHEALTH.
Please re-import the custom health view to reflect this change in OMS.
- Change the target for the 'Fujitsu ServerView Collect Health State to OMS' rule from 'Management Server' to 'Management Group' to prevent sending the same data multiple times to OMS.
- Update the queries to the new 'Azure Log Analytics' language.
- Updated Out-of-Band Collect Performance Data to OMS Management Pack due to changed Run-As account in SCOM for the Fujitsu integrated Remote Management Controller (iRMC).
- Updated Management Pack Description strings.
- Updated OMS Home Page link to <http://www.microsoft.com/OMS>

1.3. Notational Conventions

The following notational conventions are used in this manual:

	Warning This symbol is used to draw attention to risks which may represent a health hazard or which may lead to data loss or damage to the hardware
	Information This symbol highlights important information and tips.
	This symbol refers to a step that you must carry out in order to continue with the procedure.
<i>italics</i>	Commands, menu items, names of buttons, options, file names and path names are shown in italics in descriptive text.
<variable>	Angle brackets are used to enclose variables which are replaced by values.

Screen output

Please note that the screenshots shown in this manual may not correspond to the output from your system in every detail. System-related differences between the menu items available can also arise.

1.4. Related Links

The following links prove technical details and background information:

[1]	Microsoft 'Operations Management Suite' (OMS) Start Page	http://www.microsoft.com/OMS
[2]	Microsoft 'Operations Management Suite' Workspace Selection	https://mms.microsoft.com
[3]	Inside the Microsoft Operations Management Suite (eBook)	https://gallery.technet.microsoft.com/Inside-the-Operations-2928e342
[4]	Log Analytics Overview	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-overview/
[5]	Log Analytics Search Reference	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-search-reference/
[6]	Log Analytics View Designer	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-view-designer/
[7]	Log Analytics HTTP Data Collector API	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-data-collector-api/
[8]	Custom Log File as Data Source in Log Search	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-data-sources-custom-logs/
[9]	Custom Fields in Log Search	https://azure.microsoft.com/en-us/documentation/articles/log-analytics-custom-fields/
[10]	Connect Operation Manager (SCOM)	https://azure.microsoft.com/en-us/documentation/articles/log-

	to Log Analytics (OMS)	analytics-om-agents/
[11]	OMS is not SCOM (Blog Entry)	https://cloudadministrator.wordpress.com/2016/08/12/msoms-is-not-scom/
[12]	OMS Survival Guide (Wiki from Pete Zerger)	https://social.technet.microsoft.com/wiki/contents/articles/31909.ms-operations-management-suite-survival-guide.aspx
[13]	Sign up for an OMS Trial Version	https://www.microsoft.com/en-us/cloud-platform/operations-management-suite-trial

2. Integration requirements

The requirements specified below must be satisfied for integration.

Microsoft Operations Management Suite workspace

- A valid Microsoft account or corporate account in order to use any Microsoft Azure Cloud solution.
- A valid Azure Subscription is needed to use OMS. You can use the free trial version of OMS with limited amount of data but must link it to an Azure Subscription.
- A Standard or Premium Data Plan for your OMS workspace is recommended. These paid subscriptions have unlimited data per day and differ only in the retention period of the stored log data.
- Alternatively, Microsoft provides a free trial version of OMS which is limited by the data amount which can be sent per day (currently 500Mbytes/day) as well as a fixed 7day retention period of the stored log files. Depending on your monitoring scenarios and installed standard Microsoft Solutions the daily amount of data sent to the cloud varies. This white paper assumes that you do not have exhausted your daily data volume when using the free trial or have a paid subscription with unlimited data per day.



You can change the data plan for your OMS workspace under:
Setup → Accounts → Azure Subscription and Data Plan

- Web Browser: not all features of an OMS workspace are always visible or rendered the same way with different web browsers (e.g. extracting custom fields from an alert was easier with Chrome than Firefox). You may need to try a different browser for a certain feature to work as described. Google Chrome was used for the screenshots in this white paper.

Management Station

- Microsoft System Center 2016 or 2012 R2 Operations Manager with installed latest updates.
- Installed updated Advisor Management Packs.



For SCOM 2012 R2 make sure you have updated to the latest Update Release and have also installed the updated Advisor Management Packs before connecting your SCOM to OMS.
See section [3.2](#) for details.

- Successful registration of your SCOM Management Group(s) to OMS
- Installed .NET Framework 4.5 or later is highly recommended
- Installed Fujitsu ServerView Management Pack for your Operating System or Out-Of-Band Monitoring via the integrated Remote Management Controller (iRMC).
Optional, needed to report overall server health to OMS.
- Installed Fujitsu PRIMERGY Performance Monitoring Management Packs for your Operating System to support Temperature and Power Consumption data collection.
Optional, only needed when collecting Temperature or Power Consumption performance data to OMS.
 - The 'Collect Performance Data to OMS' rules use the same data sources as the regular Fujitsu PRIMERGY SCOM performance collection rules and can be enabled and configured independently.

Managed PRIMERGY servers





- When using Out-Of-Band Monitoring: Network access to the embedded Management Controller iRMC S4 or iRMC S5 (integrated Remote Management Controller).
- Appropriate ServerView® Agents or ServerView® CIM Providers installed on the managed PRIMERGY servers (see documentation for Windows/Linux/ESXi Integration Packs).

3. Installation and setup

3.1. Setting up a Microsoft Operations Management Suite workspace

You can setup a basic OMS workspace with a few clicks which is ready to use within minutes. A free trial version is available from <http://www.microsoft.com/OMS> or you can create an OMS workspace from your existing Azure Subscription page. Alternatively you can create the OMS workspace on demand when executing the 'Register to Operations Management Suite' Wizard from SCOM by specifying a non-existing workspace id.


After the OMS workspace has been created you have to configure where the data is collected from by either installing the standalone Microsoft OMS Management Agent (Windows or Linux) or connect an existing SCOM installation to OMS.

-  The integration options described within this white paper require that you have successfully registered your SCOM Management Group(s) to your OMS workspace. The additional functionality is implemented by means of standard SCOM Management Packs which need to be installed into your Management Group. Extending the functionality of the standalone Microsoft Management Agents is not covered by these Management Packs or this white paper.
-  **Important:** After you have connected your SCOM installation to OMS you need to **add all** your SCOM Management Servers from the Management Group to the OMS 'Managed Computers' in the SCOM Console → Administration → Operations Management Suite → Managed Computers. If you do not include all SCOM Management Servers some workflows running on these SCOM Servers might not be able to send data to OMS.
-  It is recommended (but not required) that you setup the OMS workspace before registering your SCOM Management Group to OMS, otherwise the required workspace will be created on demand and you will have to finish some steps after you have received the confirmation E-Mail.
-  If you are using or planning to use some of the Microsoft provided OMS Solutions for your Windows systems: After you have connected your SCOM installation to OMS you need to specify which (Windows or Linux) systems you want to monitor by adding them to the 'Managed Computers' in the SCOM Console → Administration → Operations Management Suite → Managed Computers.

3.2. Registering a SCOM Management Group to OMS

In order send data from a SCOM Management Group to an OMS workspace you have to register your SCOM installation to OMS by finishing the Wizard from the SCOM Console under Administration → Operations Management Suite → Connection.

If you have not yet setup your OMS workspace it will be created on demand. Multiple E-Mails inform about the progress.

-  Currently a SCOM Management Group can send data only to only a single OMS workspace while the dedicated OMS Management Agent for Windows or Linux support multi-homing (e.g. send data to multiple OMS workspaces and multiple SCOM Management Groups).

i Make sure you have updated to the latest Update Release before connecting your SCOM to OMS.

i SCOM2012 R2: Make sure you have installed the updated Advisor Management Packs before connecting your SCOM to OMS; otherwise the registration of your SCOM Management Group to OMS may fail.

The following updated Advisor Management Packs have to be imported since they **are not installed by default** when you update SCOM 2012 R2:

- Microsoft.SystemCenter.Advisor.Internal.mpb
- Microsoft.SystemCenter.Advisor.mpb

The location of the updated Advisor Management Packs is:

[file:///C:/Program Files/Microsoft System Center 2012 R2/Operations Manager/Server/Management Packs for Update Rollups](file:///C:/Program%20Files/Microsoft%20System%20Center%202012%20R2/Operations%20Manager/Server/Management%20Packs%20for%20Update%20Rollups)

After importing the updated Advisor Management Packs it is recommended to close and re-open your SCOM console.

i In order to send data via https to OMS your SCOM environment needs a connection to the internet. If you are using a proxy you have to **manually** configure this proxy as well for OMS. This is independent from the system wide windows proxy configuration.

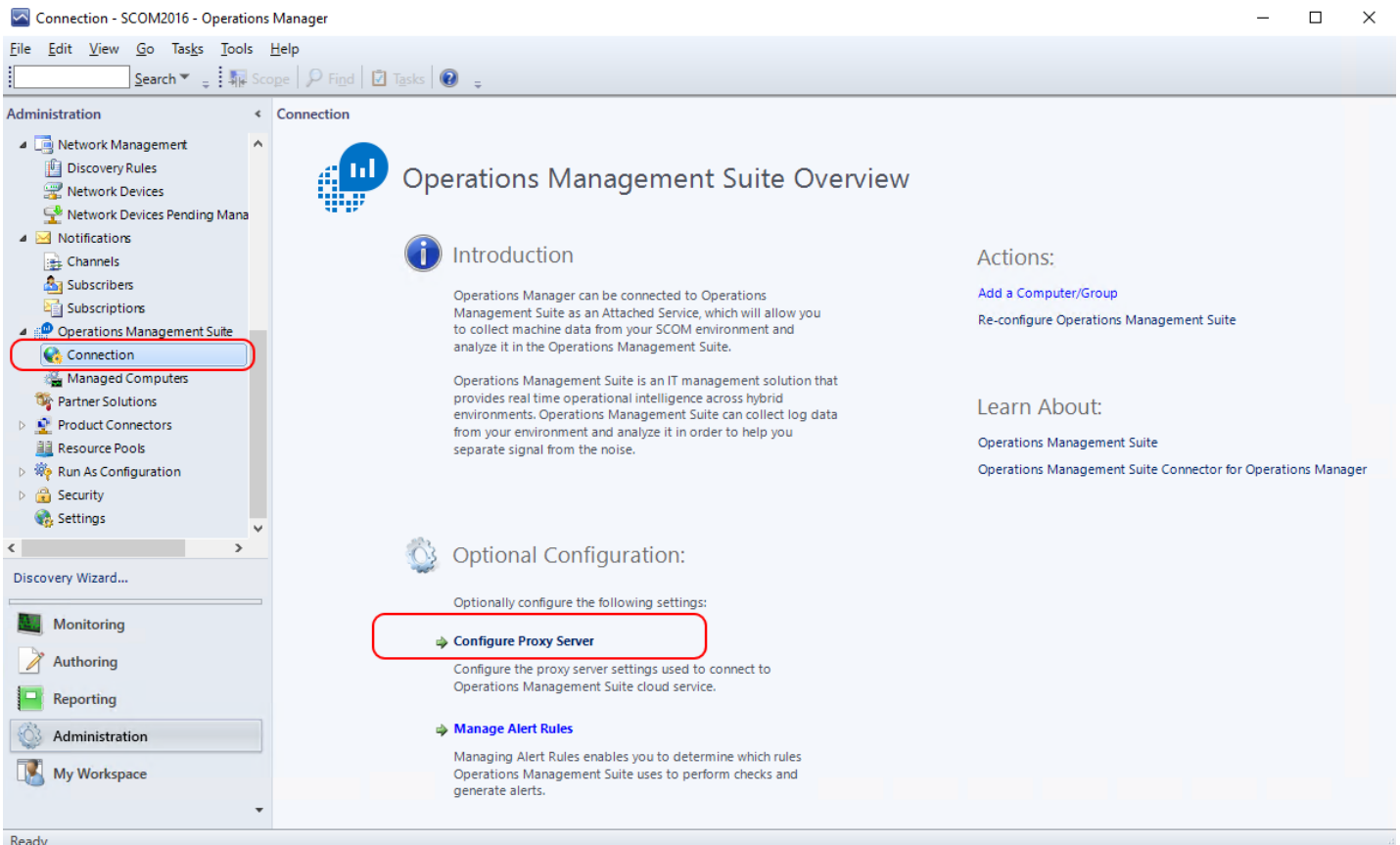


Figure 1 - Proxy Configuration for OMS

4. Log Analytics

Log Analytics is the basic building block for any OMS functionality. "Log Analytics helps you collect, correlate, search, and act on log data. It gives you real-time operational insights using an integrated search, custom dashboards, and Microsoft developed solutions for data analytics via Solution Gallery. Log Analytics enables you first to collect machine data from all your on-premises and cloud infrastructure and then to gain deep insights into the data from your environment through intelligent search, analysis and visualization. Log analytics in OMS enables you to interact with real-time and historical machine data to rapidly develop insights to drive decisions." [1]

For an introduction see [1] [4]. The available data can be queried with a powerful query language [5] and visualized by custom or pre-defined views.

4.1. Recommended OMS Solutions

The following standard OMS solution packs are recommended for SCOM / OMS integration:

- **Log Search**
Provides ability to collect and analyze logs and events from all your computers
- **Alert Management** (recommended)
View your Operations Manager and OMS alerts to easily triage alerts and identify the root causes of problems in your environment.
- **Agent Health** (recommended)
The Agent Health solution gives customers insight into the health, performance and availability of their agents (both Windows and Linux agents) based on the agents heartbeat.
- **Custom Logs** (recommended)
- **View Designer** (required for the step by step instructions of this white paper)

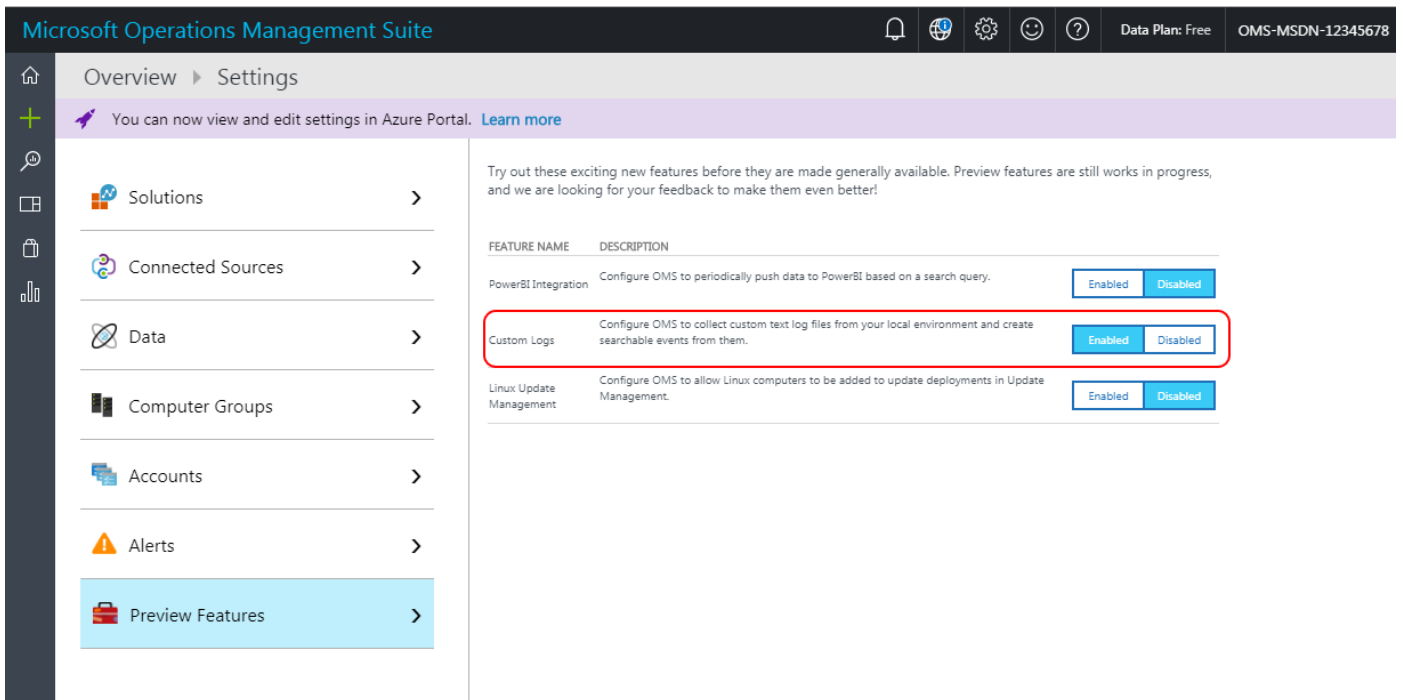


Figure 2 - OMS Public Preview Features (optional)


4.2. Enabling Data Sources

In addition to the installed OMS solutions you may want to configure additional data sources for your OMS workspace. Available Data Sources include (but are not limited to):

- Application specific Windows Event Logs
(e.g. 'Operations Manager' to forward SCOM related Critical or Warning events to OMS)
- Windows / Linux Performance Counters of Managed Computers
(e.g. 'Processor(_Total)\% Processor Time' or 'Power Meter(_Total)\Power')
- Generic Performance Counter available from SCOM
- Custom Log Files
- Custom Fields

4.3. SCOM Alert forwarding

This is part of the Microsoft 'Alert Management' solution in OMS and automatically forwards all SCOM alerts to OMS including alerts related to non-Windows systems. This gives an administrator the possibility to view alerts from his existing/entire SCOM environment within a cloud based solution with any Web Browser or from within one of the dedicated Microsoft OMS Apps for Android or iOS.

 The alerts are sent to OMS as raw SCOM alerts. Parameter substitution is not performed which may result in some cryptic looking entries (e.g. AlertName:"Fujitsu Out-Of-Band {0} : {1}").

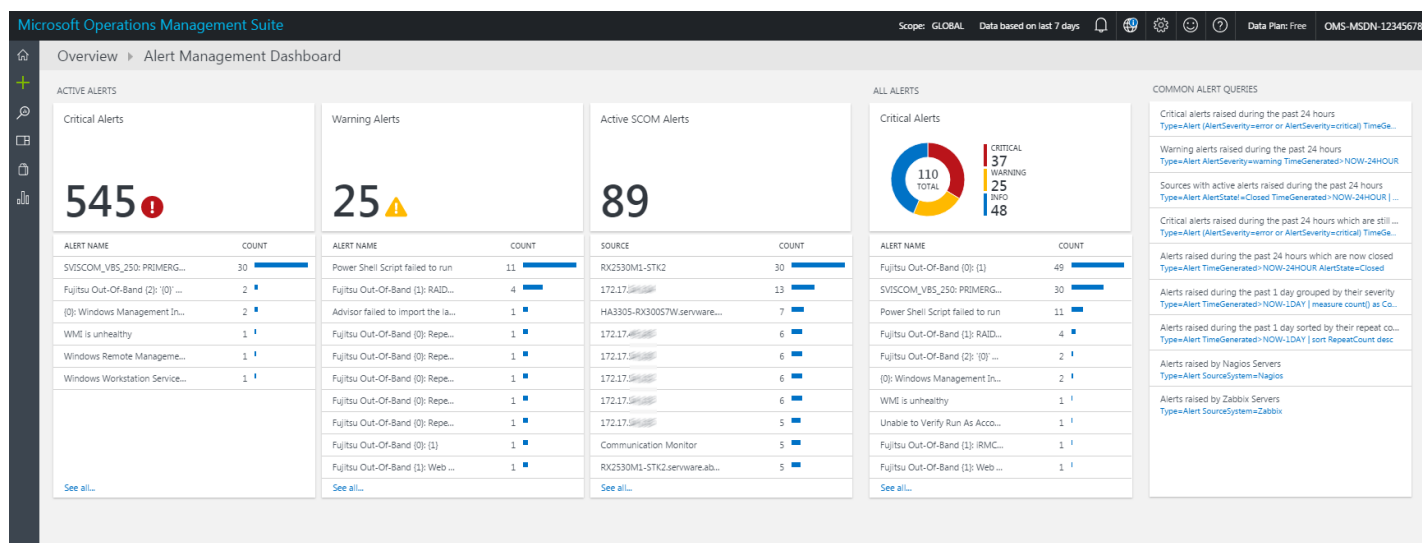


Figure 3 - Alert Management Solution Dashboard

4.4. Custom Windows Event Log forwarding

This is also part of the 'Alert Management' solution and in addition to forwarding SCOM related alerts supports forwarding events from **any** available Windows Application Event Logs with optional severity based filtering. Only entries from systems configured under the 'Managed Computers' or directly attached systems can be forwarded to OMS for processing.

 It is recommended to collect Critical and Warning Events from the 'Operations Manager' Event Log.

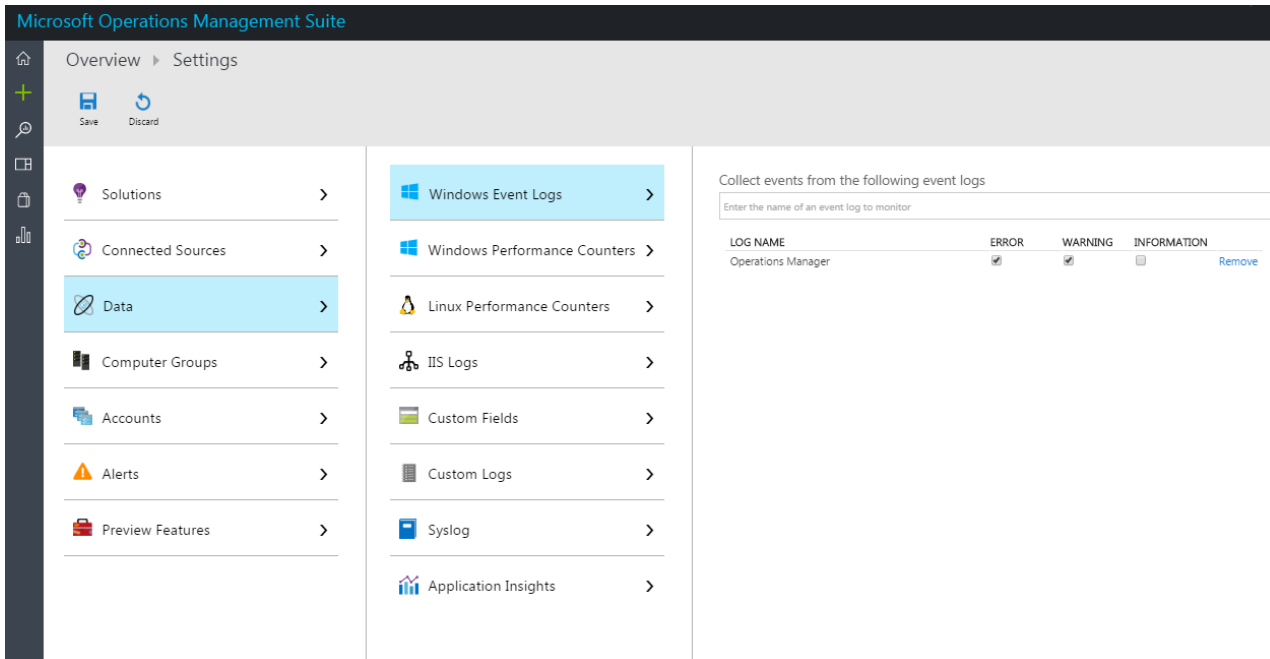





Figure 4 - Operations Manager / Custom Event Log as Data Source

4.5. Performance Data forwarding from Managed Computers

For Systems with installed OMS Agent or SCOM monitored Windows systems any Windows performance counter data can be forwarded as 'Near Real-time Counter (NRT)' with intervals ranging from 10 Seconds to 30 Minutes. This enables detailed performance analysis and application monitoring independent from SCOM performance monitoring.


Start typing the name of the desired counter and OMS will provide a list under the search box.

Configuration is pushed back to SCOM as a Management Pack.

-  These performance collection rules target all 'Managed Computers', fine tuning (e.g. different collection intervals per system or monitoring a single system) is not possible.
-  OMS performance data is independent from performance data collected and stored by standard SCOM performance collection rules. Both use the same data source, but differ only in the Write Action.
-  Basically every performance counter from the Operating System can be collected, not only the by default recommended ones.

4.6. SCOM Performance Data forwarding with custom rules

Since OMS Performance Data collection is technically a regular SCOM performance rule with a 'Cloud Write Action' it is possible to extend the list of collected performance data with data not covered by the default Microsoft rules or data not available as native O/S performance counter.

 One of the advantages of this approach is that fine tuning and granularity (per Server collection interval, different performance counter by server etc.) is available with standard SCOM overrides.

This feature can be used to forward performance data from Fujitsu PRIMERGY Servers to an OMS workspace. See section [5.2.2](#) for step-by-step instructions.

5. Custom Views

In OMS every solution consists of one or multiple specific log entries as well as dashboard views to visualize various core aspects of the solution. It is possible to extend the OMS functionality by creating custom views.

Custom views allow users to create single pane of glass dashboards based on custom queries across data sets for which data is collected. Based on the Log Search and Query feature a customer can create personal visualizations of query results.

Custom Views consist of a *Tile* which will be displayed in the OMS Overview / Home Screen pane and one or more *View Blades* which will be displayed when you click on the tile.

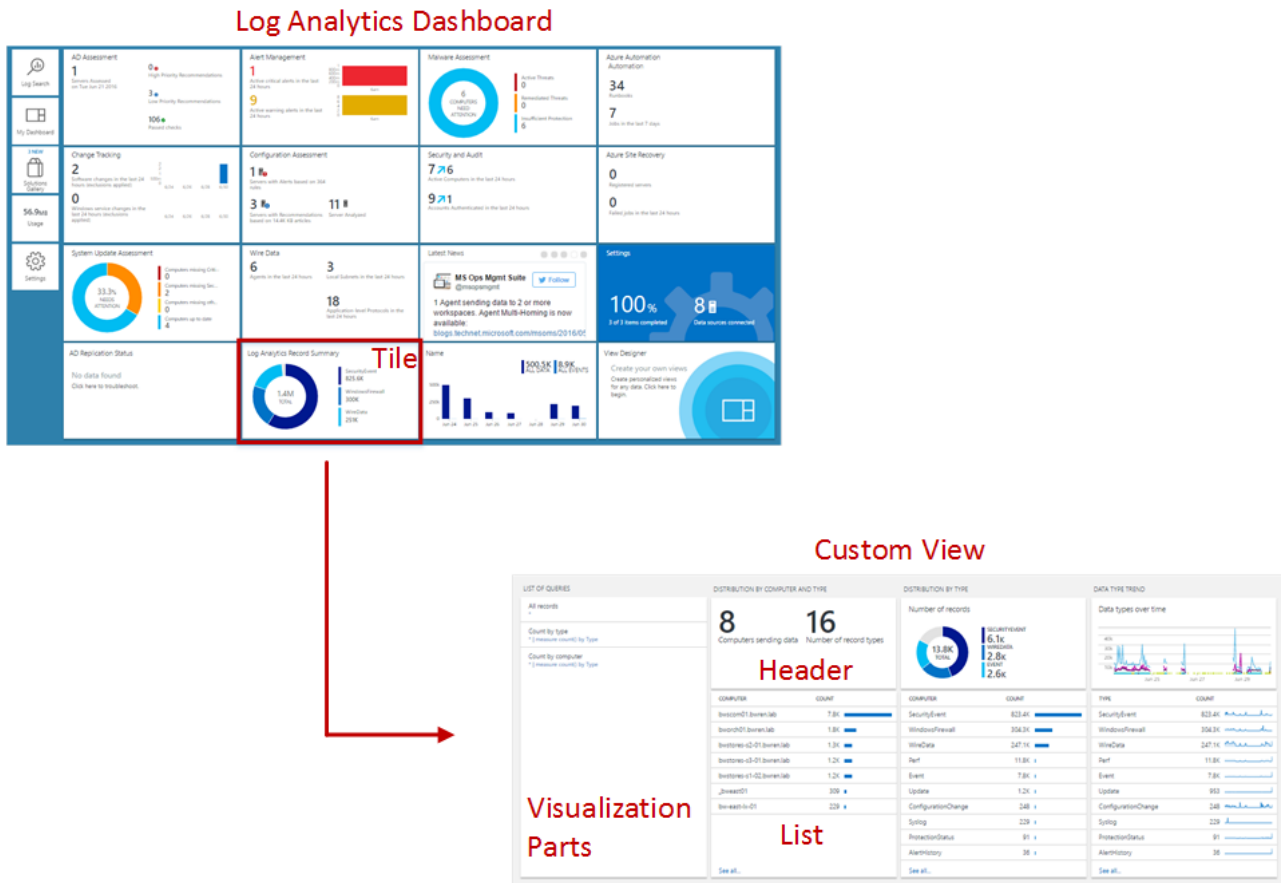


Figure 5 - View Designer Conceptual Overview

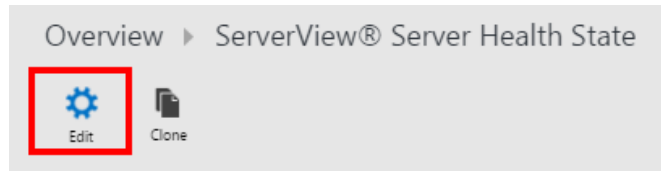
5.1. Creating and editing custom views

5.1.1. Create a new view

Open a new view in the View Designer by clicking on the View Designer Tile in the main OMS dashboard.

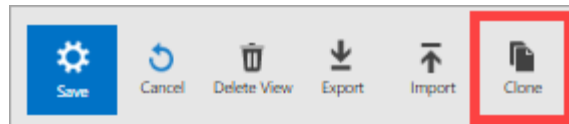
5.1.2. Edit an existing view

To edit an existing view in the View Designer, open the view by clicking on its tile in the main OMS dashboard. Then click the **Edit** button to open the view in the View Designer.



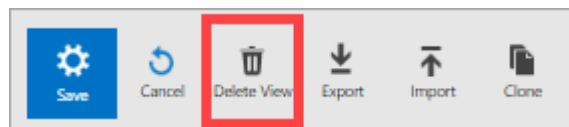
5.1.3. Clone an existing view

When you clone a view, it creates a new view and opens it in the View Designer. The new view will have the same name as the original with "Copy" appended to the end of it. To clone a view, open the existing view by clicking on its tile in the main OMS dashboard. Then click the **Clone** button to open the view in the View Designer.



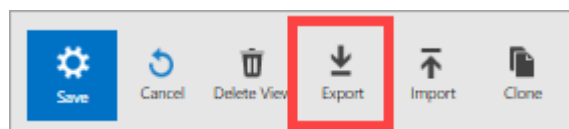
5.1.4. Delete an existing view

To delete an existing view, open the view by clicking on its tile in the main OMS dashboard. Then click the **Edit** button to open the view in the View Designer, and click **Delete View**.




5.1.5. Export an existing view

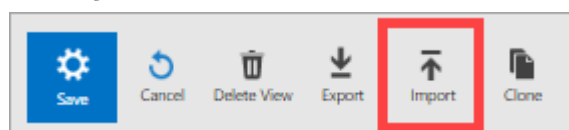
You can export a view to a JSON file that you can import into another workspace. To export an existing view, open the view by clicking on its tile in the main OMS dashboard. Then click the **Export** button to create a file in the browser's download folder. The name of the file will be the name of the view with the extension *omsview*.



5.1.6. Import an existing view

 To import an existing view, you first need to create a new view.

You can import an *omsview* file that you exported from another management group. After you have created a new view, click the **Import** button and select the *omsview* file. The configuration in the file will be copied into the existing view.



5.2. Custom Views for Performance Data

5.2.1. Power Consumption Performance Data of Windows servers

i The following steps demonstrate how to create a custom view based on a standard Windows performance counter. These steps also apply to all the other views from this white paper and are not repeated in detail in every section.

Selected PRIMERGY servers provide the possibility to monitor the actual Power Consumption within the embedded integrated Remote Management Controller (iRMC). The overall server power consumption sensor with an optional configured power limit is exposed from the iRMC via the server BIOS as a standard ACPI000D object to the operating system. As such it can be read and monitored by the Operating System without knowing technical details of the actual implementation and without any additional software (e.g. no Agent needs to be installed). Technical details about the exposed ACPI object for Power Consumption can be found [here](#).

i The power consumption of the ACPI000D object is measured MilliWatt. You may need to convert it to Watt or BTU/h if needed.

To collect and visualize the overall Power Consumption of a Fujitsu PRIMERGY Windows Server perform the following configuration steps within your OMS workspace:

- ▶ Within the OMS workspace setup pane select *Data*
- ▶ Within the '*Data*' pane select '*Windows Performance Counters*'
- ▶ In the Search bar type '*Power Meter(_Total)|Power*' and click the Plus Sign for Add
- ▶ Select the monitoring interval. This can be changed later on if needed. Typical Power Consumption data can be collected every 5 Minutes (300 Seconds) or as fast as every 10 seconds depending on your monitoring needs.

i Since this is based on a standard Windows Performance Counter collection rule, this rule is pushed and executed on every Computer of your OMS 'Managed Computers' Group in your SCOM Management Group as well as to all standalone Windows OMS or SCOM Management Agents.

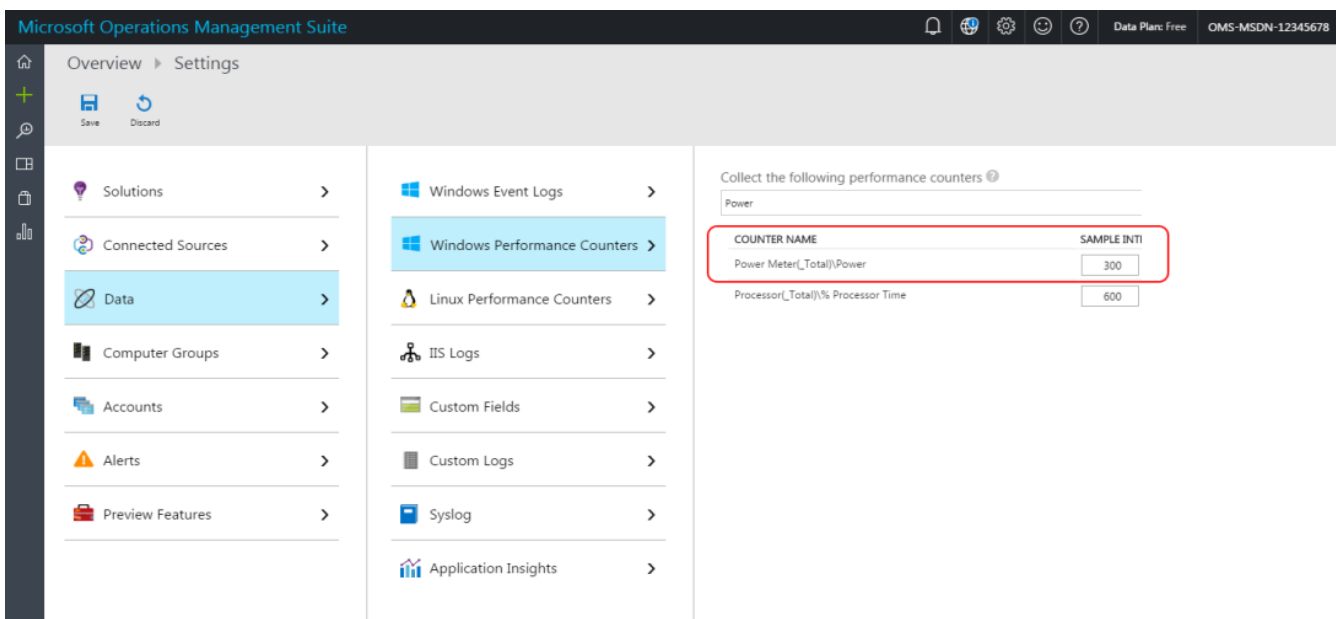


Figure 6 - Adding Windows Server Power Consumption Performance Counter

5.2.1.1. Custom View creation

Performance data will be available in OMS after some time. Configuration needs to be pushed back to the agents and data needs to be collected and indexed by OMS first. It can take up to one hour before the first data is available for search, but typically data is available within a few Minutes after a changed configuration. You can check for the availability of the "Power Meter" Performance data with the following query:

```
Perf | where ObjectName == "Power Meter"
```

In order to visualize the average Power Consumption over time and average the values over 15 Minutes use the following query:

```
Perf | where ObjectName == "Power Meter" | summarize AggregatedValue = avg(CounterValue) by bin(TimeGenerated, 15m), Computer | render timechart
```

Since the Power Meter counter is available in MilliWatt it is recommended to convert the value to Watt by dividing it by 1000:

```
Perf | where ObjectName == "Power Meter" | summarize AggregatedValue = avg((CounterValue / 1000)) by bin(TimeGenerated, 15m), Computer | render timechart
```

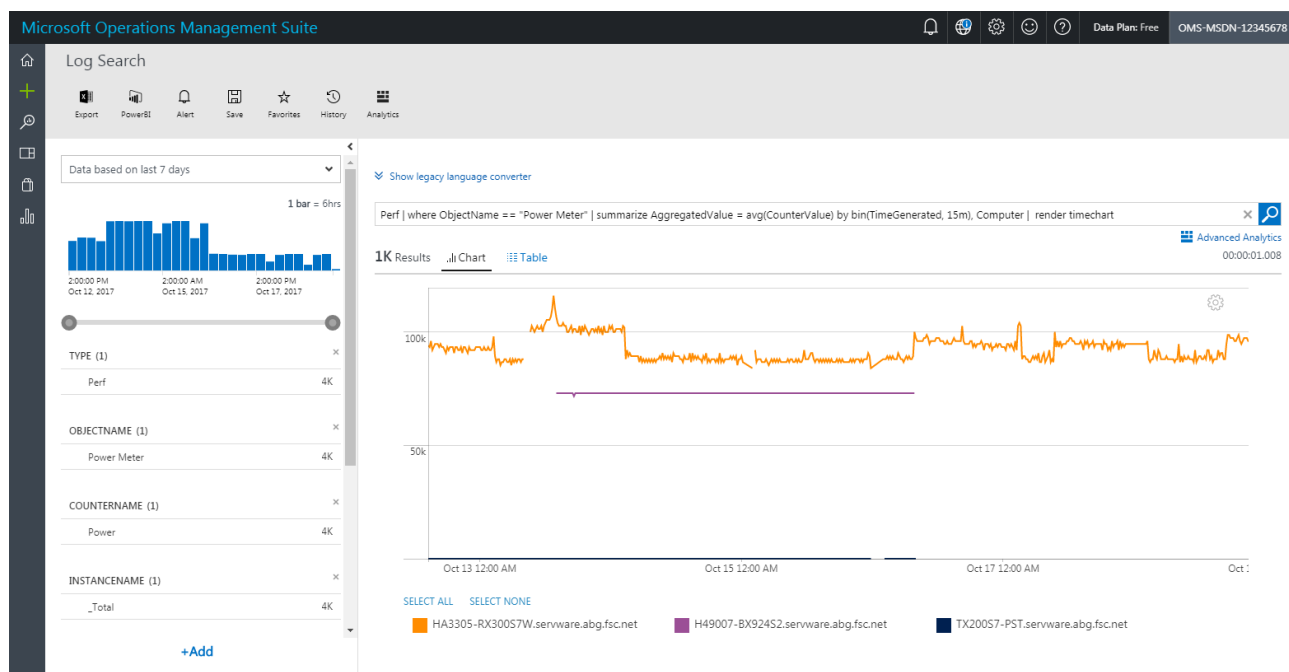


Figure 7 - Windows Power Consumption over time in MilliWatt

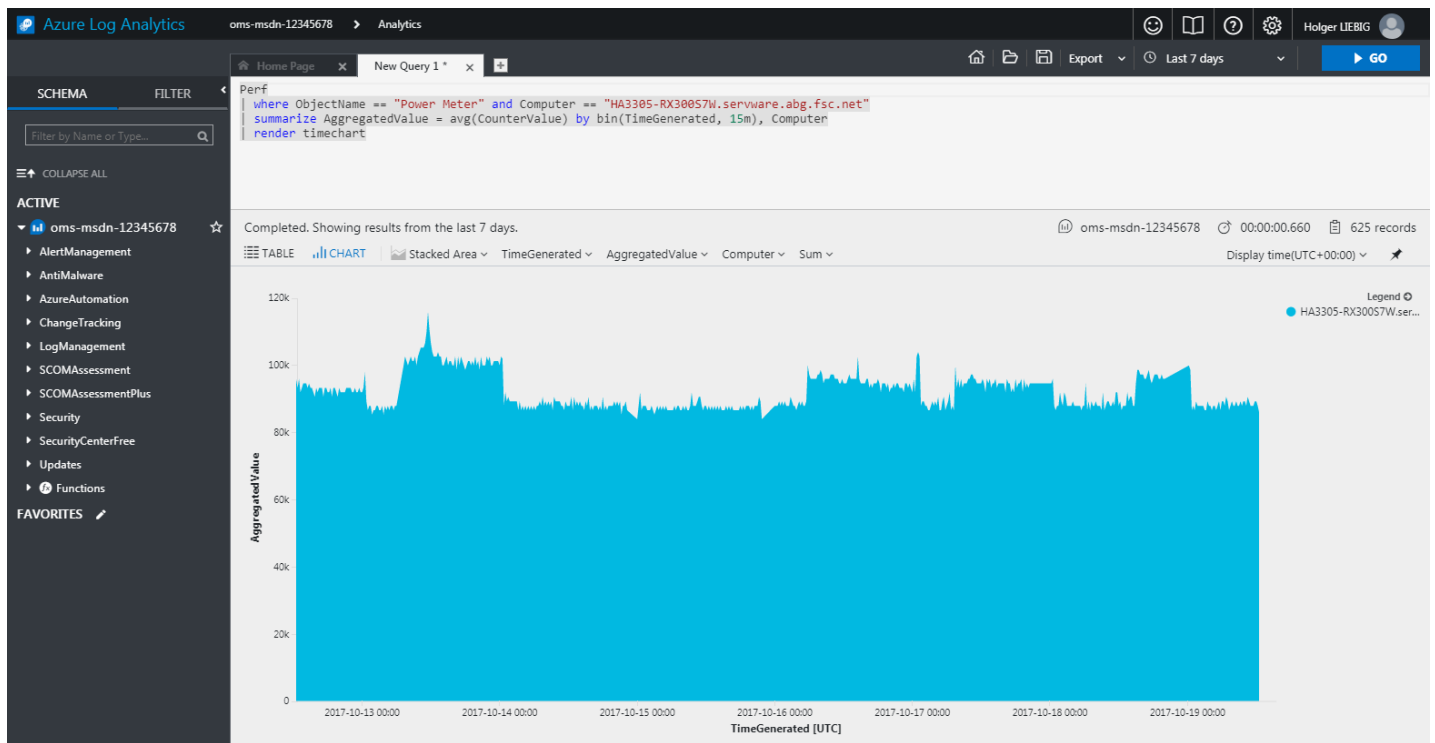



Figure 8 - Windows Power Consumption opened in Advanced Analytics from your workspace

 You can save this query to your 'Favorites' or create a custom view for it. You can also fine tune the aggregation interval to your needs if needed.

To create a custom view follow perform the following steps:

1. Define a view for the tile displayed in the OMS home screen
2. Define one or more view blades which are displayed when you click on the tile in your OMS home screen.

To create the tile for your OMS home screen perform the following steps:

- ▶ Within your OMS home screen click the 'View Designer'
- ▶ Select the *Overview Tile* tab and drag the 'Line Chart' template to your working area
- ▶ Enter 'Windows Power Consumption' as Name
- ▶ Enter the following query in the Line Chart Query field:
`Perf | where ObjectName == "Power Meter" | summarize AggregatedValue = avg((CounterValue / 1000)) by bin(TimeGenerated, 15m), Computer`
- ▶ Expand the 'Y Axis' tree and enter 'Watt' as custom Label.
 Note: instead of on the fly conversion you could also modify the Y Axis settings by selecting 'Unit Type' Count and convert from 'Ones' to 'Thousands'
 Click 'Apply' to preview the result

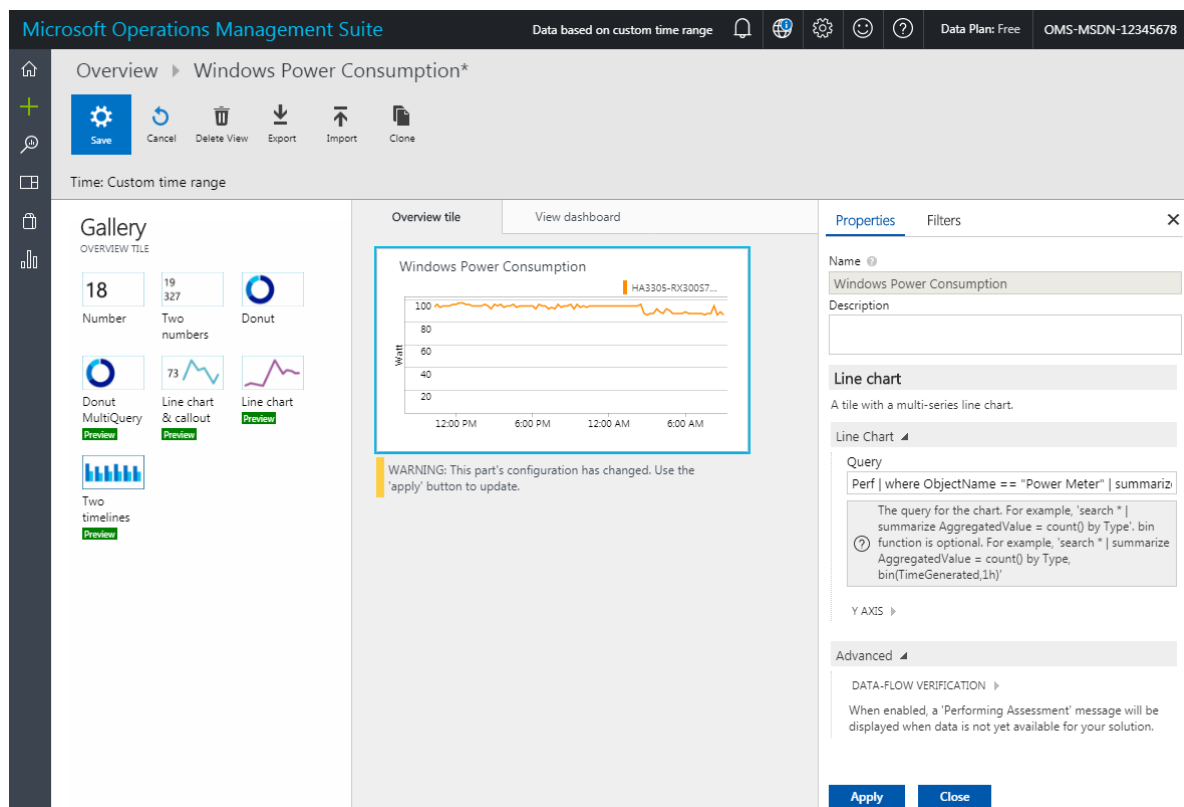


Figure 9 - Designing the Overview Tile for the OMS Home screen

To create the view dashboard part perform the following additional steps in the view designer:

- ▶ On the left overview side: Click on the *'View dashboard'* Pane
- ▶ Drag 'Line Chart and list' template to your working area
- ▶ Enter 'Power Distribution' as Group Title.
- ▶ Enter 'Windows Consumption over Time' as Header Title
- ▶ Enter the same query as above for the Line Chart Query:
`Perf | where ObjectName == "Power Meter" | summarize AggregatedValue = avg((CounterValue / 1000)) by bin(TimeGenerated, 15m), Computer`
- ▶ Enter the same query as above for the List Query:
`Perf | where ObjectName == "Power Meter" | summarize AggregatedValue = avg((CounterValue / 1000)) by bin(TimeGenerated, 15m), Computer`
- ▶ Click Apply to preview the view
- ▶ When finished with the tile and the view part, click Save

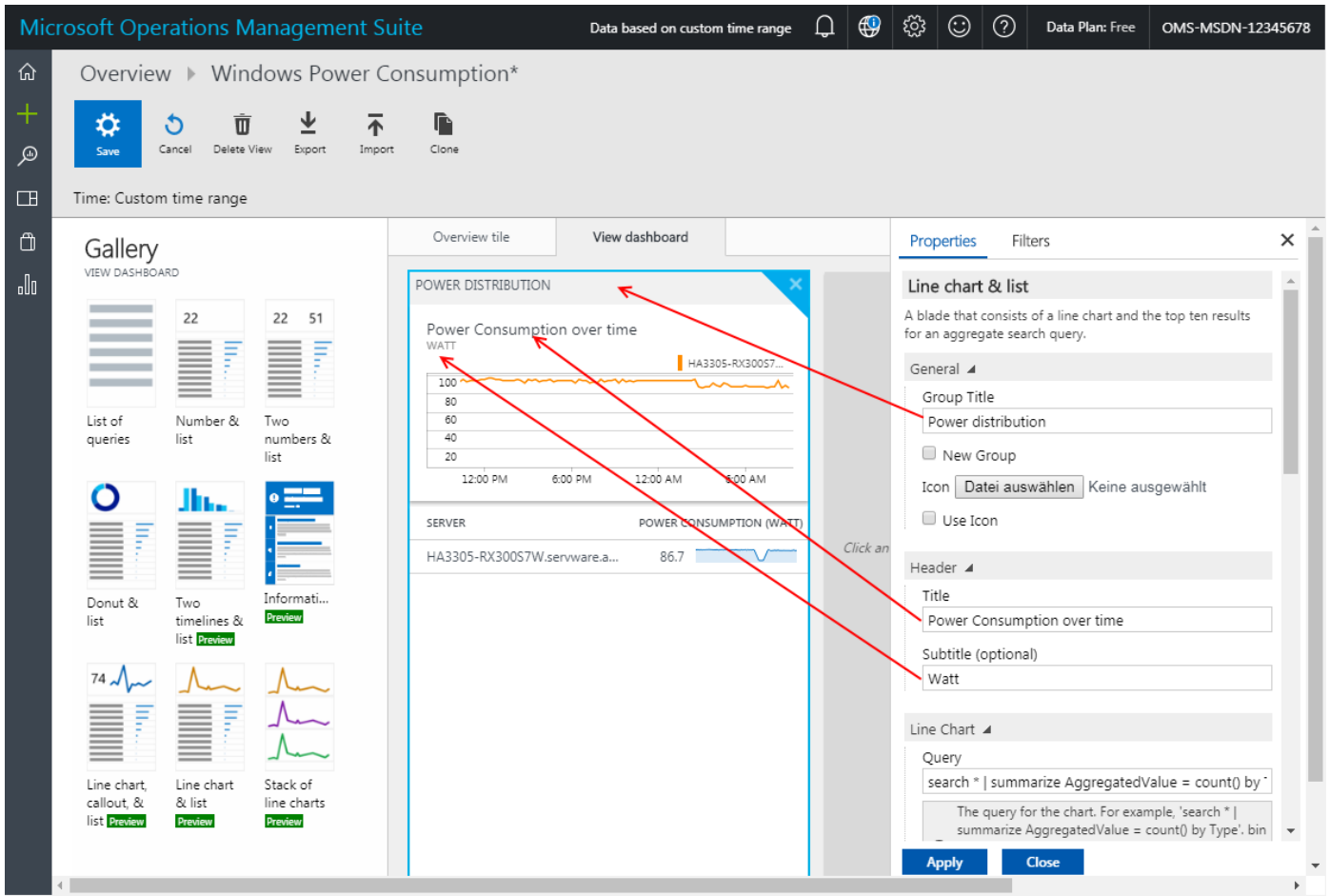


Figure 10 - Designing the View dashboard

5.2.2. Custom Performance Data of Fujitsu PRIMERGY servers

In addition to standard O/S specific performance counter data it is possible to forward custom SCOM performance data to OMS. In order to forward these additional performance counter data you need to install additional Fujitsu O/S specific Management Packs on your SCOM Management Server since these counters are collected in O/S specific ways. See section 6.1.2 for a list of available O/S specific 'Fujitsu PRIMERGY Collect Performance Data to OMS' Management Packs.

i In order to collect custom performance counters from non-Windows servers (Linux, ESXi, Out-of-Band) **all** the SCOM Management Servers from your Management Group need to be in the list of OMS 'Managed Computers'. To collect custom performance data from Windows Server instances these also need to be in the group of OMS 'Managed Computers'.

5.2.2.1. Ambient Temperature Performance Data Monitoring

i Make sure you have enabled the required performance collection rules and configured the desired performance collection interval with SCOM overrides for the O/S specific 'Fujitsu PRIMERGY Collect Performance Data to OMS' Management Pack.

All SCOM performance counter instances are uniquely identified by a combination of ObjectName, CounterName and InstanceName; this can be mapped directly to an OMS query:

```
Perf | where ObjectName=="AAA"
      and CounterName=="BBB"
      and InstanceName=="CCC"
```

Fujitsu PRIMERGY Performance Management Packs support the following temperature related performance counter:

- ObjectName="Temperature"
- CounterName one of the following:
 - CounterName="Ambient"
 - CounterName="System Board"
 - CounterName="Processor"
 - CounterName="Memory"
 - Countername="Power Supply"
- InstanceName
 - Name of the actual Sensor in the iRMC

i Depending on the actual Sensor Data a PRIMERGY server can have multiple instances for a specific CounterName (e.g. 'Ambient' and 'Front' as instances for 'Air Inlet' sensors)

i All PRIMERGY server have an Air Inlet sensor named 'Ambient', Blade server optional have an Air Inlet sensor named 'Front' so it is sufficient to use the following query:
Perf | where ObjectName=="Temperature" and CounterName=="Ambient" to list all Air Inlet sensors or the following query *Perf | where InstanceName like "Ambient"* to get only the sensors named 'Ambient' in the following custom views.

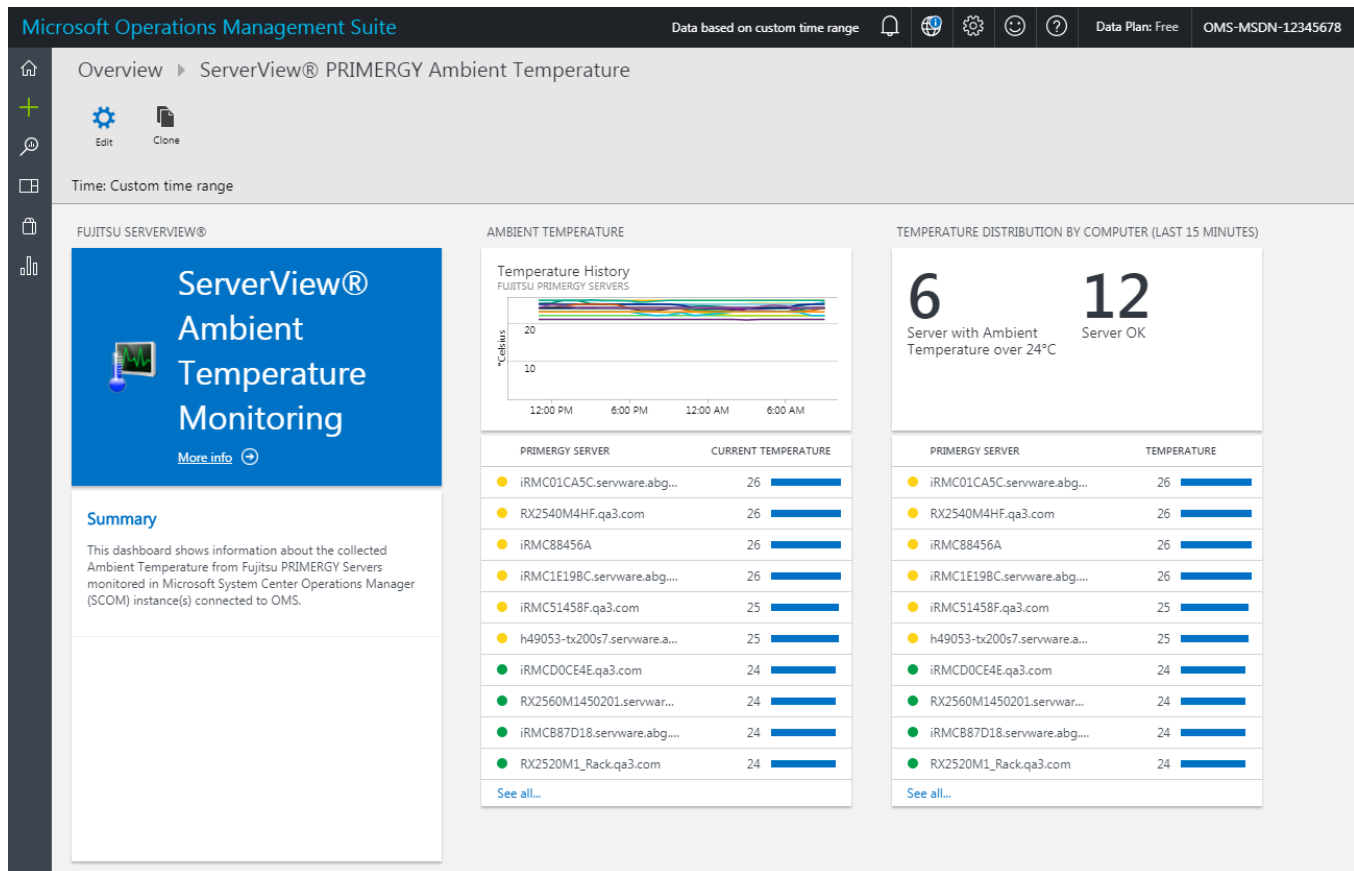
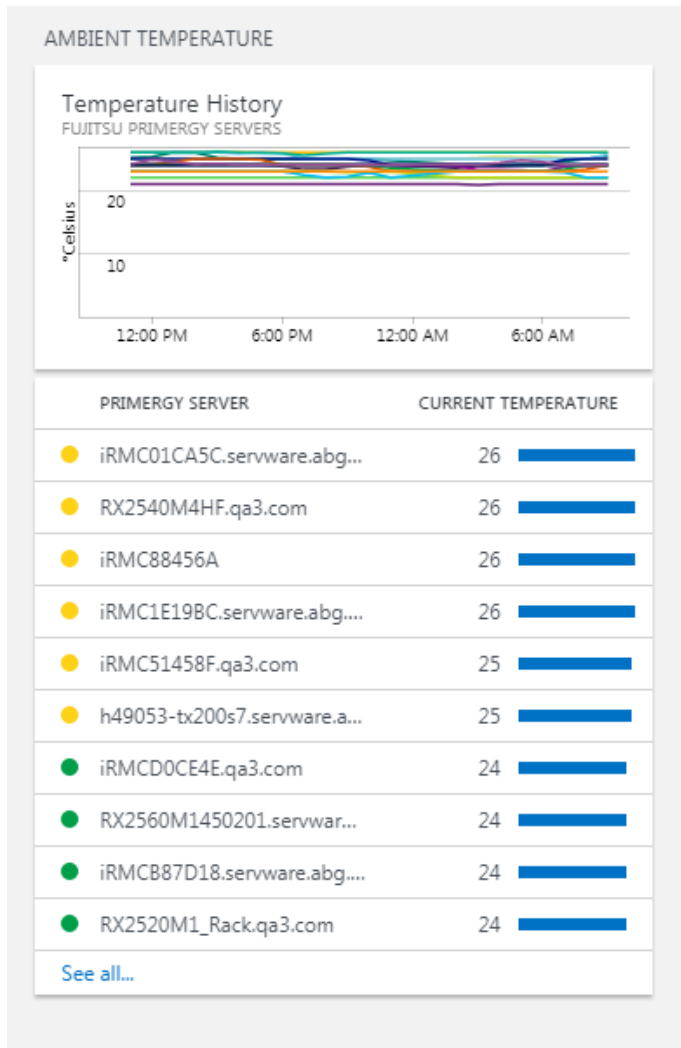


Figure 11 - Sample Custom View for Ambient Temperature Monitoring

5.2.2.2. Temperature History' View

The following view templates and queries were used in the 'Temperature History' custom view. You can adopt this to your personal needs by modifying the query



View Template:

- Line Chart & List

General Section:

- Group Title: Ambient Temperature

Header Section:

- Title: Temperature History
- Subtitle: Fujitsu PRIMERGY Servers

Line Chart:

- Query:


```
Perf |
where ObjectName=="Temperature"
and CounterName=="Ambient" | summarize
AggregatedValue = avg(CounterValue)
by bin(TimeGenerated, 1h), Computer |
sort by TimeGenerated
```
- Y-Axis
 - Custom Label: °Celsius

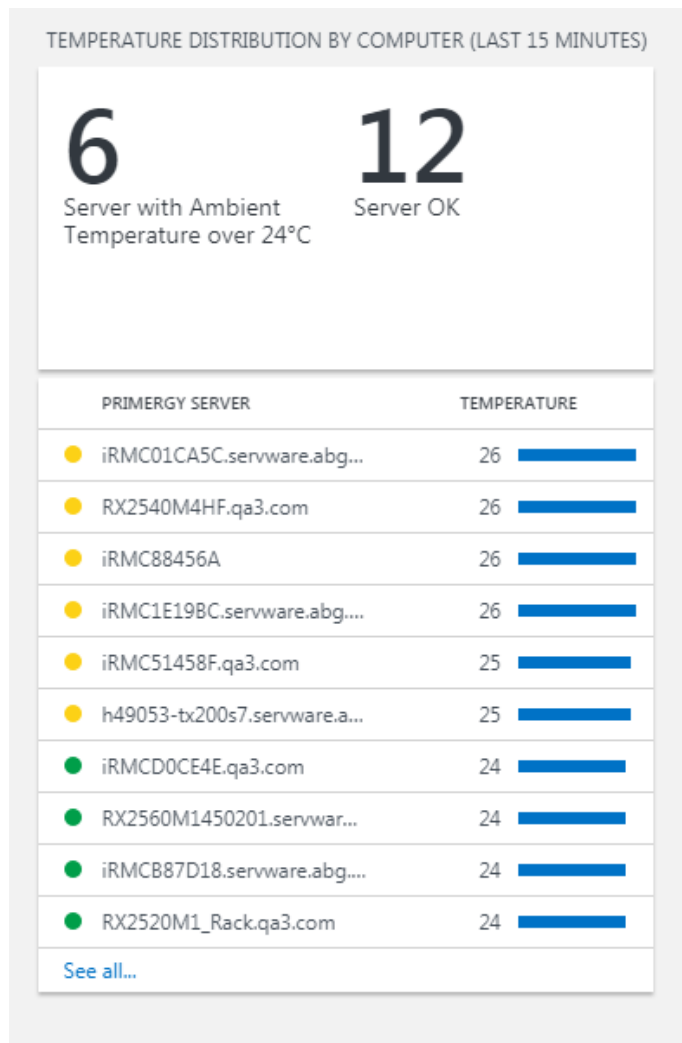
List:

- Query:


```
Perf |
where ObjectName == "Temperature" and
CounterName == "Ambient"
and TimeGenerated > ago(15m) |
summarize AggregatedValue =
max(CounterValue) by Computer |
sort by AggregatedValue
```
- Column Titles:
 - Name: PRIMERGY Server
 - Value: Current Temperature
- Color: select based on your personal preference

5.2.2.3. 'Temperature Distribution by Computer' View

The following view templates and queries were used in the 'Temperature Distribution by Computer' custom view. You can adopt this to your personal needs by modifying the query.



View Template:

- *Two Numbers & List*

General Section:

- **Group Title:** *Temperature Distribution by Computer*

Title Section:

- **Legend:** *Server with Temperature over 24°C*
- **Query:**
`Perf | where ObjectName == "Temperature" and CounterName == "Ambient" and TimeGenerated > ago(15m) | summarize AggregatedValue = max(CounterValue) by Computer | where AggregatedValue > 24 | count`

Title Section:

- **Legend:** *Server OK*
- **Query:**
`Perf | where ObjectName == "Temperature" and CounterName == "Ambient" and TimeGenerated > ago(15m) | summarize AggregatedValue = max(CounterValue) by Computer | where AggregatedValue <= 24 | count`

List:

- **Query:**
`Perf | where ObjectName == "Temperature" and CounterName == "Ambient" and TimeGenerated > ago(15m) | summarize AggregatedValue = max(CounterValue) by Computer | sort by AggregatedValue`
- **Column Titles:**
 - **Name:** *PRIMERGY Server*
 - **Value:** *Temperature*
- **Color:** *select based on your personal preferences*

5.2.3. Power Consumption Performance Data Monitoring



Make sure you have enabled the required performance collection rules and configured the desired performance collection interval with SCOM overrides for the O/S specific 'Fujitsu PRIMERGY Collect Performance Data to OMS' Management Pack.

All SCOM performance counter instances are uniquely identified by a combination of ObjectName, CounterName and InstanceName; this can be mapped directly to an OMS query:

```
Perf | where ObjectName=="AAA"  
       and CounterName=="BBB"  
       and InstanceName=="CCC"
```

Fujitsu PRIMERGY Performance Management Packs support the following Power Consumption related performance counter:

- ObjectName="Power Consumption"
- CounterName one of the following:
 - CounterName="Total"
 - CounterName="System Chassis"
 - CounterName="Processor"
 - CounterName="Power Supply"
- InstanceName
 - Name of the actual Sensor in the iRMC



Depending on the actual Sensor Data a PRIMERGY server can have multiple instances for a specific CounterName (e.g. 'CPU1 Power' and 'CPU2 Power' as instances for 'Processor' power consumption sensors)

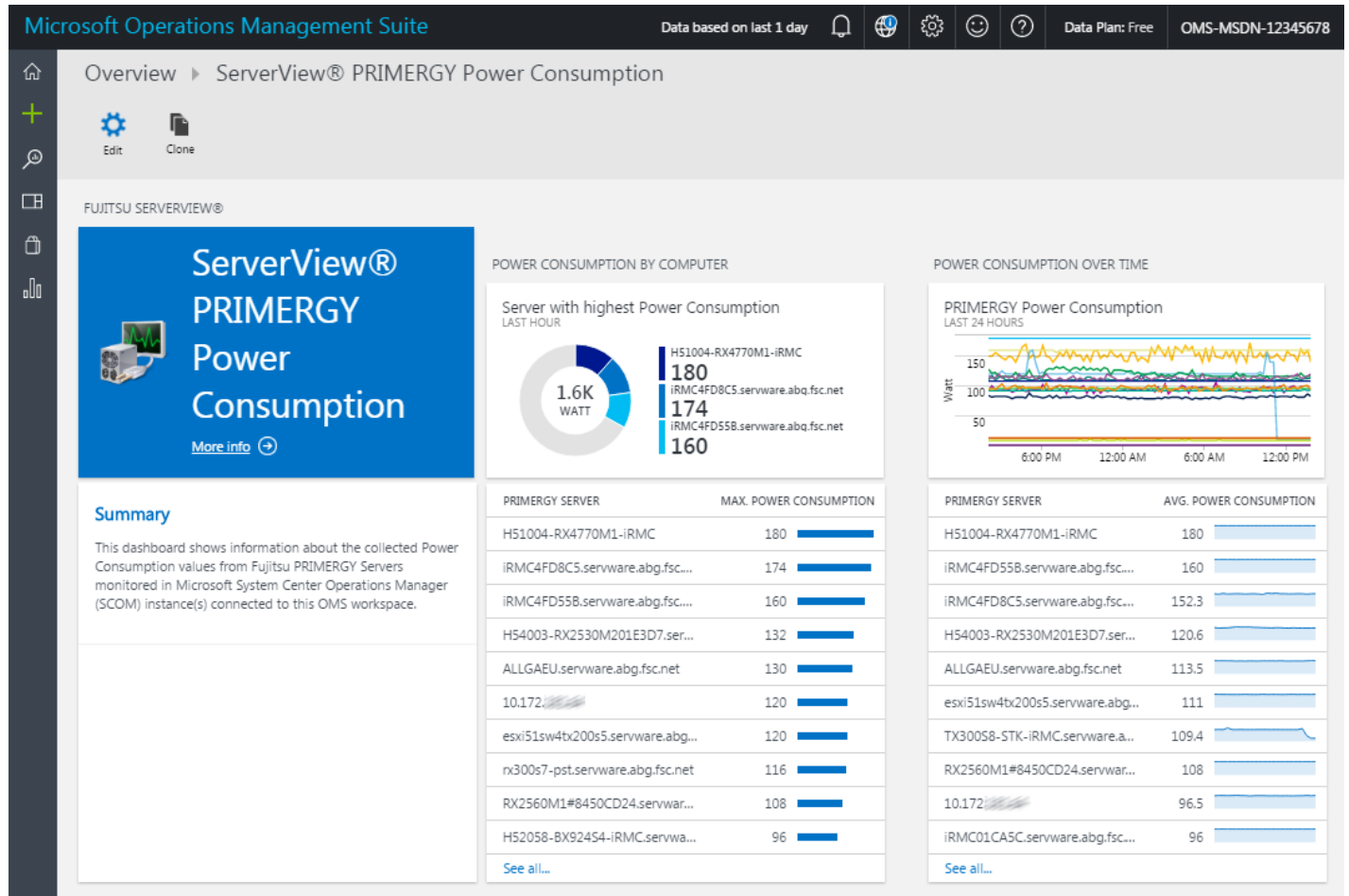
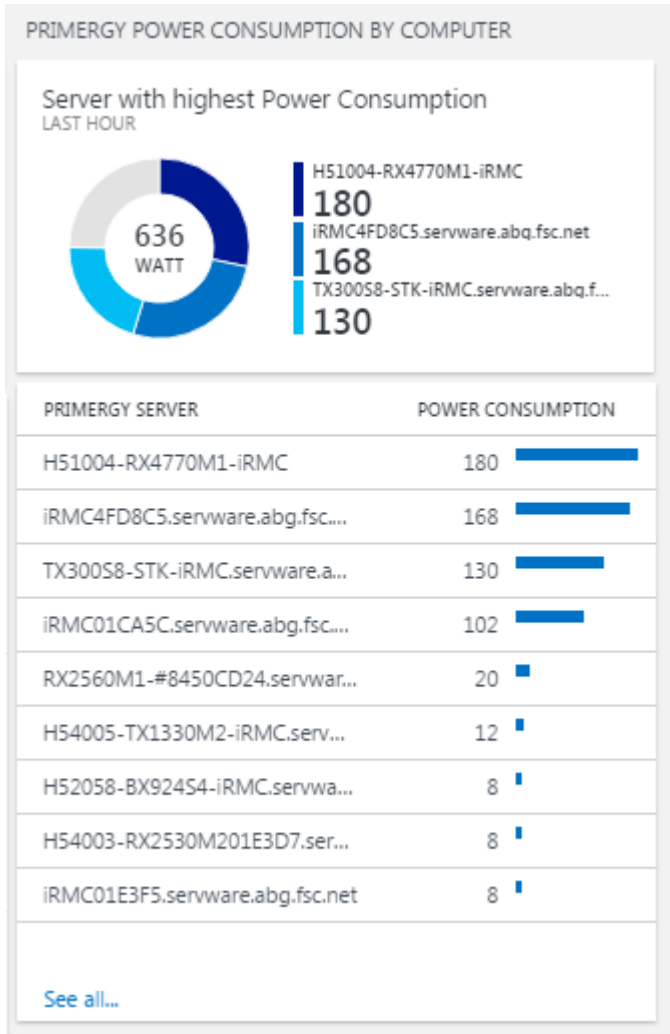


Figure 12 - Sample Custom View for Power Consumption Monitoring

5.2.3.1. 'PRIMERGY Power Consumption by Computer' View

The following view templates and queries were used in the 'Top 3 Server Power Consumption by Computer' custom view. You can adopt this to your personal needs by modifying the queries.



View Template:

- *Donut & List*

General Section:

- **Group Title:** *Top 3 Server Power Consumption by Computer*

Header Section:

- **Title:** *Server with highest Power Consumption*
- **Subtitle:** *Add optional text as needed*

Donut Section:

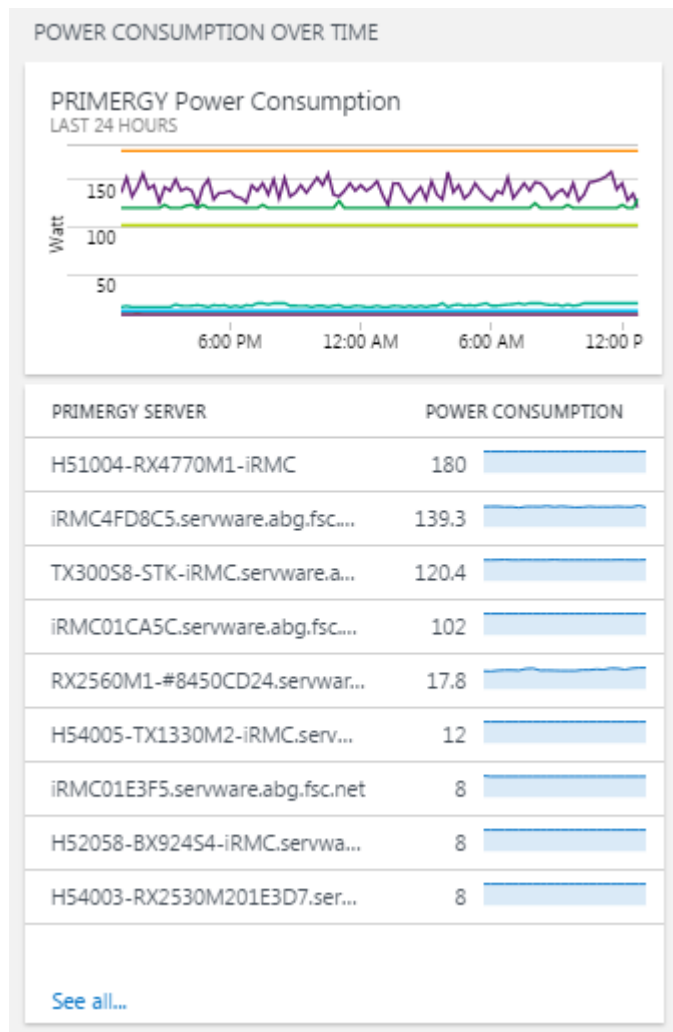
- **Query:**
`Perf | where
 ObjectName == "Power Consumption"
 and CounterName == "Total"
 and TimeGenerated > ago(1h) |
 summarize LastValue =
 max(CounterValue) by Computer |
 sort by LastValue desc`
- **Center**
 - **Text:** *Watt*
 - **Operation:** *Sum*
- **Additional Options**
 - **Colors**
 - **Color 1:** select based on your personal preferences
 - **Color 2:** select based on your personal preferences
 - **Color 3:** select based on your personal preferences

List:

- **Query:**
`Perf | where
 ObjectName == "Power Consumption"
 and CounterName == "Total"
 and TimeGenerated > ago(1h) |
 summarize LastValue =
 max(CounterValue) by Computer |
 sort by LastValue desc`
- **Column Titles:**
 - **Name:** *PRIMERGY Server*
 - **Value:** *Power Consumption*
- **Color:** select based on your personal preferences

5.2.3.2. 'Power Consumption over Time' View

The following view templates and queries were used in the 'Power Consumption over Time' custom view. You can adopt this to your personal needs by modifying the query.



View Template:

- *Line Chart & sparklines*

General Section:

- **Group Title:** *Power Consumption over Time*

Header Section:

- **Title:** *PRIMERGY Power Consumption*
- **Subtitle:** *Last 24 Hours*

Line Chart:

- **Query:**
`Perf | where
 ObjectName == "Power Consumption" and
 CounterName == "Total"
 and TimeGenerated > ago(1d) |
 summarize AggregatedValue =
 avg(CounterValue) by
 bin(TimeGenerated, 15m), Computer`
- **Y-Axis**
 - **Custom Label:** *Watt*

List:

- **Query:**
`Perf | where
 ObjectName == "Power Consumption" and
 CounterName == "Total"
 and TimeGenerated > ago(1d) |
 summarize AggregatedValue =
 avg(CounterValue) by
 bin(TimeGenerated, 15m), Computer`
- **Column Titles:**
 - **Name:** *PRIMERGY Server*
 - **Value:** *Power Consumption*
- **Color:** select based on your personal preference

5.3. Health State Monitoring with OMS

Health State monitoring is (currently) not part of the standard Microsoft solutions for OMS and SCOM integration. It is important to remember that OMS is a cloud based solution which is based on the feature of Log Search. Only items for which Log entries are defined and present can be visualized in OMS based on the key features for every Log Entry: Log Type and its timestamp. SCOM on the other side periodically executes workflows to determine the current monitor state of a managed entity and stores the result in a SQL database as last known state.

To bridge the gap and provide basic health state information in OMS an additional Management Pack is needed. This Management Pack contains a rule which periodically queries the current health state of Fujitsu PRIMERGY

servers from SCOM and sends the data JSON formatted to the OMS workspace which has been registered with the SCOM Management Server.

i Even if the configured "Fujitsu ServerView Collect Health State to OMS" rule interval matches the time condition for the OMS query it can happen that zero records are reported. This is caused by the fact that the collected health records needs to be indexed first by OMS before they are available and the indexing cannot be influenced or triggered on demand.

i It is important to remember that you have to correlate the monitoring interval of the rule running on the SCOM Management Group with the same interval used in the OMS queries e.g. limit the OMS search results to entries with TimeGenerated > ago(10m). Otherwise you might end up with an incorrect number of log records (e.g. if your TimeGenerated windows is larger than the rule interval you can run into the condition that you have the result from 2 rule cycles).

5.4. Implementation details

Health state information for Fujitsu PRIMERGY servers is collected on the SCOM Management Server as a custom rule which periodically executes a PowerShell Script and sends the data as JSON formatted data to OMS. Since all specific PRIMERGY server instances in SCOM are derived from a Base Class 'Fujitsu.ServerView.Server' this rule will enumerate PRIMERGY server objects from different O/S specific Management Packs, including Windows, Linux, ESXi and Out-of-Band servers.

i You can configure which O/S specific server types are enumerated as well as the interval period for the rule with standard SCOM overrides. See section 6.1.1 for details.

A single JSON record for a Fujitsu PRIMERGY server looks like the following:

```
{ "ServerName": "TX300S8-MUC-iRMC.subdomain.domain.net",
  "NetworkName": "192.168.1.100",
  "ServerModel": "PRIMERGY TX300 S8",
  "ServerHealth": "Error",
  "MaintenanceMode": false,
  "ClassType": "PRIMERGY Out-Of-Band Server",
  "ClassName": "Fujitsu Out-Of-Band TX Server"
}
```

OMS automatically extracts Custom Fields based on the JSON name and data type which can be used for additional filtering:

JSON Type	JSON Field Name	OMS Custom Field Name
String	ServerName	ServerName_s
String	NetworkName	NetworkName_s
String	ServerModel	ServerModel_s
String	ServerHealth	ServerHealth_s
Boolean	MaintenanceMode	MaintenanceMode_b

String	ClassType	ClassType_s
String	ClassName	ClassName_s

5.5. Defining Custom Health State Views based on the available OMS data

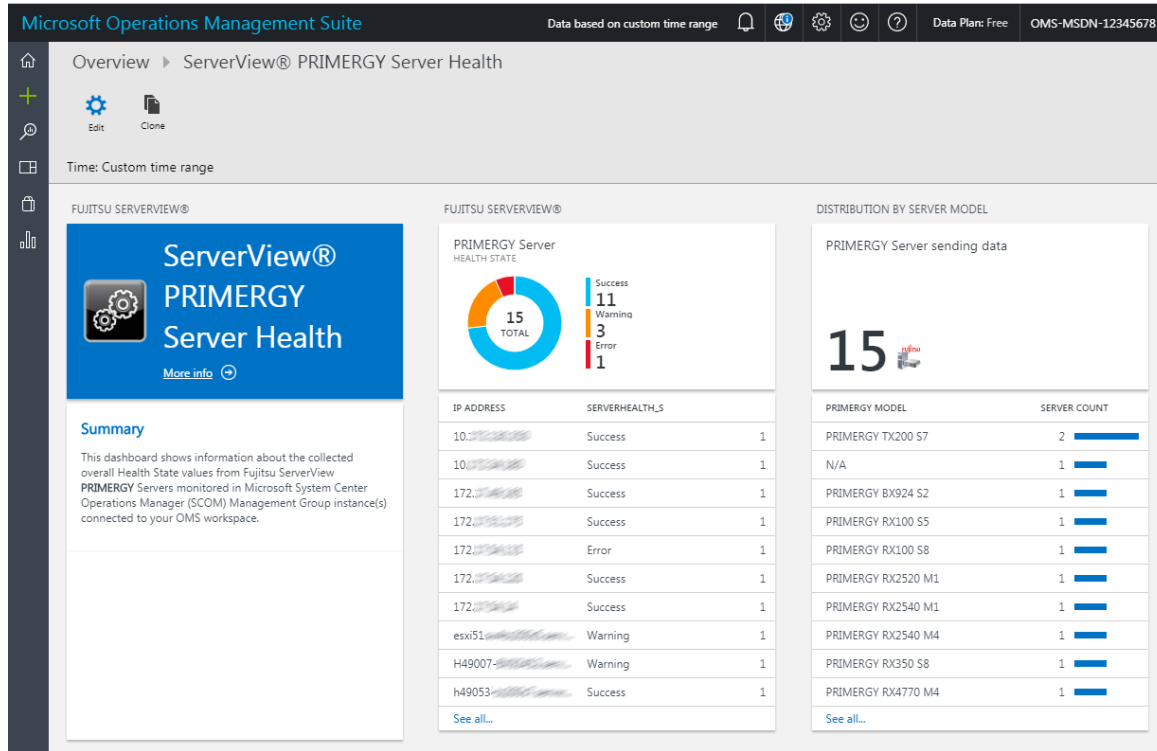


Figure 13 - Custom View with Basic Health State

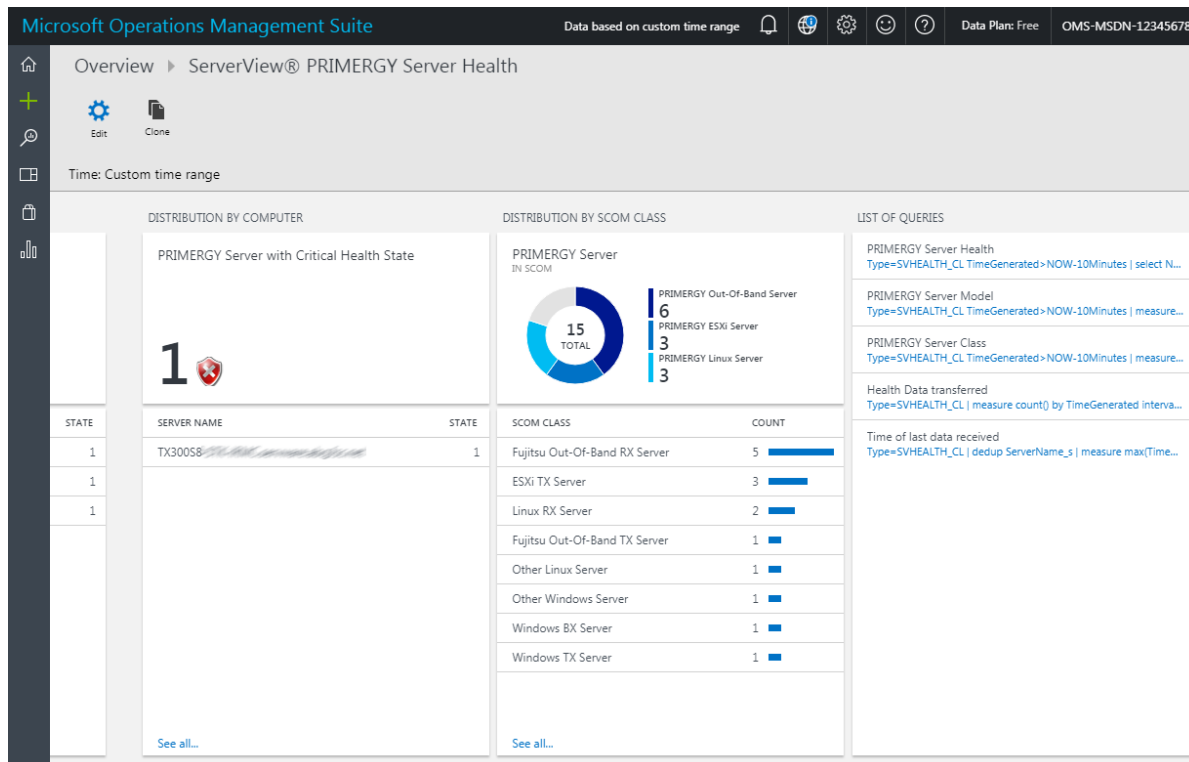
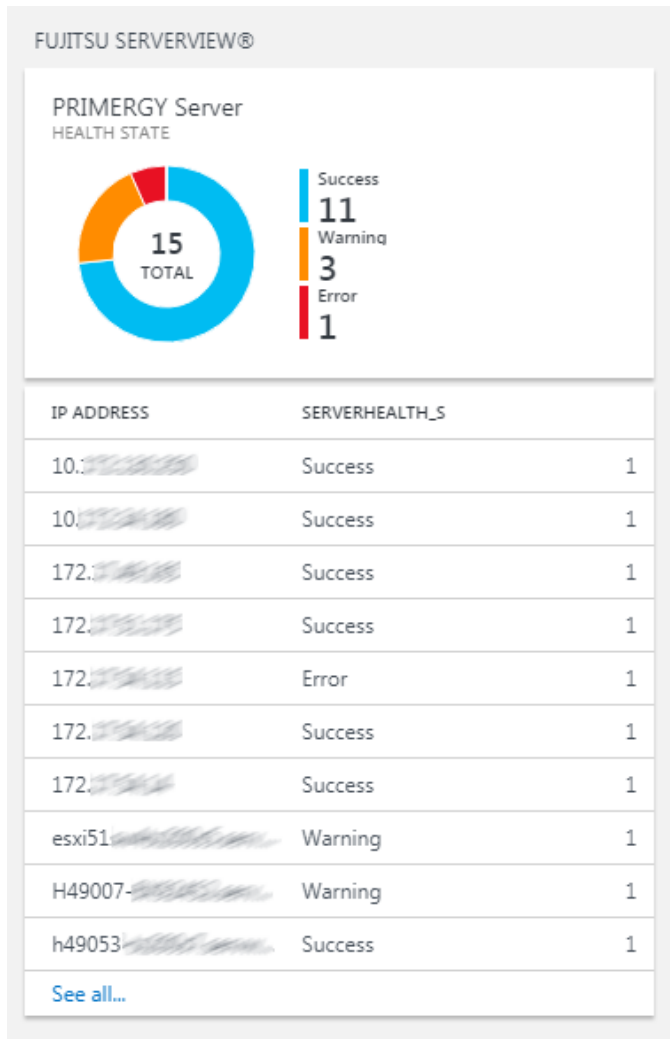


Figure 14 - Part II of the Server Health View

5.5.1. 'PRIMERGY Server Health State' View

The following view templates and queries were used in the 'PRIMERGY Server Health State' Custom View. You can adopt this to your personal needs by modifying the query.



View Template:

- *Donut & List*

General Section:

- **Group Title:** *Fujitsu ServerView®*

Header Section:

- **Title:** *PRIMERGY Server*
- **Subtitle:** *Health State*

Donut Section:

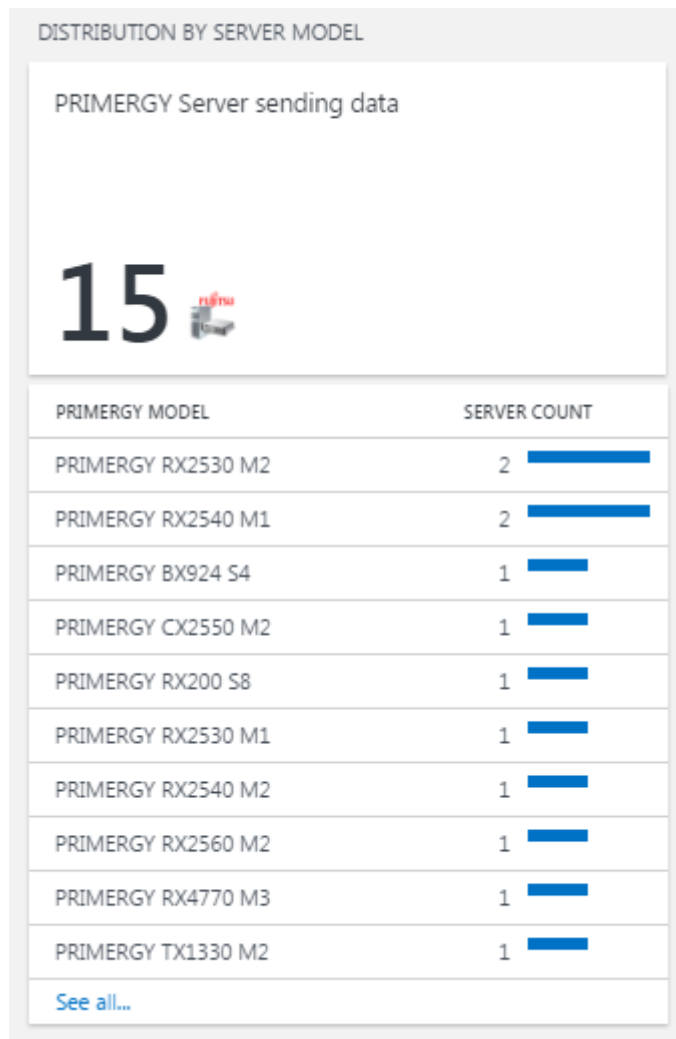
- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = count() by ServerHealth_s | sort by AggregatedValue desc*
- **Center**
 - **Text:** *Total*
 - **Operation:** *Sum*
- **Advanced Color Mapping**
 - **Mapping 1**
 - **Field Value:** *Error*
 - **Color:** *#e81123 (red)*
 - **Mapping 2**
 - **Field Value:** *Warning*
 - **Color:** *#ff8c00 (orange)*
 - **Mapping 3**
 - **Field Value:** *Success*
 - **Color:** *#00bcf2 (blue)*
 - **Mapping 4**
 - **Field Value:** *Uninitialized*
 - **Color:** *#fff100 (yellow)*

List:

- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = count() by NetworkName_s, ServerHealth_s | sort by NetworkName_s asc*
- **Column Titles:**
 - **Name:** *IP Address*
 - **Value:** *<empty>*
- **Hide Graph:** *<checked>*
- **Color:** *select based on your personal preferences (only when 'Hide Graph' is not checked)*

5.5.2. Number of 'PRIMERGY Server sending Data' View

The following view templates and queries were used in the 'PRIMERGY Server sending data' Custom View. You can adopt this to your personal needs by modifying the query.



View Template:

- *Number & List*

General Section:

- **Group Title:** *Distribution by Server Model*
- **Icon:** *Fujitsu Server Icon*
- **Use Icon:** *<checked>*

Title Section:

- **Legend:** *PRIMERGY Server sending data*
- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = dcount(NetworkName_s) by NetworkName_s | count*

List:

- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = count() by ServerModel_s*
- **Column Titles:**
 - **Name:** *PRIMERGY Model*
 - **Value:** *Server Count*
- **Hide Graph:** *<un-checked>*
- **Color:** *select based on your personal preferences*

5.5.3. Number of 'PRIMERGY Server with Warning State' View

The following view templates and queries were used in the 'PRIMERGY Server with Warning Health State' Custom View. You can adopt this to your personal needs by modifying the query.

DISTRIBUTION BY COMPUTER

PRIMERGY Server with Warning Health State

7

SERVER NAME	STATE
H54003-RX2530M201E3D7.servware.abg.fsc.net	1
H54005-TX1330M2-iRMC.servware.abg.fsc.net	1
RX2560M1-#8450CD24.servware.abg.fsc.net	1
TX300S4-STK2	1
esxi51sw4tx200s5	1
esxi60	1
iRMC01E3F5.servware.abg.fsc.net	1

[See all...](#)

View Template:

- *Number & List*

General Section:

- **Group Title:** *Distribution by Computer*
- **Icon:** *Warning Shield Icon*
- **Use Icon:** *<checked>*

Title Section:

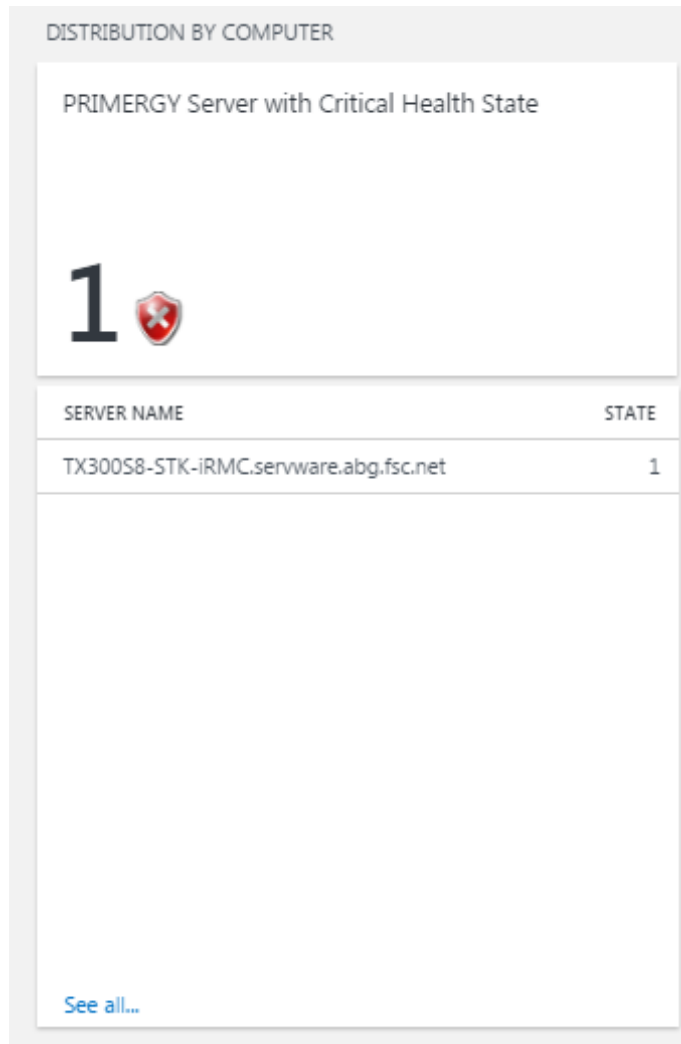
- **Legend:** *PRIMERGY Server with Warning Health state*
- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) and ServerHealth_s == "Warning" | summarize AggregatedValue = count() by ServerName_s | count*

List:

- **Query:** *SVHEALTH_CL | where TimeGenerated > ago(10m) and ServerHealth_s == "Warning" | summarize AggregatedValue = count() by ServerName_s*
- **Column Titles:**
 - **Name:** *Server Name*
 - **Value:** *State*
- **Hide Graph:** *<checked>*
- **Color:** *select based on your personal preferences (only when 'Hide Graph' is not checked)*

5.5.4. Number of 'PRIMERGY Server with Critical State' View

The following view templates and queries were used in the 'PRIMERGY Server with Critical Health State' Custom View. You can adopt this to your personal needs by modifying the query.



View Template:

- *Number & List*

General Section:

- **Group Title:** *Distribution by Computer*
- **Icon:** *Error Shield Icon*
- **Use Icon:** *<checked>*

Title Section:

- **Legend:** *PRIMERGY Server with Critical Health state*
- **Query:**

```
SVHEALTH_CL |
where TimeGenerated > ago(10m)
and ServerHealth_s == "Critical" |
summarize AggregatedValue = count()
by ServerName_s | count
```

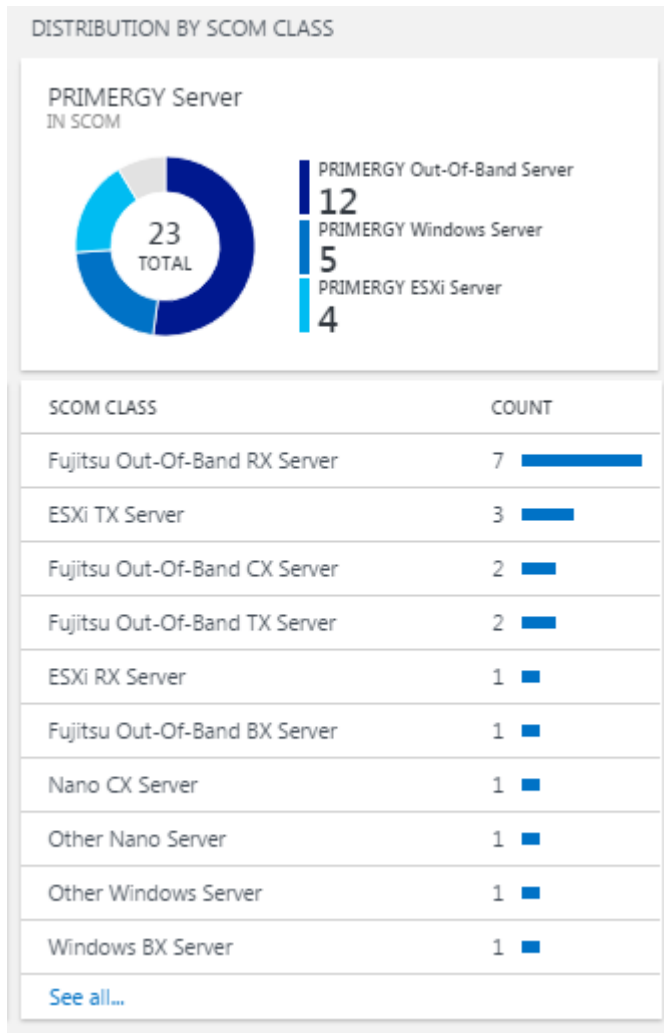
List:

- **Query:**

```
SVHEALTH_CL |
where TimeGenerated > ago(10m)
and ServerHealth_s == "Critical" |
summarize AggregatedValue = count()
by ServerName_s
```
- **Column Titles:**
 - **Name:** *Server Name*
 - **Value:** *State*
- **Hide Graph:** *<checked>*
- **Color:** *select based on your personal preferences (only when 'Hide Graph' is not checked)*

5.5.5. Number of 'PRIMERGY Server in SCOM' View

The following view templates and queries were used in the 'PRIMERGY Server SCOM' Custom View. You can adopt this to your personal needs by modifying the query.



View Template:

- Donut & List

General Section:

- Group Title: *Distribution by SCOM Class*

Header Section:

- Title: *PRIMERGY Server*
- Subtitle: *In SCOM*

Donut Section:

- Query: `SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = count() by ClassType_s | sort by AggregatedValue desc`
- Center
 - Text: *Total*
 - Operation: *Sum*
- Advanced Color Mapping
 - select based on your personal preferences

List:

- Query: `SVHEALTH_CL | where TimeGenerated > ago(10m) | summarize AggregatedValue = count() by ClassName_s | sort by AggregatedValue`
- Column Titles:
 - Name: *SCOM Class*
 - Value: *Count*
- Hide Graph: *<unchecked>*
- Color: select based on your personal preferences (only when 'Hide Graph' is not checked)

5.5.6. 'List of Queries' View

The following view templates and queries were used in the 'List Of Queries' Custom View. You can adopt this to your personal needs by modifying or adding queries.

LIST OF QUERIES
PRIMERGY Server Health <code>SVHEALTH_CL where TimeGenerated > ago(10m) sort by Time...</code>
PRIMERGY Server Model <code>SVHEALTH_CL where TimeGenerated > ago(10m) summarize A...</code>
PRIMERGY Server Class <code>SVHEALTH_CL where TimeGenerated > ago(10m) summarize A...</code>
Health Data transferred <code>SVHEALTH_CL summarize AggregatedValue = count() by bin(Ti...</code>
Time of last data received <code>SVHEALTH_CL summarize LastValue = max(TimeGenerated) by ...</code>

View Template:

- *List of queries*

General Section:

- Group Title: *List of queries*
- Render mode: `<grid>`

Query 1:

- Query:
`SVHEALTH_CL |
 where TimeGenerated > ago(10m) | sort
 by TimeGenerated desc | project
 NetworkName_s, ServerName_s,
 ServerModel_s, ServerHealth_s,
 MaintenanceMode_b`
- Friendly Name: *PRIMERGY Server Health*

Query 2:

- Query:
`SVHEALTH_CL |
 where TimeGenerated > ago(10m) |
 summarize AggregatedValue = count()
 by ServerModel_s`
- Friendly Name: *PRIMERGY Server Model*

Query 3:

- Query:
`SVHEALTH_CL |
 where TimeGenerated > ago(10m) |
 summarize AggregatedValue = count()
 by ClassType_s`
- Friendly Name: *PRIMERGY Server Class*

Query 4:

- Query:
`SVHEALTH_CL |
 summarize AggregatedValue = count()
 by bin(TimeGenerated, 15m) |
 sort by TimeGenerated desc`
- Friendly Name: *Time of last data received*

Query 5:

- Query:
`SVHEALTH_CL |
 summarize LastValue =
 max(TimeGenerated) by ServerName_s`
- Friendly Name: *Health Data transferred*

5.6. Further analyze SCOM Alerts in OMS with Custom Fields

All SCOM Alerts are forwarded from SCOM to OMS as part of the Microsoft 'Alert Management' Solution. Unfortunately the raw alert strings from the Management Pack are transferred without parameter substitution as AlertName field. As a result, some alert log entries may look very cryptic to OMS end customers and may need special attention to see the real root cause by carefully examining the also provided Alert Description field - which contains expanded properties.

The following section describes how you can extract valuable data from the AlertDescription as Custom Fields which then can be used for additional filtering and in Custom Views. The examples use traps sent Out-of-Band from an iRMC to the SCOM Server and extract the SNMP Trap Number and the Target IP from the raw alert data. The Source IP of the iRMC sending the trap sender is already available as standard alert field SourceDisplayName.

Technical description of Custom Fields is available from [9] of section 1.4.



Custom Field extraction may not work with your default web browser. It is recommended to use a Microsoft Browser or Google Chrome.



Custom Field extraction will be performed on new entries only. Old log entries will not be re-indexed.

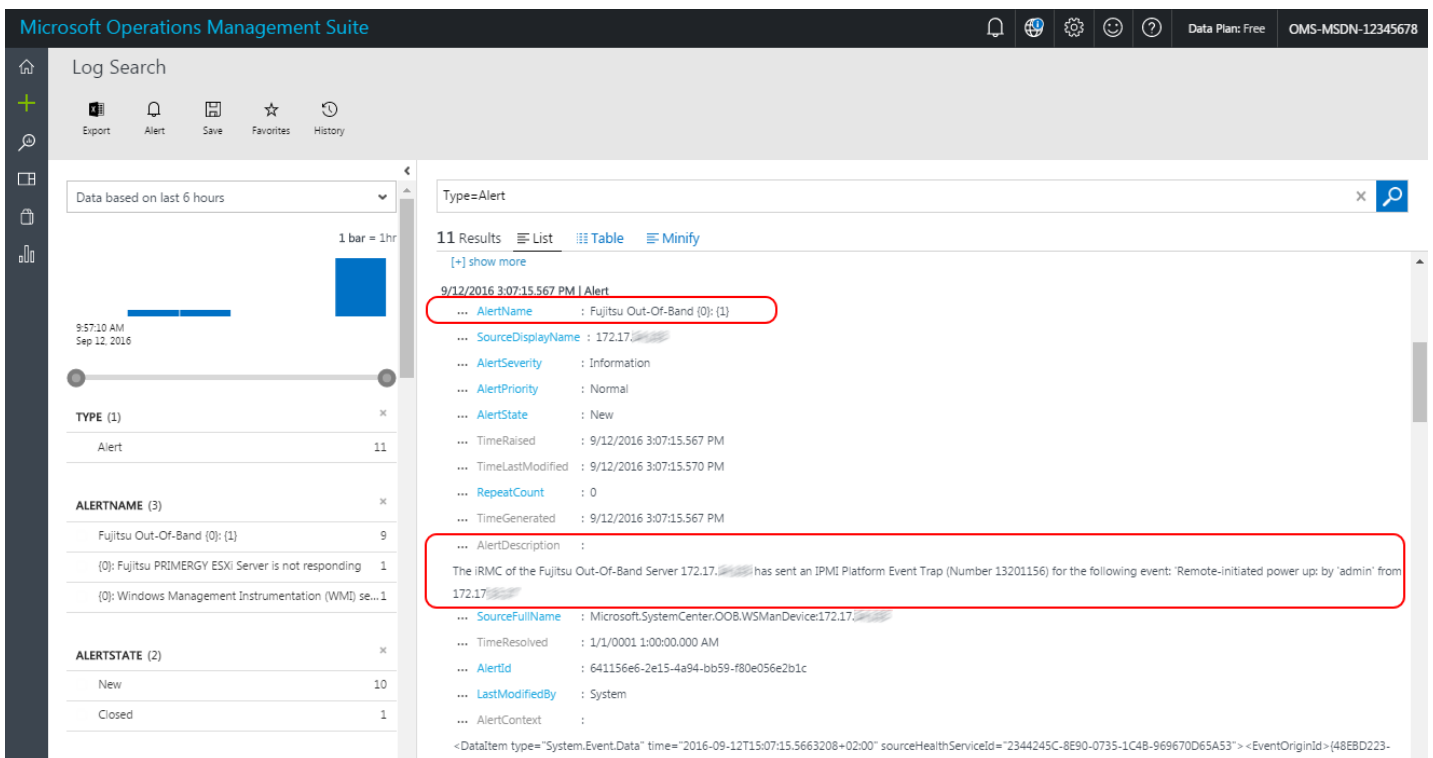
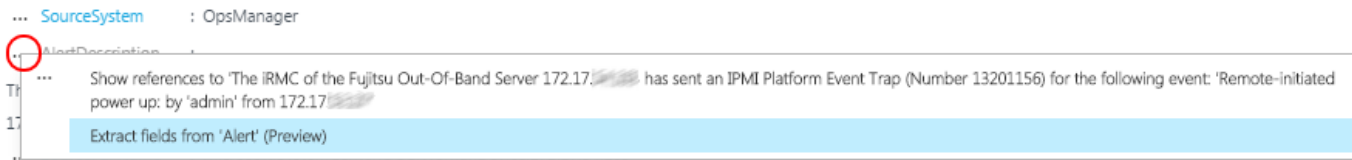


Figure 15 - Raw Alert name and Alert Description from a SNMP trap

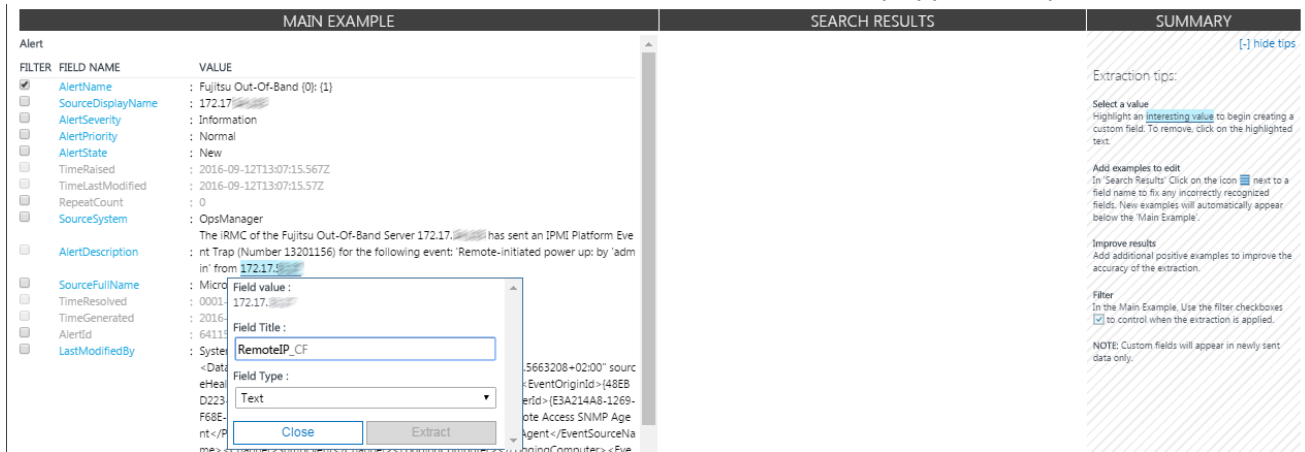
To define Custom Field extraction rules:

- ▶ Within the OMS workspace select *Log Search*
- ▶ Limit the displayed alerts to the ones of interest by applying filters from the left pane or by limiting the time range
- ▶ Switch to List View
- ▶ Expand the complete log entry by clicking on the *Show More*

- ▶ Click on the ... on the left side of the AlertDescription field. From the displayed context menu select 'Extract Fields'



- ▶ In the new menu select the IP address shown in the text after the 'by user 'xxx' from 192.168.1.100'. Give it the name RemoteIP (Note: the _CF for Custom Field will be automatically appended by OMS)



- ▶ Select 'Extract' and verify from the list of displayed results the extraction is correct.



- ▶ Click 'Save Extraction'

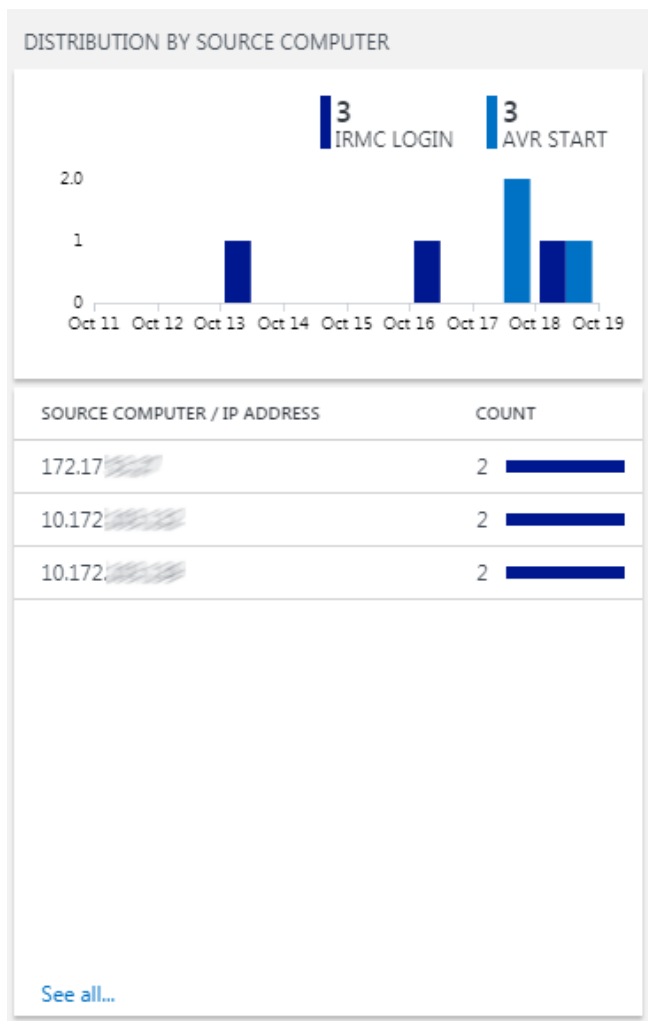
Repeat these steps for the trap number displayed after the text (Number 12345678) and save it as Custom Field *TrapNum_CF*

5.7. Create Custom Views with Custom Fields

5.7.1. 'iRMC Login and AVR Started' View

The following view templates and queries were used in the 'iRMC Login and AVR Started' Custom View. You can adopt this to your personal needs by modifying the query.

The queries use the previously defined Custom Fields to filter for specific trap numbers and display the source IP address from the computer where the Login/AVR was started (not the IP address of the iRMC which is available as SourceDisplayName field). See [iRMC Trap Numbers](#) for a subset of possible Platform Event Trap numbers sent from the iRMC.



View Template:

- Two Timelines & List

General Section:

- Group Title: *Distribution by Target iRMC / Computer*

First Chart:

- Legend: *iRMC Login*
- Color: *select based on your personal preferences*
- Query: `Alert | where AlertName=="Fujitsu Out-Of-Band {0}: {1}" and TrapNum_CF==13135873`
- Calculation: `<Sum>`

Second Chart:

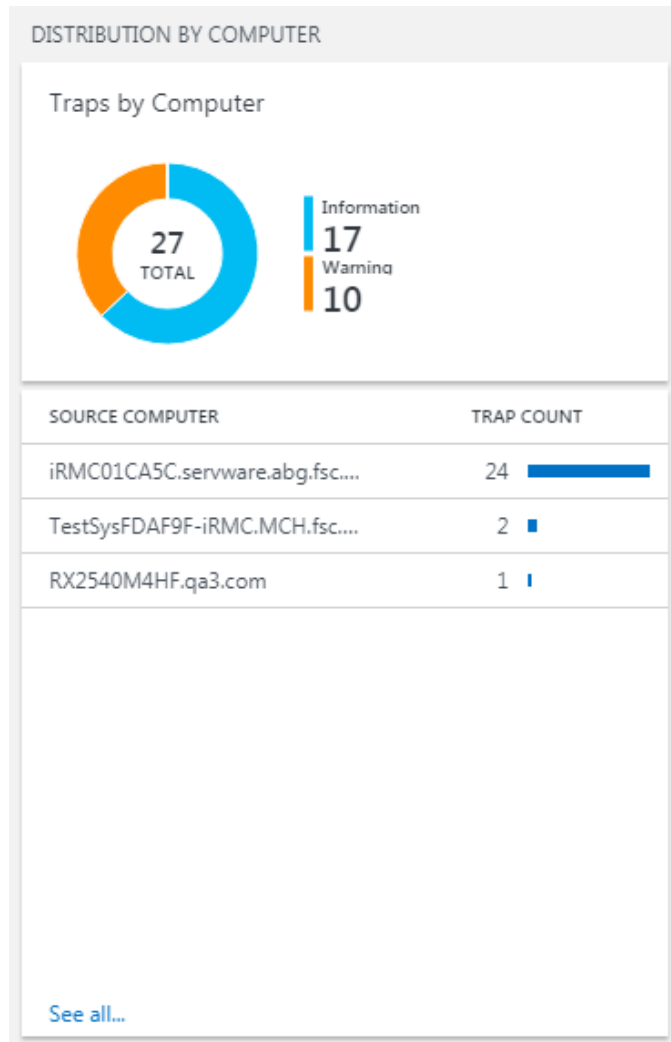
- Legend: *AVR Start*
- Color: *select based on your personal preferences*
- Query: `Alert | where AlertName=="Fujitsu Out-Of-Band {0}: {1}" and TrapNum_CF==13139712`
- Calculation: `<Sum>`

List:

- Query: `Alert | where AlertName=="Fujitsu Out-Of-Band {0}: {1}" and (TrapNum_CF==13135873) or (TrapNum_CF==13139712) | summarize Count = count() by RemoteIP_CF`
- Hide Graph: `<unchecked>`
- Enable Sparklines: `<unchecked>`
- Column titles:
 - Name: *Source Computer*
 - Value: *iRMC Login From*
- Hide Graph: `<unchecked>`

5.7.2. 'iRMC Traps by Severity' View

The following view templates and queries were used in the 'iRMC Traps by Severity' Custom View. You can adopt this to your personal needs by modifying the query.



View Template:

- *Donut & List*

General Section:

- **Group Title:** *Distribution by Computer*

Header Section:

- **Title:** *iRMC Traps by Computer*
- **Subtitle:** *<empty>*

Donut:

- **Query:**

```
Alert | where
AlertState != "Closed"
and AlertName == "Fujitsu Out-Of-Band
{0}: {1}" |
summarize AggregatedValue = count()
by AlertSeverity |
sort by AggregatedValue desc
```
- **Center**
 - **Text:** *Total*
 - **Operation:** *Sum*
- **Advanced Color Mapping**
 - **Mapping 1**
 - **Field Value:** *Error*
 - **Color:** *#e81123 (red)*
 - **Mapping 2**
 - **Field Value:** *Warning*
 - **Color:** *#ff8c00 (orange)*
 - **Mapping 3**
 - **Field Value:** *Information*
 - **Color:** *#00bcf2 (blue)*

List:

- **Query:**

```
Alert | where
AlertState != "Closed"
and AlertName == "Fujitsu Out-Of-Band
{0}: {1}" |
summarize AggregatedValue = count()
by SourceDisplayName
```
- **Hide Graph:** *<unchecked>*
- **Column titles:**
 - **Name:** *Source Computer*
 - **Value:** *Trap Count*
- **Hide Graph:** *<unchecked>*

6. Appendix

6.1. Management Packs

The following Fujitsu SCOM Management Packs were used to create this white paper. All Fujitsu OMS Management Packs require a successful registration of your SCOM to an OMS workspace.

Install only the features which are of specific interest to your hybrid management scenarios. Depending on the feature you can fine tune them with standard SCOM rule overrides.

Feature	Management Pack
Fujitsu ServerView Server Collect Health State to OMS	Fujitsu.ServerView.Monitoring.Cloud.mpb
Fujitsu PRIMERGY Out-Of-Band Server Collect Performance Data to OMS	Fujitsu.Servers.PRIMERGY.OutOfBand.PerfMon.Cloud.mpb
Fujitsu PRIMERGY Windows Server Collect Performance Data to OMS	Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.mpb
Fujitsu PRIMERGY Linux Server Collect Performance Data to OMS	Fujitsu.Servers.PRIMERGY.Linux.PerfMon.Cloud.mpb
Fujitsu PRIMERGY ESXi Server Collect Performance Data to OMS	Fujitsu.Servers.PRIMERGY.ESXi.PerfMon.Cloud.mpb

6.1.1. Fujitsu ServerView Server - Collect Health State to OMS

This Management Pack contains a rule targeting the SCOM Management Group and collects PRIMERGY Health State information using the OMS HTTP Data Collector API from [7] in Section 1.4.

The name of the rule is "Fujitsu ServerView Collect Health State to OMS"

The following overrides are supported:

Parameter Name	Parameter Type	Default Value
Enabled	Boolean	True
Interval Seconds	Integer	600
Timeout Seconds	Integer	120
Sync Time	String	0:00
Log Type	String	SVHEALTH
Skip Windows Server	Boolean	False
Skip Linux Server	Boolean	False
Skip ESXi Server	Boolean	False
Skip Out-Of-Band Server	Boolean	False

6.1.2. Collect Performance Data to OMS Management Packs

These Management Packs contain O/S specific performance collection rules for PRIMERGY servers (Windows, Linux, ESXi and Out-Of-Band). The list of OMS rules is identical to the list of SCOM performance collection rules for the O/S specific Performance Management Pack and uses the same SCOM Data Source; therefore Cookdown will be performed by SCOM.



Since OMS performance data is stored as log entry in the cloud the collection interval can be shorter than standard SCOM performance collection interval. OMS supports collection intervals as low as 10 seconds up to 30 minutes as Near Realtime Performance (NRT) Counter.

Temperature Performance Collection Rules:

Rule Name	Default Enabled	Default Interval
Fujitsu Windows 'Ambient (°C)' to OMS Temperature Data Collection Rule	False	600
Fujitsu Windows 'Processor (°C)' to OMS Temperature Data Collection Rule	False	600
Fujitsu Windows 'Memory (°C)' to OMS Temperature Data Collection Rule	False	600
Fujitsu Windows 'Power Supply (°C)' to OMS Temperature Data Collection Rule	False	600
Fujitsu Windows 'System Board (°C)' to OMS Temperature Data Collection Rule	False	600
Fujitsu Windows 'Other (°C)' to OMS Temperature Data Collection Rule	False	600

Power Consumption Performance Collection Rules:

Rule Name	Default Enabled	Default Interval
Fujitsu Windows 'Total (Watt)' to OMS Power Consumption Data Collection Rule	False	300
Fujitsu Windows 'System Chassis (Watt)' to OMS Power Consumption Data Collection Rule for Multi Node Systems	False	300
Fujitsu Windows 'Processor (Watt)' to OMS Power Consumption Data Collection Rule	False	300
Fujitsu Windows 'Power Supply (Watt)' to OMS Power Consumption Data Collection Rule	False	300
Fujitsu Windows 'Other (Watt)' to OMS Power Consumption Data Collection Rule	False	300

6.2. iRMC Trap Numbers

The iRMC sends IPMI Platform Event Traps (PET) which technically are SNMPv1 traps. The trap number is based on a fixed calculation schema including the IPMI Sensor Type, Event Reading Type and Sensor Event Offset (see below). The following table lists some of the possible standard IPMI and OEM trap numbers an iRMC can send. The full list of possible events is available as MIB file and available with the ServerView Operations Manager (file WfM.mib).

Sensor Type (hex)	Event Reading Code (hex)	Offset (hex)	Trap Number (decimal)	Trap Description
C8	71	00	13136128	CLI Consecutive Login Failed
C8	71	01	13136129	CLI Login
C8	71	02	13136130	CLI Logout
C8	71	06	13136134	CLI Login Failed
C8	70	00	13135872	Consecutive Login Failed
C8	70	01	13135873	Login
C8	70	02	13135874	Logout
C8	70	03	13135875	Auto Logout
C8	70	06	13135878	Login Failed
C9	6F	01	13201153	Server Reset
C9	6F	02	13201154	Power Cycle
C9	6F	03	13201155	Power Off
C9	6F	04	13201156	Power On
C8	7F	00	13139712	AVR Started
C8	7F	01	13139713	AVR Finished
20	6F	00	2125568	Critical Stop during OS load / initialization
20	6F	01	2125569	Run time Critical Stop (a.k.a. 'core dump', 'blue screen')
20	6F	02	2125570	OS Graceful Stop
20	6F	03	2125571	OS Graceful Shutdown

Specific Trap and Variable Bindings Fields

The specific-trap and variable-bindings fields carry the heart of the Platform Event Trap information. The content and definition of these fields is specified in the following tables.

Table 2 - "Specific Trap" field

Field #	Name	size/ type	Description
1	Event	integer	<p>31:24 reserved. 0000_0000b</p> <p>23:16 Event Sensor Type An <i>Event Sensor</i> is a logical entity that is responsible for detecting events. The <i>Event Sensor Type</i> field indicates what types of events the sensor is monitoring. E.g. <i>temperature, voltage, current, BIOS, POST, processor, fan, etc.</i> (This field corresponds to the IPMI 'Sensor Type' field, and conceptually maps to the 'cause of trap' field in the Phoenix proposal.)</p> <p>15:8 Event Type Code indicating what type of transition / state change triggered the trap. (Corresponds to IPMI 'Event Type' field) The code is split into the following ranges: 00-0Bh = generic - can be used with any type of sensor 6Fh = sensor specific 70h-7Fh = OEM all other = reserved See Table 4, below, for generic event type codes</p> <p>7:0 Event Offset Indicates which particular event occurred for a given Event Type. This field allows events to be extended on a per Event Type basis—making it easier to manage the Event Type 'name space'. 7 0 = Assertion Event. (Event occurred when state became asserted) 1 = Deassertion Event. 6:4 reserved. 000b. 3:0 Offset Value. Per IPMI, up to 15 different discrete states are allowed per each Event Type. 0Fh = unspecified.</p>

6.3. Custom Views

The following Custom Views are distributed as part of this white paper. These can be imported as described in section 5.1.6 and can be used as starting point for creating your own custom OMS views.

ServerView® PRIMERGY Server Health.omsview	
ServerView® PRIMERGY Power Consumption.omsview	
ServerView® PRIMERGY Ambient Temperature.omsview	
ServerView® iRMC Login and AVR Started.omsview	
Windows Power Consumption.omsview	

Contact
FUJITSU Technology Solutions GmbH
Address: Mies-van-der-Rohe-Strasse 8,
80807 Munich, Germany
Website: www.fujitsu.com
October 2017

Copyright 2016 - 2017 FUJITSU LIMITED
Fujitsu, the Fujitsu logo are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. Other company, product and service names may be trademarks or registered trademarks of their respective owners. Technical data subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.