

Why use Azure Log Analytics

Many companies are already using Azure services; directly or indirectly. Directly is a workload like virtual server or appliance. Indirectly would be using Azure Directory Services while using Teams. In either case there is already some level of experience with Azure. This includes Directory Synchronization and access delegation to service payments. Because of this adding Azure log services becomes a simple add-in. Azure Log Services can be used to monitor more than just Skype Room Systems. It can monitor all levels of a Windows based system as well as syslog services and direct file analytics. It offers a robust tools and query languages to develop reports on different types of logs.

What is Azure Log Analytics

Azure Log Analytics is a subset of the Azure Monitoring service. Log data collected by Azure Monitor is stored in a Log Analytics workspace, which is based on Azure Data Explorer. It collects telemetry from a variety of sources.

Set up your Skype Room Systems

Ensure that you have one Skype Room System completely setup and working. Having these setup now will make the next steps easier. If you don't have IPv6 running, I will go through managing that in a later step. This includes the following components

1. IP Connectivity (v4 and v6)
2. Camera
3. Audio Device
4. Device Ingest (HDMI In)
5. Signed into a room account

Setting up Azure Log Monitoring, Analytics, And Reporting for a PC

Setting up Azure log analytics is not just a click and go solution. There is setup required for this to work

1. Setup and account in Azure.
2. Setting up a Resource Group.
3. Configure the workspace
4. Configure the logs
5. Setup the Dashboard
6. Configure Alerting

First you need to set yourself up with an account in Azure. Note that the Free Trial runs for 30 days with \$200 credit. As a starting point to monitor 10 systems for 1 month is under \$1/month. The more system you add and the more log files, the more it will cost. But for the cost of it and what it can do. Chrome seems to work the best with Azure.

1. <https://azure.microsoft.com/en-us/free/>
2. Click on Start Free Trial (or pay as you go, either way it is the same)
3. Go through the signup process, should only take about 10 minutes

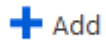
Set up a Resource Group

A Resource Group is a container that holds related resources for an Azure solution. It is a logical grouping such as Room Systems, Log Analytics, storage accounts, virtual networks, and virtual machines (VMs) as a single entity. For example you may want to create a Resource Group just for Room System Log Analytics

1. Click on Resource Groups



2. Click Add



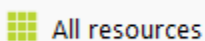
3. When you create your account, you either had a free trial or Pay-as-you go. From the Subscription choose that options
4. In the resource group enter a descriptive name, here are some ways to think about this: <https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions>
5. Under Region choose the location where you want your data stored. This is typically near your primary office. In this example I will call it VideoConferencing
6. Once you have reviewed the configuration it will take a few minutes to create it.

Setting up the Workspace

A workspace is a container in which to manage a subset of data from a Resource Group. For example to access, manage, and query data from Log Analytics a workspace is used.

The following steps are also found at: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

1. Go to All Resources



2. Click Add



3. In the Search type Log Analytics
4. At the bottom of the screen click Create
5. In the Workspace enter a name. This is just a name of a place to store the data and configuration. Typically this would be OMS... In this example I am using OMSDevices
6. Choose the subscription used when creating the Resource Group
7. Choose the location of where you want to store your data, this is usually the same as the Resource Group

Log Analytics workspace ✕
Create new or link existing workspace

☒ Create New ☐ Link Existing

* Log Analytics Workspace ?
OMSDevices ✓

* Subscription
Pay-as-you-go ▼


* Resource group ?
☐ Create new ☒ Use existing
VideoConferencing ▼

* Location
West US 2 ▼

* Pricing tier
Per GB >

Download the Agent

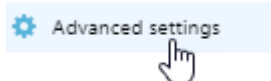
1. Click on All resources

 All resources

2. There you should see the workspace just created, OMSDevices, click on it



3. Click on Advanced Settings



General

4. There you will get dropped into the agent details

Connected Sources >

Data >

Computer Groups >

Windows Servers >

Linux Servers >

Azure Storage >

System Center >

Windows Servers
Attach any Windows server or client.

0 WINDOWS COMPUTERS CONNECTED

[Download Windows Agent \(64 bit\)](#)

[Download Windows Agent \(32 bit\)](#)

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID

PRIMARY KEY
 [Regenerate](#)

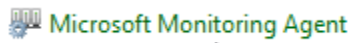
SECONDARY KEY
 [Regenerate](#)

5. Download the 64bit agent since you are most likely running 64bit Windows 10
6. You will need to copy the Workspace ID and Primary Key.

Install the Agent

There are two ways to install the agent, command line and the GUI. The GUI is pretty straight forward, so I will focus on the command line.

1. Extract the MSI file you can use 7ZIP or running the download with
2. Create a batch file with the following line in it (notice the quotes), save it as
c:\source\MMA\installMMA.cmd
3. Open a command prompt with elevated permissions and run the above batch file
4. You can tell if the agent installed correctly in two ways. First check the control panel for the Microsoft Monitoring Agent
5. Go to the Azure Log Analytics Tab (OMS). If it shows a green checkbox you are good, if it shows anything else, remove it and re-add it. Most likely the WorkspaceID or Primary Key are wrong
6. Now WAIT at least 5 minutes, it takes some time for the device to show up in the advanced settings tab (from the same place where you downloaded the agent)



Configure Log Data

The steps listed below are derived from: <https://docs.microsoft.com/en-us/microsoftteams/room-systems/azure-monitor-deploy>. The entire process should take about 20 minutes to setup.

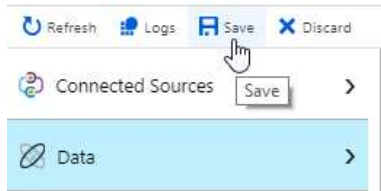
Configure the log sources

1. Configure the SRS logging: https://docs.microsoft.com/en-us/microsoftteams/room-systems/azure-monitor-deploy#configure_test_devices
2. To get there click on click on All Resources, then the workspace (OMSDevices in this example) and then advanced settings
3. Then click on Data Windows Event Logs
4. In the name enter Skype Room System and then the + to add it (it will not auto fill that event log since it is not a common file)

Collect events from the following event logs

LOG NAME	ERROR	WARNING	INFORMATION	
Skype Room System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove

5. Then click Save (in the left side of the window, DON'T forget to SAVE)



Validate the logs

This can take a long time (sometimes up to a few hours) to retrieve the data. It depends on how long your system has been active and internet, and so on.

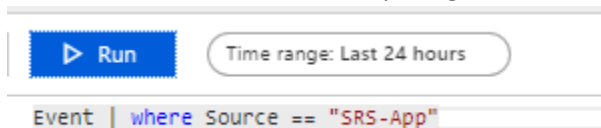
1. Click on Monitor in the left navigation window



2. Click on Logs



3. That will take you to the query window where you can enter your test commands. It can take some time for data to show up, so give it about 5 minutes



4. Then click Run. That should return a list in the bottom window. Repeat this for the other examples. Note that if you get stuck at "We're getting your data, hang in there", for a long time, you will need to start over (Monitor → OMS Devices → Logs)
5. I have found it helpful to save commands as I go
 - a. Click Save in the right hand side



- b. Then give it a name, save it as a query and a category. The category can be re-used. So the next time you save, it will be a drop down list as well as a free-form text

Name

Save as

Category

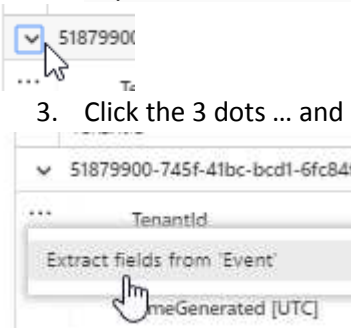
Map Custom Fields

Before continuing make sure the SRS has been configured. To generate an event, unplug a device for 3 seconds and plug it back in. Then wait a few for the log to be updated in OMS. If you don't do this, the

next step will not be doable. https://docs.microsoft.com/en-us/microsoftteams/room-systems/azure-monitor-deploy#Custom_fields

Mapping custom fields takes time, it is repetitive. In the example we will map the field Description

1. Run the search: *Event | where Source == "SRS-App" and EventID == 2000*
2. Expand one of the records, doesn't matter which



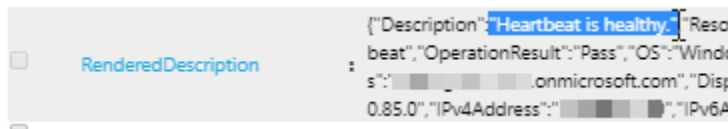
3. Click the 3 dots ... and choose Extract Fields

4. Check the box next to the Event ID, this should be checked by default

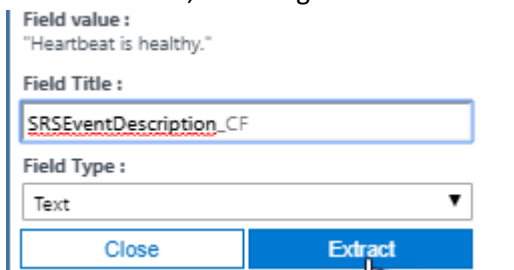


5. Under Rendered Description select the text of the field to the right of "Description":

6. The first field that is being sampled is Conference Speaker Status. Select the value of that field, not the field name, include the quotes.



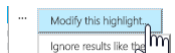
7. When selected a you will be asked to give the field a name. Make sure you have the value correct, and assign it the name SRSEventDescription. The _CF cannot be changed.



8. Click Extract
9. This will then show you where that string shows up from the above query that you used to get to this screen

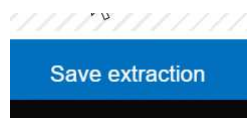


10. If you need to make a change to the selection you can click on the edit button at the upper right of the blue box and then select Modify this highlight



11. Then at the far right is the summary. This is also how you can double check if you checked the EventID box or not.

12. If everything is correct click on the save extraction on the bottom right



13. Once you click the Save extraction you will go back to the query window. You will now need to repeat these steps for each of the JSON fields:

If you are not running IPv6, you can skip that field, and changes to the dashboard will have to be manually edited.

JSON field	Log Analytics custom field	Event ID	Query to use with the extraction
Description	SRSEventDescription	2000	Event where Source == "SRS-App" and EventID == 2000
ResourceState	SRSResourceState	2000	Event where Source == "SRS-App" and EventID == 2000
OperationName	SRSOperationName	2000	Event where Source == "SRS-App" and EventID == 2000
OperationResult	SRSOperationResult	2000	Event where Source == "SRS-App" and EventID == 2000
OS	SRSOSVersion	2000	Event where Source == "SRS-App" and EventID == 2000
OSVersion	SRSOSLongVersion	2000	Event where Source == "SRS-App" and EventID == 2000
Alias	SRSAlias	2000	Event where Source == "SRS-App" and EventID == 2000
DisplayName	SRSDisplayName	2000	Event where Source == "SRS-App" and EventID == 2000
AppVersion	SRSAppVersion	2000	Event where Source == "SRS-App" and EventID == 2000

Pv4Address	SRSIPv4Address	2000	Event where Source == "SRS-App" and EventID == 2000
Pv6Address	SRSIPv6Address	2000	Event where Source == "SRS-App" and EventID == 2000
Conference Microphone status	SRSConfMicrophoneStatus	3001	Event where Source == "SRS-App" and EventID == 3001
Conference Speaker status	SRSConfSpeakerStatus	3001	Event where Source == "SRS-App" and EventID == 3001
Default Speaker status	SRSDefaultSpeakerStatus	3001	Event where Source == "SRS-App" and EventID == 3001
Camera status	SRSCameraStatus	3001	Event where Source == "SRS-App" and EventID == 3001
Front of Room Display status	SRSFORDStatus	3001	Event where Source == "SRS-App" and EventID == 3001
Motion Sensor status	SRSMotionSensorStatus	3001	Event where Source == "SRS-App" and EventID == 3001
HDMI Ingest status	SRSHDMIIngestStatus	3001	Event where Source == "SRS-App" and EventID == 3001

Removing an incorrect JSON field

Once you have gone through and done these all and realized that you forgot to uncheck or check the EventID box, you will need to delete those entries and re-create them, here is how

1. Go to All Resources → WorkspaceName (OMSDevices) → Advanced Settings
2. Then click on Data → Custom Fields

FIELD NAME	LOG TYPE	FIELD TYPE	Go to	Remove
AppVersion_CF	Event	Text	Go to	Remove
SRSCameraStatus_CF	Event	Text	Go to	Remove
SRSConfSpeakerStatus_CF	Event	Text	Go to	Remove
SRSDefaultSpeakerStatus_CF	Event	Text	Go to	Remove
SRSEventDescription_CF	Event	Text	Go to	Remove
SRSFORDStatus_CF	Event	Text	Go to	Remove
SRSHDMIIngestStatus_CF	Event	Text	Go to	Remove
SRSIPv4Address_CF	Event	Text	Go to	Remove
SRSMotionSensorStatus_CF	Event	Text	Go to	Remove

3. Find the field in question and click Remove. There is no way to edit the extraction. You will just need to re-create them.

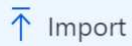
Importing the Dashboard

The process can be found here: https://docs.microsoft.com/en-us/microsoftteams/room-systems/azure-monitor-deploy#Define_Views

1. Download the pre-canned view: <https://go.microsoft.com/fwlink/?linkid=835675>
2. Go to All Resources → Select the Work Space
3. Click on View Designer



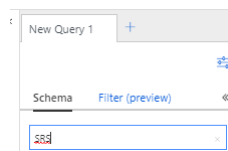
4. Click on import to upload the file



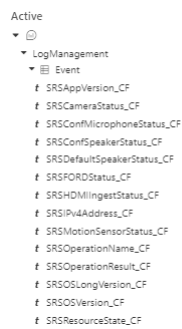
5. Upload the file SkypeRoomSystems_v2.omsview
6. CLICK SAVE!
7. After clicking save, press the push pin in the upper right corner to save it to your main Dashboard

Troubleshooting

1. Usually if you don't see what you expect, it means that somewhere during the export you grabbed the wrong fields or gave it the wrong name. You can troubleshoot this by doing the following
 - a. Go back to Logs Query window (Monitor > Logs)
 - b. On the left under the Query Tab in the Schema Search type SRS

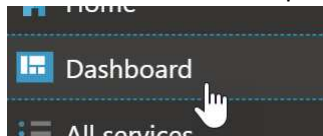


- c. That will filter out and show you just the Custom Fields you created



- d. In the Query Window enter the following. This example will show the IP address for all the computers. You can get the value for any by simply replacing the SRSIPv4Address_CF with one of the values above. Note that this is all Case Sensitive.

2. From the main panel click on Dashboard



If you are not running IPv6

If you are not running IPv6 or decided not to import a field you will need to manually remove it from the imported field.

1. In the dashboard click on Edit



2. On the properties windows scroll down to Click-Through Navigation
3. Copy the text in the Navigation Query and paste it into notepad
4. Find the text that you want to remove, for example SRSIPv6Address_CF,
5. Delete the text, make sure there is a space after all commas and paste it back into the Navigation Query field
6. Repeat this for each view in the Dashboard

Setting Up Alerts

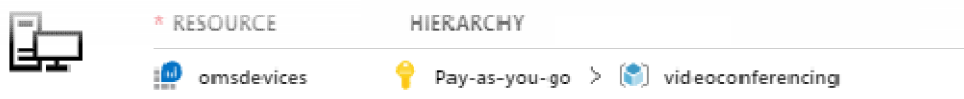
The documented process for building alerts can be found at <https://docs.microsoft.com/en-us/microsoftteams/room-systems/azure-monitor-deploy#Alerts>

1. Go back to log search and enter the following query (note that if you are not using IPv6 you should remove the SRSIPv6Address_CF,

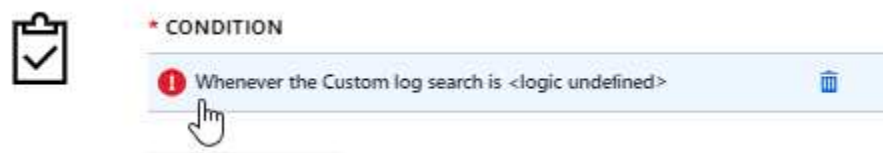
2. Once the query returns records, click on the New alert rule



3. Resource should show the workspace for logs:



4. The Condition will show a red bang symbol, click on that



5. In the Based on section choose Number of results is greater than 0
6. Set the evaluated based on 60 minutes and frequency 60 minutes. You will need to adjust these times as needed. Basically this means every 60 minutes (frequency) it will see what happened in the past 60 minutes (based on).

Alert logic

Based on [?] Operator [?] * Threshold value [?]

Number of results Greater than 0 ✓

Condition preview

Whenever the custom log search is greater than 1 count

Evaluated based on

* Period (in minutes) [?] * Frequency (in minutes) [?]

5 5

7. Under Action Groups click Create new



* ACTION GROUPS

Notify your team via email and text messages or aut

ACTION GROUP NAME

No action group selected

Select existing

Create New



- Fill out the details, make sure to pick the Resource Group that contains the Log analytics workspace. Choose the type of action. Once you fill that out, click the edit details. Usually Email/SMS/Push is most common, all of those are configured in the window that shows up. You will need to add an action item per email or push. So I would recommend distribution lists when possible (just to simplify the process)

* Action group name [?] IT VC Team ✓

* Short name [?] ITVCTeam ✓

* Subscription [?] Pay-as-you-go ✓

* Resource group [?] VideoConferencing ✓

Actions

ACTION NAME	ACTION TYPE	STATUS	DETAILS	ACTIONS
Email IT VC Team ✓	Email/SMS/Push/V... ✓		Edit details	✕

Please configure the action by clicking the link.

Unique name for the act... ✓

[Privacy Statement](#)

[Pricing](#)

- In the details you can add the email address, push, SMS, etc...

Name
Email IT VC Team

☒ Email
[Redacted] ✓

☐ Email Azure Resource Manager Role
None

☐ SMS
Country code: [1] Phone number: 1234567890

Carrier charges may apply.

☐ Azure app Push Notifications
[Learn about the connecting to your Azure resources using the Azure app.](#)
email@example.com
This is the email you use to log into your Azure account.

☐ Voice
Country code: [1] Phone number: 1234567890

OK

10. When you have configured that single notification, click OK. And email or message will go to whomever you have configured in that specific policy.
11. When all of your Policies have been configure click OK to take you back to the main screen
12. Check the box to change the subject to: Skype Room Systems v2 Hardware Failure Alert (or anything descriptive)

Customize Actions

☒ Email subject ⓘ

* Subject line ⓘ
Skype Room Systems v2 Hardware Failure Alert

13. Then click Create alert rule

Create alert rule

14. Now create a second rule. It will use almost the same process.
15. In the query window use the following statement (note that the SRSIPv6Address_CF has been removed in this example)

16. Click on the New Alert Rule
17. Set the Conditions the same as before
18. Under Action Groups, click Select existing:, the one you created previously
19. Change the subject to: Skype Room Systems v2 Application Failure Alert
20. Alert Rule Name: Skype Room Systems v2 Application Failure Alert
21. Description: List of devices that encountered an application issue within the last hou
22. Severity Critical (Sev0)

Changing Alerts

If you ever need to change alert (frequency, notifications, etc..), or view current alerts

1. Go to your resources and select the workspace
2. Under monitoring choose alerts



3. Then choose what you want to change



Some Advanced Queries

List Rooms with Details

This example will show details by computer, you can add any other details as well.

```
Event |  
where EventLog == "Skype Room System" and EventID == 2000 and SRSOperationName_CF  
== "Heartbeat" |  
summarize by Computer, SRSAlias_CF, SRSApVersion_CF, SRSOSVersion_CF,  
SRSOSLongVersion_CF
```