

Network Bandwidth Measurement & Monitoring Solution using Azure Monitoring (Service Map)

Intended for planning or monitoring SaaS/PaaS network connectivity.

> Published: December 2019 Version: 3.4

> > This document provides the steps to implement a solution which allows customers to remotely capture information from network connections so as to provide insights into connectivity and also monitor bandwidth utilization of machines or individual processes/services

© 2018 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This

document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Table of Contents

1	Inti	roduction	2
2	Pre	requisites	3
3	Ant	ticipated Usage Scenarios	4
4	Ste	p by Step Guide	6
4	4.1	Login to Azure portal	6
2	4.2	Creating the Log Analytics workspace	6
4	4.3	Configure Log Analytics workspace for Service Map	8
2	4.4	Client-Side Configuration	. 11
2	4.5	Analyzing Data in Log Analytics	. 15
4	4.6	Example Queries	. 21
2	4.7	Adding graphs to an Azure Dashboard	. 28
4	4.8	Building a Dashboard in Power Bl	. 29
4	4.9	Publish a Power BI Dashboard	. 32
4	4.10	AutoRefresh Power BI Dashboard	. 33
5	Sur	nmary	. 34

1 Introduction

As the world moves to the cloud, a critical piece of this transformation is around the network which connects users and businesses to their data and services. The path changes from a relatively simple line between the location of the users and the data/services, to a distributed model where data is in multiple places, and users are accessing it from a variety of locations and devices.

Planning physical connectivity for Microsoft cloud users should revolve around local egress as close to the user as possible so that the traffic can reach Microsoft's global network as quickly as possible. More detail on this specific to Office 365 can be found <u>here</u>.

Another major part of this transformation is planning how much bandwidth is required on the circuits which connect out of the enterprise. As user's data and services move from being hosted on the internal network, to being hosted in Microsoft datacenters, the path this data takes changes. in addition, the amount of data users send and receive changes as their available services increases or changes.

However, planning the amount of bandwidth can be a major challenge as every user and enterprise is different so it's impossible to give an average figure, what will be correct for one enterprise will be insufficient for another customer and far too much for another.

The traditional approach to solving this problem is a combination of monitoring pilot users and using process specific calculators to give an estimate based on assumed information or that obtained from pilot users. There are however multiple challenges with this model

- a. It's not always easy to obtain accurate data from pilot users
- b. Calculators provide an estimated answer, if incorrect information is entered, the result is therefore wrong. As the investment in bandwidth is normally a lengthy process which has an associated cost, it is imperative this information is correct so that the right long-term planning decisions can be taken.
- c. Calculators focus on a single service where the planning needs to be done at a higher level covering all services.

With these challenges in mind we have created a more scalable, simpler solution to allow the accurate collection and display of the data required to make informed decisions in this space, and to enable easier monitoring of connectivity of our clients as we move to the cloud.

This solution will allow you to monitor and analyse the following example scenarios:

- Bandwidth used for a particular process or set of processes over a set period of time
- Bandwidth used by the machine over a set period of time
- Bandwidth used in connections to a specific port
- Bandwidth used to a specific IP address or range of addresses
- IP geolocation of the endpoints connected to

The approach in this document can be used for:

- 1. Measuring network bandwidth usage for pilot users on-boarded to Office 365 or network bandwidth usage of on-premises users.
- 2. Endpoint monitoring dashboard post on-boarding users to Office 365

You can apply this concept for measuring any SaaS/PaaS traffic, not just Office 365.

2 Prerequisites

The solution in this document requires a number of components bought together to provide the desired outcome, the good news is they are all easy to implement and should take 30-60 minutes in total to set up. For reference, the requirements are:

1. An Azure Subscription

As the solution has Azure at its core, a valid Azure subscription with permissions to add components to that subscription (or the ability to ask an administrator to add them) is required. You can use your work or personal account to login to Azure, if this is for your organization then its recommended you use your work account and a subscription associate with your work account.

2. Azure Log analytics workspace

You could opt to use Log Analytics as an individual service and in this case, billing is based on the data ingested into the workspace (Per GB pricing). This features cloud-friendly, consumption-based pricing that includes a Free tier for testing. You only pay for what you use, here is the pricing.

3. Agent installs

a. Microsoft monitoring agent can be installed from the Azure portal itself by going to Log Analytics workspace and then the Advanced settings blade.



- b. You will also need Dependency agent for Windows or Linux (see section 4.4 Client-Side configuration)
- c. **UDP is now supported to measure network bandwidth usage for Teams**, just ensure you have the latest version of the Dependency agent installed.

4. Scaling this solution & connecting via OMS Gateway

Enterprise customers have scaled the agent deployment to thousands of workstations/servers by using SCCM. Enterprise customers also tend to use OMS Gateway as a gateway to ingest data to log analytics workspace if direct connection to the workspace from workstations/server is not an option.

5. <u>Resources at Github</u>

All resources referred in this document like scripts, templates are available at <u>Github</u>, there is also an INTRO pdf document for a high-level summary of this solution with visuals.

3 Anticipated Usage Scenarios

The usage scenarios for this solution depends on the network setup in place, or that which is possible for use.

Below are some anticipated scenarios:

A. Client has direct network connectivity (i.e. no proxy)

This is the simplest of scenarios, where the client/s being monitored connects directly connect to internet resources, i.e. they do a DNS lookup and directly connect to the public IP address in question. in this case we simply need to install the agents on the client and point them at our log analytics workspace. This method also works the same way when a transparent proxy is in place.

The Microsoft monitoring agent and Dependency agent is installed on the clients directly.

B. Client uses a proxy where the administrator can install the Agents on the proxy OS

If the clients to be monitored connect to the internet via a managed Linux proxy where the agents can be installed, for example a Squid proxy running on CentOS then we can simply monitor the clients by analysing the traffic leaving the proxy. Supported Linux versions can be found <u>here</u>.

It may be feasible for an organization to set up a temporary proxy of this type in Azure or on Premises simply for the monitoring of Bandwidth to specific endpoints, leaving standard browsing to traverse the standard web proxy.

C. Client uses a proxy where the administrator cannot install the agents.

In this scenario, where the user's only connection method to the internet is through a proxy solution where the agents cannot be installed to the host OS, then we need to get a little creative. One method is to open up secondary/tertiary ports on the existing proxy and edit the PAC file to send specific traffic we wish to monitor to that port.

For example:

Port 8080 – Default Web traffic port

Port 8081 – Exchange Online URLs

Port 8082 – SharePoint/OneDrive URLs

We can then monitor the bandwidth of traffic sent to the specific ports in Log analytics to give us an accurate view of traffic to the particular service. This usage scenario requires the agents to be installed on the clients we wish to monitor, as per scenario A.

D. Monitoring connectivity based on process vs destination IP's

One option which may be used is to monitor connectivity which originates from a single process. The above scenarios are necessary as some cloud services will have data accessed from a multitude of processes, it is therefore necessary to look at the destination address to capture the information for the service in question, regardless of the source process.

When an explicit proxy is used, the destination IP will always be the proxy IP for web bound traffic, thus we need to either capture on the proxy itself where we can see the destination IP to differentiate traffic, or we need to send known endpoints to a unique destination, such as a specific proxy port.

An example would be OneDrive for Business where access to data could come from the OneDrive Sync client, or any Office application, or the browser. We therefore need to filter based on the published SharePoint/OneDrive IP addresses to capture access from all sources.

However, some services will only be used by a single process in most cases, such as Outlook client being used for accessing Exchange. Technically OWA could be used in the browser but it would be known in advance if this is likely.

Therefore, for scenarios like this, the egress model does not matter as filtering can be performed against the Outlook.exe process and not the destination address which will differ based on the network egress model. This can also be a useful method for examples such as monitoring bandwidth usage to Exchange when on premises before any cloud deployment to give a view of current usage by the process, which also may aid in planning.

4 Step by Step Guide

4.1 Login to Azure portal

The first step is to login to the Azure portal for the account where you wish to host this solution. If you already have a tenant, simply login at https://portal.azure.com

If you don't already have one, or would like to test this solution in a new Azure instance, you can set up a free trial <u>here</u>.

4.2 Creating the Log Analytics workspace

- a. Once logged into the Azure Portal <u>https://portal.azure.com/</u>
- b. Start typing 'Log Analytics' in the search bar at the top, select 'Log Analytics' under Services
- c. Add a workspace if you don't have one already created
 - Give the workspace an appropriate name
 - Subscription is the one you wish to use for the workspace (as you may have more than one available)
 - Resource group is simply a collection of resources, you can either use an existing one, or create a new one.
 - Location is which Azure region you host the workspace in.

$\leftarrow \rightarrow 0$ G \Box http:	s://ms.portal.azure.com/#			
Preview Microsoft Azure		Report a bug	₽ log ana	× Q >_ 8
Create a resource	Dashboard ~ + New dashboard	🛪 Upload 🛛 🛨 Download 🖉 Edit 🖒 Share	RESOURCES	0 results
			SERVICES	0 Hours
	All resources All subscriptions	Quickstarts + tutorials	🧔 Log Analytics	
\leftrightarrow \rightarrow \circ $rac{1}{2}$	https://ms.portal.azure.com/#create/	hub		
≡ Microsoft Azure (P	review) 👸 Report a bug	, Search res	ources, services, and docs (G+/)	
Home > New > Log Analyti	CS			
Log Analytics				
Overview Plans				
Create a new workspace Workspace provides visibility machine data in a region you Link an existing workspace to Do you have an existing works	and insight across all the machines you have specified. To create a new workspa to Azure subscription space in the OMS portal? You can link y	manage through Operations Manageme ice, select the Create button below. our workspace with your Azure subscrip	ent Suite, including Log Analytics. tion by selecting the Create butto	Workspace stores collected
About Log Analytics The Microsoft Operations Mar Manage and protect Azure or	nagement Suite (OMS) takes IT manage AWS, Windows Server or Linux, VMwar	ment solutions to the cloud and gives y e or OpenStack with a cost-effective, all-	ou greater control and new capab in-one cloud IT management solu	ilities across your hybrid cloud. ution
Useful Links				

Watch Video Learn More Documentation Notice the options for pricing tier, you can select Pay-as-you-go or another option depending your subscription, typically Pay-as-you-go is preferred since you get first 5GB data ingestion free along with 31days for data retention.

← → Ů ŵ Å https://ms.portal.azure.com/#create/MicrosoftLogAnalyticsOMS
≡ Microsoft Azure (Preview) <mark>Č</mark> i Report a bug
Home > New > Log Analytics > Log Analytics workspace
Log Analytics workspace \Box × Create new or link existing workspace
Create New Link Existing
Log Analytics Workspace * 🕕
enter workspace name
Subscription *
O365 FT PM Internal Consumption - r 💙
Resource group *
Create new
Location *
East US 🗸
*Pricing tier > Pay-as-you-go (Per GB 2018)

Pay-As-You-Go

With Pay-As-You-Go pricing, you are billed per gigabyte (GB) of data ingested into the Log Analytics workspace.

FEATURE	FREE UNITS INCLUDED	PRICE
Data Ingestion	5 GB per organization per month ³	\$2.30 per GB

³The first 5 GB of data ingested per organization to the Azure Monitor Log Analytics service every month is offered free.

Data Retention

Every GB of data ingested into your Azure Monitor Log Analytics workspace can be retained at no charge for up to first 31 days. Data retained beyond first 31 days will be charged per the data retention prices listed below.

FEATURE	FREE UNITS INCLUDED	PRICE
Data Retention	31 days ⁴	\$0.10 per GB per month
⁴ For Azure Sentinel enabled workspaces the data is retained for free for 90	days.	

If you need more information regarding pricing for Azure Monitoring/Log analytics workspace please refer <u>here</u> or use the <u>Azure Pricing calculator</u>.

4.3 Configure Log Analytics workspace for Service Map

We will now configure Service Map in the workspace.

a. Go to the workspace you created in Log Analytics and click on 'workspace summary' on the left blade.

	demobandwidthmeasurement
	E Overview
	Activity log
	Access control (IAM)
	P Tags
Home > Log Analytics > demobandwidthmeasurement	X Diagnose and solve problems
Log Analytics « 🖈 🗙 Microsoft	SETTINGS
Add == Edit columns More	Locks
	Automation script
Filter by name	Advanced settings
NAME 1	GENERAL
	📣 Quick Start
demobandwidthmeasurement	Workspace summary

b. The workspace will be blank, click on 'Add' and select Service Map from the 'Management Solutions'.



Manag	gement Solutions 🛛 🖈 🗖 🗙
3	System Center Operations Manager Health Check (Preview) Microsoft
.	SQL Health Check Microsoft
0	Security and Audit Microsoft
Ŷ	Service Fabric Analytics Microsoft
10	Service Map Microsoft
•	Start/Stop VMs during off-hours Microsoft
E	Update Compliance Microsoft

c. Select Service Map and click 'Create', ensure you have the right workspace selected

Service Map			\$2	
Service Map presents Jeliver services and r process dependencie components, service eliminate the guessw rour environment, ar von't be left behind. prem.	a view of your servers a ely on other technologie s in real-time, without ar dependencies, and supp ork of problem isolation d perform Azure migrat Service Map supports W	is you think of them - as int is. Service Map discovers ar ny predefinition, and visual orting infrastructure config , identify surprise connection ions knowing that critical sy findows and Linux guests, f	terconnected systems the nd maps server and izes application juration. This helps you ons and broken links in ystems and endpoints or any cloud and on-	hat
Diagnostic and Usage	e Data			
Map service. Microso he Service Map servi	ft uses this Data to provi ice. Data includes inform d version and also includ	ide and improve the quality ation about the configurati es IP address, DNS name, a	y, security and integrity ion of your software like and Workstation name i	of e in
order to provide accu addresses or other co for more information Privacy Statement.	irate and efficient troubl ontact information. In on data collection and i	eshooting capabilities. We usage, please see the Micro	do not collect names, psoft Online Services	
order to provide accu addresses or other cc or more information Privacy Statement.	irate and efficient troubl intact information. I on data collection and i	eshooting capabilities. We usage, please see the Micro	do not collect names,	
Content op provide accu addresses or other co or more information Privacy Statement.	irate and efficient troubl intact information.	eshooting capabilities. We usage, please see the Micro August E	do not collect names, osoft Online Services	>
Contraction of the second of t	irate and efficient troubl intact information. If on data collection and in integer *	eshooting capabilities. We usage, please see the Micro ≜upped R @ @ @	do not collect names, psoft Online Services administration appro-	>
C Trincolle Allow And	irate and efficient troubl intact information. If on data collection and in interval of the second s	eshooting capabilities. We usage, please see the Micro ▲ upmed ES € € €	do not collect names.	>
C 11/1/2014 400 AM - 420 AM (01)	irate and efficient troubl intact information.	eshooting capabilities. We usage, please see the Micro	do not collect names, pooft Online Services	
Correcter to provide accu addresses or other co or more information rivacy. Statement. Corrected accurate Save for later Corrected accurate Corrected accurate Co	and efficient troublent tr	eshooting capabilities. We usage, please see the Micro	do not collect names, psoft Online Services there interview again there interview again	
creater to provide accu addresses or other cc or more information rrivacy. Statement. Save for later C 1115014 480 AM - 400 AM DP- C 1115014 480 AM DP- C 1115014 AM DP	irate and efficient troubl ontact information.	eshooting capabilities. We usage, please see the Micro	do not collect names, psoft Online Services	
creater to provide accuration of the provide accurate to provide accurate the term of the construction of the constructio	Intract information.	eshooting capabilities. We usage, please see the Micro	do not collect names, pooft Online Services	
content to provide accuration of the pr	and efficient troublentact information.	eshooting capabilities. We usage, please see the Micro	do not collect names, pooft Online Services	
content to provide accuration of the pr	and efficient troublentate information.	eshooting capabilities. We usage, please see the Micro	do not collect names, pooft Online Services additional	

(ensure the the right workspace is selected)



Once the deployment succeeds, go to 'Service Map' by clicking on 'Go to resource' from the Notifications pane



- Find and add 'Network Performance Monitor'
- Find and add 'Service Map'
- d. You can also navigate to the resource (Service Map) by going to Log Analytics, selecting the workspace and clicking on 'workspace summary'



e. Your Solutions will then indicate they require further config, this is mainly the need for client setup and will change once it detects a client connected.

Home > ServiceMap(demobandwidthme	easurement)			
ServiceMap(demobandy	vidthmeasurement)			
	🛅 Delete			
Overview	Essentials 🔨			
Activity log	Resource group		Solution ServiceMap(demobandw	idthmeasurement)
Access control (IAM)	Status Type Active Microsoft-OperationsManageme			nagement/solutions
✗ Diagnose and solve problems	Location Workspace Name West Europe demobandwidthmeasurement			ment
Settings	Subscription name (change)		Management services Operations logs	
Locks				
😫 Automation script				
General	Summary			
🥏 OMS Workspace	Service Map	Solution Resources		
Properties		1 🐢		
★ Saved searches	- 25	ServiceMap(demobandwidthmeasurement)		
Workspace Data Sources				
Virtual machines				
Storage accounts logs				
Azure Activity log				
Solution Targeting (Preview)				

And that's it for the server-side setup. Now we need to configure some clients to provide data to the solution.

4.4 Client-Side Configuration

To send the data into our new solution, we need to install two client-side applications 'Microsoft Dependency Agent' and 'Microsoft Monitoring Agent'

The dependency agent collects the data we need and sends it to the Monitoring agent for transmission to Log analytics workspace. You have access to the ingested data from your Log analytics workspace in Azure.



Microsoft Dependency Agent install links for 64-bit Windows and Linux Machines:

https://aka.ms/dependencyagentwindows

https://aka.ms/dependencyagentlinux

More information on scripting this install can be found <u>here</u>.

- 1. To obtain the correct **Microsoft Monitoring Agent** you'll need to go through the Azure Portal.
- a. In the Azure Portal click on "All Services" then search for 'Log Analytics' and then click on it

Microsoft Azure				
Create a resource	All services LOG			
i≘ All services			Log Analytics	
	Activity log Keywords: logs	*	🧔 Log Analytics	*
- 🛧 FAVORITES	Can Monitor Keywords: logs	☆	Operation log (classic)	*
🖪 Dashboard				

b. Select your workspace, click on "Advanced Settings" from the workspace blade

Microsoft Azur	e	Report a bug
*	Home > Log Analytics > demobandwidthmeasurement	
resource	Log Analytics « 🖈 🗙	demobandwidthmeasurement
es	➡ Add ≡ Edit columns • • • • More	
	Filter by name	Overview
warehouses	NAME †↓	Activity log
smos DB	demobandwidthmeasurement	Access control (IAM)
achines		Tags
ancers		X Diagnose and solve problems
ccounts		SETTINGS
etworks		Locks
tive Directory		Automation script
		Advanced settings
		GENERAL
Center		🗳 Quick Start
agement + B		Workspace summary

c. Here we have both the install link for the Monitoring Agent we need, and also some key information to connect it to our Log analytics worksapce.

Microsoft Azure					
*	Home > Log Analytics > DemoBandwidthMeasurement > Advanced settings				
+ Create a resource	Advanced settings				
i≡ All services	🐌 Refresh 🛛 🗮 Analytics				
				Windows Servers	
★ FAVORITES	Connected Sources	Windows Servers	>	Attach any Windows server or client.	
🗔 Dashboard				0 WINDOWS COMPUTERS CONNECTED	
	🕅 Data 💦	A Linux Servers	>		
All resources	× ••••			Download Windows Agent (64 bit) Download Windows Agent (32 bit)	
Resource groups	Computer Groups	Azure Storage	>	You'll need the Workspace ID and Key to install the agent.	
🔇 App Services				WORKSPACE ID	
Function Apps		凚 System Center	>	22f280/	
🗟 SQL databases				PRIMARY KEY	
🥭 Azure Cosmos DB				14Ctem7 Regenerate	

- d. Download and install the appropriate Windows Agent (64 bit) and install it on the client/s you wish to monitor
- e. Also copy the Workspace ID and Primary Key.
- f. Once the monitoring agent is installed, a window will pop up. We require the middle option to connect to our Azure Log Analytics workspace. Select and click next.

ៅ Microsoft Monitoring Agent Setup	×
Agent Setup Options	
Specify setup options for this installation of Microsoft Monitoring Agent.	
Enable local collection of IntelliTrace logs (requires .NET Framework 3.5 or higher)	
This installs a PowerShell interface for gathering advanced application diagnostics data in local iTrace files.	
Connect the agent to Azure Log Analytics (OMS)	
Connects the agent to the Microsoft Azure Log Analytics (OMS) service and lets you to choose the workspace that the agent uses to register with. For more information, see https://www.microsoft.com/oms.	
Connect the agent to System Center Operations Manager	
This connects the agent to System Center Operations Manager and lets you specify the management group for which this agent will participate in monitoring.	
< Back Next > Cancel	

- g. Next, we'll be asked for our Workspace ID and Primary Key we copied from the Azure Portal above. Most customers will require the Azure Commercial instance. If the client uses a proxy to connect to the internet, then this need configuring by clicking the advanced button.
- h. Click next and select whether to use Windows Update for the agent (recommended) then next again.
- To check installation succeeded, open the control panel and select Microsoft Monitoring Agent. If successfully connected you should see a green tick in the status bar on the 'Azure Log Analytics' Tab.

June 20 Microsof	t Monito	ring Agent Properties				×
Operations	Manager	Azure Log Analytics (OMS)	Proxy Settings	Properties		
The Micros can add, e <u>connectino</u>	oft Monita dit, check compute	oring Agent can report to muli the status of, or remove wo rs directly to Log Analytics.	tiple Azure Log An kspaces from this	aalytics (OMS page. Learr) workspace more about	s. You t
Workspace	es:					
Work	Status			Agent Id		
			Add	. E	dit	Remove
			C	Ж	Cancel	Apply

j. And that's it! Sit back and wait for your client to talk to Log analytics workspace and ingest data which should normally be within 5-10 minutes.

4.5 Analyzing Data in Log Analytics

After about 5 minutes you should be able to see your machine is reporting into Log analytics by logging into your portal. You can do this in two ways.

a. Log into your Azure Portal at <u>https://portal.azure.com</u> click on 'All Resources' and click on your Log Analytics workspace, if you go to the 'Workspace Summary' you will notice that Service Map has been configured and collecting data

Microsoft Azure	9	Report a bu
*	Home > Log Analytics > demobandwidthmeasurement	
resource	Log Analytics « X X Microsoft	demobandwidthmeasuremer
es	♣ Add 📑 Edit columns ···· More	
	Filter by name	Overview
warehouses	NAME 14	Activity log
smos DB	demobandwidthmeasurement	Access control (IAM)
achines		🖉 Tags
ancers		X Diagnose and solve problems
accounts		SETTINGS
etworks		Locks
tive Directory		🛓 Automation script
		Advanced settings
		GENERAL
Center		📣 Quick Start
hagement + B		E Workspace summary
Microsoft Azure		Report a bug
«	Dashboard > Log Analytics > roshanp-FT-PN	> Overview
esource	Overview	
đ	C) Refresh + Add = Analytics	
s		
	Last 24 hours	
ces	ser	×
groups	Sanico Man	
ces	Зегисе мар	*
bases	1 3 Machines reporting All-time machines re	porting
warehouses	(Last 30 min)	por unity
mos DB	5 🔲 0 😥	
ichines		

- b. Then click on 'Analytics' at the top of the page which opens up in a new tab. If you click on Service Map tab it will show you a summary of network traffic information collected. We will use Analytics so you can run queries against the workspace to extract specific information we need for Bandwidth.
- c. There are a couple of things to take note there if you are using Log analytics for the first time.

Notice you are now in Log analytics playground, you can use this console to run log analytics queries and review data that is stored in the workspace. You also have the ability to specify time range or save queries for frequent use in 'Query Explorer'

Dashboard > Log Analytics > roshanp-	FT-PM > Overview > Logs	
Logs roshanp-ft-pm		\$ X
New Query 1 +		🛄 Help 🔅 Settings 🗔 Query explorer
roshanp-ft-pm 프	Run Time range: Last 24 hours	🔄 Save 👁 Copy link 📑 Export 🕂 New alert rule 🖈 Pin
Schema Filter (preview) Filter by name or type □ □ □ Collapse all Active • Di coshanp-ft-pm ★	Type your query here	
 LogManagement NetworkMonitoring Office365 ServiceMap WireData2 Custom Logs Æ Functions Favorite workspaces monthshare 	Select queries Heartbeat Performance Usage Chart the number of reporting computers each hour Heartbeat summarize dcount(Computer/P) by bin(TimeGenerated, 1h) render timechart List all computer heartbeats from the last hour Heartbeat where TimeGenerated > ago(1h)	Current Control Contr

- d. Run a simple query like the following, replace 'DESKTOP' with your computer name. Notice the time range by default is set to Last 24 hours.
- VMConnection | where Computer contains "DESKTOP" | where ProcessName contains "outlook" 🔚 Save 📀 Copy link 📑 Export 🕂 New alert rule Run (Time range: Last hour VMConnection where Computer contains "roshwork" where ProcessName contains "outlook" ⊘ 00:00:05.668 🖺 4' Completed. Showing results from the last hour. TABLE ,I CHART Columns ~ Display time (UTC+ Drag a column header and drop it here to group by that column TimeGenerated [UTC] ∇ Computer ∇ Direction √ ProcessName √ Sourcelp ∇ DestinationIp ♥ DestinationPort √ Remotelp 2018-11-14T08:07:12.934 ROSHWORK-DXB outbound OUTLOOK 192.168.1.14 52.97.134.6 443 52.97.134.6 5 tcp OUTLOOK 52.114.32.7 2018-11-14T08:07:12.934 ROSHWORK-DXB outbound 192.168.1.14 52.114.32.7 443 tcp 5 2018-11-14T08:07:12.934 ROSHWORK-DXB outbound OUTLOOK 192.168.1.14 40.100.174.34 443 tcp 40.100.174.34 2018-11-14T08:07:12.934 ROSHWORK-DXB outbound OUTLOOK 40.100.175.146 443 40.100.175.146 192.168.1.14 tcp

If the query runs successfully you should see the results showing the data table and records. In the example above we are also setting the time range for the last one hour.

e. Service Map has the following records we can search from, you can see this in the Schema on the left hand side, expand the Service Map, VMConnection table

Logs roshanp-ft-pm		
New Query 1* +		
roshanp-ft-pm	-0	▶ Run Time range: Last hour
Schema Filter (preview)	«	VMConnection where Computer contains "roshwork"
Filter by name or type	Q	where processwame contains outlook
↓ = Colla	pse all	
Active	^	
🕶 🔟 roshanp-ft-pm	*	
LogManagement		
NetworkMonitoring		Completed. Showing results from the last hour.
 Office265 		TABLE III CHART Columns ~
- Concesos		Drag a column header and drop it here to group by that
 Serviceinap VMBoundPort 		
VMConnection		TimeGenerated [UTC] \vee Computer \vee
t AgentId		> 2018-11-14T08:07:12.934 ROSHWORK-DXB
# BytesReceived		2018-11-14T08-07-12 934 ROSHWORK-DXB
# BytesSent		
t Computer		> 2018-11-14T08:07:12.934 ROSHWORK-DXB
t ConnectionId		> 2018-11-14T08:07:12.934 ROSHWORK-DXB
t Description		> 2018-11-14T08:07:12.934 ROSHWORK-DXB
t DestinationIp		
# DestinationPort		> 2018-11-14108:08:12.934 KOSHWORK-DXB
 t Direction t FirstReportedDateTime 		> 2018-11-14T08:08:12.934 ROSHWORK-DXB
<i>t</i> IndicatorThreatType		> 2018-11-14T08:08:12.934 ROSHWORK-DXB
t IsActive		
t LastReportedDateTime		> 2018-11-14108:08:12.934 KOSHWORK-DXB

Service Map has this information which is aggregated in 1 minute intervals. For example, a single TCP session will have the bytes sent/received/total for the previous 1 minute logged as an entry. This enables us to query the data for information such as the following examples:

- Bandwidth used for a particular process or set of processes over a set period of time
- Bandwidth used by the machine over a set period of time
- Bandwidth used in connections to a specific port
- Bandwidth used to a specific IP address or range of addresses
- Number of TCP connections a process has open at any one time
- IP geolocation of the endpoints connected to

Essentially, if we know the process name or the destination IP address we can easily monitor the endpoints used for any of the fields above.

From an Office 365 perspective this allows us to collect very accurate data for bandwidth usage for pilot users to gain an accurate figure for planning for a wider rollout.

For example, you may wish to see the bandwidth usage of the Outlook client over the course of 24 hours to see how much bandwidth your Exchange connectivity may require.

To do this we query Service Map for a specific PC (or multiple if required) in this case a machine called 'DESKTOP' where the process name contains 'Outlook', where the TCP session start time was in the last day and output the total bytes used in each sample of 1 minute (TimeGenerated).

Add the above to the query then hit 'Run'. You need to ensure the timeframe for the query is set correctly at the top, in this case as we're specifying one day, it needs to be at least 'Last 24 Hours' which allows us to search through the data for the last 24 hours or you can specify the time range in the query itself as shown below

let startTime=datetime(2018-11-14T00:01:00);								
let endTime=datetime(2018-11-14T11:59:59);								
VMConnection								
where Computer contains "roshwork"								
where ProcessNam	ne contains "outlool	k"						
where TimeGenera	ted > startTime and	d TimeGenerated	< endTime					
Run Time range: Set in	query	📙 Save 📿	Copy link 🗧	Export 🕂 New al	ert rule 🔗 Pin			
<pre>et startTime=datetime(2018-11-14T00:01:00); et endTime=datetime(2018-11-14T11:59:59); /MConnection where Computer contains "roshwork" where ProcessName contains "outlook" where TimeGenerated > startTime and TimeGenerated < endTime</pre>								
where TimeGenerated > startT								
where TimeGenerated > startT:				♂ 00:00:01.399 E	립 1,699 records			
Completed				් 00:00:01.399 ව් Display time	립 1,699 records e (UTC+00:00) ~			
where TimeGenerated > startT: Completed TABLE , II CHART Columns ~ Drag a column header and drop it here to g	group by that column			් 00:00:01.399 [Display time] 1,699 records e (UTC+00:00) 〜			
Where TimeGenerated > startT: Completed TABLE , CHART Columns ~ Drag a column header and drop it here to g TimeGenerated [UTC] \(\nabla \) Compute	group by that column uter 7 Direction 7	···· 7 ProcessName →	Sourcelp 🗸	⊘ 00:00:01.399 E Display time DestinationIp ▽	〕 1,699 records e (UTC+00:00) 〜 DestinationPort			
where TimeGenerated > startT: Completed TABLE IICHART Columns > Drag a column header and drop it here to g TimeGenerated [UTC] V Comput 2018-11-14T08:22:12.936 ROSHW	group by that column uter V Direction S VORK-DXB outbound	 7 ProcessName OUTLOOK 	Sourcelp 7 192.168.1.14	⑦ 00:00:01.399 E Display time DestinationIp 7 52.97.131.130	 1,699 records (UTC+00:00) ~ DestinationPort 443 			
where TimeGenerated > startT: Completed TABLE ,IICHART Columns > Drag a column header and drop it here to g TimeGenerated [UTC] Compu 2018-11-14T08:22:12.936 ROSHW 2018-11-14T08:22:12.936	group by that column uter V Direction N VORK-DXB outbound VORK-DXB outbound	 ProcessName OUTLOOK OUTLOOK 	Sourcelp 7 192.168.1.14 192.168.1.14	Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Control of the second system Image: Contro of the second system Image: Control of the second	 1,699 records (UTC+00:00) ~ DestinationPort 443 443 			
where TimeGenerated > startT: Completed TABLE IIICHART Columns > Drag a column header and drop it here to g TimeGenerated [UTC] Compu 2018-11-14T08:22:12.936 ROSHW 2018-11-14T08:22:12.936 ROSHW 2018-11-14T08:22:12.936 ROSHW	group by that column uter V Direction S VORK-DXB outbound VORK-DXB outbound VORK-DXB outbound	7 ProcessName ▼ OUTLOOK OUTLOOK OUTLOOK OUTLOOK	Sourcelp 20192.168.1.14 192.168.1.14	 O0:00:01.399 Display time Destination p ∇ 52.97.131.130 40.103.45.182 52.97.134.6 	 1,699 records (UTC+00:00) ~ DestinationPort 443 443 443 			

le le VM

If the query worked, you'll see a table of data output. We can then turn this into a graph within Analytics by clicking 'Chart' then when rendered, click 'Stacked Column' and change to Line or any other graph you prefer.

In the graph produced, we can clearly see the bytes used by the Outlook process for the time range specified on this machine. This allows us to see the peaks and normal usage and thus allow us to plan for bandwidth across all our clients.



If we just want to find out the key points, i.e. 95th percentile of sent/received Kbps and Total sent/received MB over a time period, we can run the following query:

```
let startTime=datetime(2018-11-14T00:01:00);
let endTime=datetime(2018-11-14T11:59:59);
VMConnection
| where Computer contains "desktop"
| where ProcessName contains "outlook"
| where TimeGenerated > startTime and TimeGenerated < endTime
                                         (sum(BytesSent)/1024*8/60),
     summarize
                     SentKbps
                                                                        ReceivedKbps
                                  =
                                                                                          =
(sum(BytesReceived)/1024*8/60) by bin(TimeGenerated, 1m), Computer
summarize Percentile95SentKbps = round(percentile(SentKbps, 95),2), Percentile95ReceivedKbps
= round(percentile(ReceivedKbps, 95),2) by Computer
| join (
  VMConnection
  | where Computer contains "desktop"
  | where ProcessName contains "outlook"
  | where TimeGenerated > startTime and TimeGenerated < endTime
      summarize
                    TotalSentMB
                                         sum(BytesSent)/1024/1024,
                                                                      TotalReceivedMB
                                    =
                                                                                           =
sum(BytesReceived)/1024/1024 by Computer
) on Computer
              Computer,
    project
                           Percentile95SentKbps,
                                                   Percentile95ReceivedKbps,
                                                                               TotalSentMB,
TotalReceivedMB
```

С	ompleted ≣TABLE ,, CHART │ Columns ~					O:00:01.974	曽 1 records
D	rag a column header and drop it here to g	roup by tha	t column				
	Computer 🖓 Percentile95SentKb	ps 🖓	Percentile95ReceivedKbps	\bigtriangledown	TotalSentMB 🛛 🗸	TotalReceivedMB 🛛 🖓	
~	ROSHWORK-DXB 78		67		21	34	
	Computer	ROSHWC	ORK-DXB				
	Percentile95SentKbps	78					
	Percentile95ReceivedKbps	67					
	TotalSentMB	21					
	TotalReceivedMB	34					

This method can be used for any process running on the machine and will work regardless of whether a proxy is used or not because we're monitoring the process, not the IP address of the endpoint (which will always be the proxy IP if one is used for all non-internal traffic).

4.6 Example Queries

The data can be analyzed to a limited extent within the Analytics portal itself. For more comprehensive analysis we can use Power BI which is covered in the next session. Regardless, the Power BI query can be obtained within Azure Analytics via the example queries below.

*Time is defined in UTC by default, you can change this by going to the 'Settings' tab

田 Help 🐯 Settings	Query explorer
🔚 Save 🐵 Copy link 📑 Export 🕂 New alert rule 📌 Pin	Filter by name or path

*Full Query = Give me all the data and I will perform my own query to filter it

*Key Points Query = Filter the data and display only the key points, for example SentKbps, ReceivedKbps, Total Sent and Received in MB. For Sent/Received Kbps the query is set to use 95th percentile function you can modify (increase/decrease) this as per your requirement.

EXO Full Query (Exchange Online)

let startTime=datetime(2020-01-03T00:01:00); let endTime=datetime(2020-01-07T23:59:59); VMConnection | where ProcessName contains "outlook" | where TimeGenerated > startTime and TimeGenerated < endTime</pre>

EXO Key Points Query

let startTime=datetime(2020-01-03T00:01:00); let endTime=datetime(2020-01-07T23:59:59); VMConnection | where ProcessName contains "outlook"

| where TimeGenerated > startTime and TimeGenerated < endTime | summarize SentKbps = (sum(BytesSent)/1024*8/60), ReceivedKbps = (sum(BytesReceived)/1024*8/60) by bin(TimeGenerated, 1m), Computer summarize Percentile95SentKbps = round(percentile(SentKbps, 95),2), Percentile95ReceivedKbps = round(percentile(ReceivedKbps, 95),2) by Computer | join (VMConnection | where ProcessName contains "outlook" | where TimeGenerated > startTime and TimeGenerated < endTime TotalSentMB sum(BytesSent)/1024/1024, TotalReceivedMB summarize = sum(BytesReceived)/1024/1024 by Computer) on Computer project Computer, Percentile95SentKbps, Percentile95ReceivedKbps, TotalSentMB, TotalReceivedMB

If you need filter for traffic from a specific computer, you can always add a filter like:

| where Computer contains "XXXX"

The query logic is the same for Skype for Business and Teams too but just replaced 'outlook' with 'lync' or 'teams'

The query logic for **SPO (Sharepoint Online)** and **OD4B (OneDrive for Business)** is as follows since it is based on destination IP ranges:

SPO/OD4B Full Query (Sharepoint Online / OneDrive for Business)

let sta	rtTime=datetime(2020-01-0)2T01:	00:00);			
let en	dTime=datetime(2020-01-0	7T23:3	30:00);			
VMCc	onnection					
wher	e Computer contains "XXXX	(II				
wher	e TimeGenerated > startTim	ne and	TimeGenerated < endTime			
wh	ere (parse_ipv4(Destination	nlp)	>= parse_ipv4('13.107.136.0)) and	parse_ipv4(DestinationIp)	<=
parse_	_ipv4('13.107.139.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('40.108.128.0')	and	parse_ipv4(DestinationIp)	<=
parse_	_ipv4('40.108.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('52.104.0.0')	and	parse_ipv4(Destinationlp)	<=
parse	_ipv4('52.107.255.255'))					
or (parse_ipv4(DestinationIp)	>=	parse_ipv4('104.146.128.0')	and	parse_ipv4(DestinationIp)	<=
parse_	_ipv4('104.146.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('150.171.40.0')	and	parse_ipv4(Destinationlp)	<=
parse_	_ipv4('150.171.43.255'))					

SPO/OD4B Key Points Query

```
let startTime=datetime(2020-01-02T01:00:00);
let endTime=datetime(2020-01-07T23:30:00);
VMConnection
| where Computer contains "XXXX"
| where TimeGenerated > startTime and TimeGenerated < endTime
| where (parse_ipv4(DestinationIp) >= parse_ipv4('13.107.136.0') and parse_ipv4(DestinationIp) <=
parse_ipv4('13.107.139.255'))
```

(parse_ipv4(DestinationIp) >= parse_ipv4('40.108.128.0') and parse_ipv4(Destinationlp) < = or parse_ipv4('40.108.255.255')) (parse_ipv4(Destinationlp) parse_ipv4('52.104.0.0') parse_ipv4(DestinationIp) or >= and <= parse_ipv4('52.107.255.255')) or (parse_ipv4(DestinationIp) parse_ipv4('104.146.128.0') parse_ipv4(DestinationIp) >= and < = parse_ipv4('104.146.255.255')) or (parse ipv4(Destinationlp) parse ipv4('150.171.40.0') and parse ipv4(DestinationIp) >= < = parse ipv4('150.171.43.255')) | summarize SentKbps = (sum(BytesSent)/1024*8/60), ReceivedKbps = (sum(BytesReceived)/1024*8/60) by bin(TimeGenerated, 1m), Computer summarize Percentile95SentKbps = round(percentile(SentKbps, 95),2), Percentile95ReceivedKbps = round(percentile(ReceivedKbps, 95),2) by Computer | join (VMConnection | where Computer contains "XXXX" | where TimeGenerated > startTime and TimeGenerated < endTime where (parse_ipv4(DestinationIp) >= parse_ipv4('13.107.136.0') and parse_ipv4(DestinationIp) < = parse ipv4('13.107.139.255')) or (parse_ipv4(DestinationIp) parse_ipv4('40.108.128.0') and parse_ipv4(DestinationIp) >= <= parse_ipv4('40.108.255.255')) (parse ipv4(Destinationlp) parse_ipv4('52.104.0.0') parse_ipv4(DestinationIp) or >= and <= parse_ipv4('52.107.255.255')) or (parse_ipv4(DestinationIp) >= parse_ipv4('104.146.128.0') and parse_ipv4(DestinationIp) <= parse_ipv4('104.146.255.255')) or (parse_ipv4(Destinationlp) parse_ipv4('150.171.40.0') parse_ipv4(DestinationIp) >= and < = parse_ipv4('150.171.43.255')) summarize TotalSentMB = sum(BytesSent)/1024/1024, TotalReceivedMB = sum(BytesReceived)/1024/1024 by Computer) on Computer project Computer, Percentile95SentKbps, Percentile95ReceivedKbps, TotalSentMB, TotalReceivedMB

Please note that the following filter for computer name is optional, comment it or remove it if you want to view the results for all computers connected to your workspace.

Computer contains "XXXX"

Only for SPO/OD4B the highlighted section in orange may need to be replaced if the IP ranges used for SPO/OD4B changes, the ranges are published in https://aka.ms/o365ip

You can use the Powershell script Generate-LAQuery-v3.ps1 in <u>Github</u> to generate the query with up to date IP ranges for the highlighted orange section only (copy/paste the output from Generate-LAQuery-v3.ps1 into your log analytics query). Syntax examples for Generate-LAQuery-v3.ps1 are available in the comments section of the file.



Teams Full Query (Microsoft Teams, including UDP for media traffic)

let startTime=datetime(2020-01-03T00:01:00); let endTime=datetime(2020-01-07T23:59:59); VMConnection | where ProcessName contains "teams" | where TimeGenerated > startTime and TimeGenerated < endTime</pre>

Teams Key Points Query

let startTime=datetime(2020-01-03T00:01:00); let endTime=datetime(2020-01-07T23:59:59); VMConnection where ProcessName contains "teams" | where TimeGenerated > startTime and TimeGenerated < endTime | summarize SentKbps = (sum(BytesSent)/1024*8/60), ReceivedKbps = (sum(BytesReceived)/1024*8/60) by bin(TimeGenerated, 1m), Computer summarize Percentile95SentKbps = round(percentile(SentKbps, 95),2), Percentile95ReceivedKbps = round(percentile(ReceivedKbps, 95),2) by Computer l join (VMConnection | where ProcessName contains "teams" | where TimeGenerated > startTime and TimeGenerated < endTime TotalSentMB summarize = sum(BytesSent)/1024/1024, **TotalReceivedMB** _ sum(BytesReceived)/1024/1024 by Computer) on Computer project Computer, Percentile95SentKbps, Percentile95ReceivedKbps, TotalSentMB, TotalReceivedMB

Query for 'Optimize' category endpoints

This query is useful when you would like to have a consolidated view of network bandwidth usage for all endpoints (IP's) that belong to the Optimize category. Refer <u>here</u> for Office 365 endpoint categories

```
let startTime=datetime(2020-01-02T01:00:00);
let endTime=datetime(2020-01-07T23:30:00);
VMConnection
| where Computer contains "XXXX"
| where TimeGenerated > startTime and TimeGenerated < endTime
where (parse_ipv4(DestinationIp) >= parse_ipv4('13.107.6.152') and parse_ipv4(DestinationIp)
                                                                                                   <=
parse_ipv4('13.107.6.153'))
or (parse_ipv4(Destinationlp)
                                >= parse_ipv4('13.107.18.10')
                                                                        parse_ipv4(DestinationIp)
                                                                 and
                                                                                                   < =
parse ipv4('13.107.18.11'))
or (parse_ipv4(DestinationIp)
                                      parse_ipv4('13.107.128.0')
                                                                 and
                                                                        parse_ipv4(DestinationIp)
                                >=
                                                                                                   < =
parse_ipv4('13.107.131.255'))
or (parse_ipv4(DestinationIp)
                                >=
                                      parse_ipv4('23.103.160.0')
                                                                 and
                                                                        parse_ipv4(DestinationIp)
                                                                                                   < =
parse_ipv4('23.103.175.255'))
or (parse_ipv4(DestinationIp)
                                        parse_ipv4('40.96.0.0')
                                 >=
                                                                and
                                                                       parse_ipv4(Destinationlp)
                                                                                                   <=
parse_ipv4('40.103.255.255'))
```

or (parse_ipv4(Destinationlp)	>=	parse_ipv4('40.104.0.0')	and	parse_ipv4(Destinationlp)	<=
parse_ipv4('40.105.255.255'))					
or (parse_ipv4(DestinationIp)	>=	parse_ipv4('52.96.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ipv4('52.99.255.255'))					
or (parse_ipv4(DestinationIp) ==	parse_	ipv4('131.253.33.215'))			
or (parse_ipv4(Destinationlp)	>=	parse_ipv4('132.245.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ipv4('132.245.255.255'))					
or (parse_ipv4(DestinationIp)	>=	parse_ipv4('150.171.32.0')	and	parse_ipv4(DestinationIp)	<=
parse_ipv4('150.171.35.255'))					
or (parse_ipv4(DestinationIp)	>=	parse_ipv4('191.234.140.0')	and	parse_ipv4(DestinationIp)	<=
parse_ipv4('191.234.143.255'))					
or (parse_ipv4(Destinationlp) ==)	oarse_	ipv4('204.79.197.215'))			
or (parse_ipv4(Destinationlp)	>=	parse_ipv4('13.107.64.0')	and	parse_ipv4(DestinationIp)	<=
parse ipv4('13.107.127.255'))				1 -1	
or (parse ipv4(Destinationlp)	>=	parse ipv4('52,112,0,0')	and	parse ipv4(DestinationIp)	<=
parse ipv4('52 115 255 255'))		h			
or (parse ipv4(DestinationIp)	>=	parse ipv4('13,107,136,0')	and	parse ipv4(DestinationIp)	< =
parse $inv4('13\ 107\ 139\ 255'))$		pulse_ipvi(10.101.100.07)	ana		
or $(\text{parse inv}/(\text{Destination}n))$	\-	narse inv//(1/10.108.128.0)	and	parse inv/(DestinationIn)	<u> </u>
parso ipv4('40, 108, 255, 255'))	/ -	parse_ipv+(+0.100.120.0)	and	parse_ipv+(Destinationip)	~-
or (parso inv/(DostinationIn)	\ -	$p_{2} = p_{1} (1 + 1) (1 + 1$	and	parso inv/(DostinationIn)	<
$(parse_ipv4(Destinationp))$	/-	parse_ipv4(52.104.0.0)	anu	parse_ipv4(Destinationip)	~-
parse_ipv4(52.107.255.255))		norra inv///10/ 1/6 100 01	and	narea in ((Destination))	
or (parse_Ipv4(DestinationIp)	>=	parse_ipv4(104.146.126.0)	and	parse_ipv4(Destinationip)	< =
parse_Ipv4(104.146.255.255))					
or (parse_Ipv4(DestinationIp)	>=	parse_Ipv4(*150.171.40.0*)	and	parse_Ipv4(DestinationIp)	<=
parse_Ipv4(150.171.43.255))			,		
summarize SentKbps = (sum(B)	ytesSe	nt)/1024*8/60), ReceivedKbj	ps = (su	im(BytesReceived)/1024*8/60) by
bin(TimeGenerated, Tm), Comput	er				
summarize Percentile95SentK	bps =	 round(percentile(SentKbp 	os, 95),2	2), Percentile95ReceivedKbp	s =
round(percentile(ReceivedKbps, 9	5),2) b	y Computer			
join (
VMConnection					
where Computer contains "XX	XX"				
where TimeGenerated > start	Time a	nd TimeGenerated < endTin	ne		
where (parse_ipv4(Destination	nlp)	>= parse_ipv4('13.107.6.15	2') and	a parse_ipv4(DestinationIp)	<=
parse_ipv4('13.107.6.153'))					
or (parse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.18.10')	and	parse_ipv4(DestinationIp)	<=
parse_ipv4('13.107.18.11'))					
or (parco inv//(DoctinationIn)					
or (parse_ipv4(Destinationip)	>=	parse_ipv4('13.107.128.0')	and	parse_ipv4(Destinationlp)	<=
parse_ipv4('13.107.131.255'))	>=	parse_ipv4('13.107.128.0')	and	parse_ipv4(Destinationlp)	<=
parse_ipv4('13.107.131.255')) or (parse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0')	and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<=
parse_ipv4('13.107.131.255')) or (parse_ipv4(DestinationIp) parse_ipv4('23.103.175.255'))	>= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0')	and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <=
parse_ipv4(/destinationip) parse_ipv4('13.107.131.255')) or (parse_ipv4(DestinationIp) parse_ipv4('23.103.175.255')) or (parse ipv4(DestinationIp)	>= >= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0')	and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	< = < = < =
parse_ipv4('13.107.131.255')) or (parse_ipv4('23.103.175.255')) or (parse_ipv4('23.103.175.255')) or (parse_ipv4('40.103.255.255'))	> = > = > =	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0')	and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <= <=
parse_ipv4('13.107.131.255')) or (parse_ipv4('DestinationIp) parse_ipv4('23.103.175.255')) or (parse_ipv4('240.103.255.255')) parse_ipv4('40.103.255.255')) or (parse_ipv4('DestinationIp)	>= >= >= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0')	and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <= <= <=
parse_ipv4('13.107.131.255')) or (parse_ipv4('DestinationIp) parse_ipv4('23.103.175.255')) or (parse_ipv4('23.103.175.255')) or (parse_ipv4('40.103.255.255')) or (parse_ipv4('40.105.255.255')) parse_ipv4('40.105.255.255'))	>= >= >= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0')	and and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <= <= <=
parse_ipv4('13.107.131.255')) or (parse_ipv4(DestinationIp) parse_ipv4('23.103.175.255')) or (parse_ipv4(DestinationIp) parse_ipv4('40.103.255.255')) or (parse_ipv4(DestinationIp) parse_ipv4('40.105.255.255')) or (parse_ipv4(DestinationIp)	>= >= >= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0')	and and and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <= <= <=
parse_ipv4('13.107.131.255')) or (parse_ipv4('DestinationIp) parse_ipv4('23.103.175.255')) or (parse_ipv4('23.103.175.255')) or (parse_ipv4('DestinationIp) parse_ipv4('40.103.255.255')) or (parse_ipv4('DestinationIp) parse_ipv4('23.99.255.255')) or (parse_ipv4('DestinationIp) parse_ipv4('52.99.255.255'))	>= >= >= >= >=	<pre>parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0') parse_ipv4('52.96.0.0')</pre>	and and and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	< = < = < = < =
parse_ipv4('13.107.131.255')) or (parse_ipv4('DestinationIp) parse_ipv4('23.103.175.255')) or (parse_ipv4(DestinationIp) parse_ipv4('40.103.255.255')) or (parse_ipv4(DestinationIp) parse_ipv4('40.105.255.255')) or (parse_ipv4(DestinationIp) parse_ipv4('52.99.255.255')) or (parse_ipv4(DestinationIp)	>= >= >= >= >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0') parse_ipv4('52.96.0.0')	and and and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	<= <= <= <=
parse_ipv4('Destinationip) parse_ipv4('13.107.131.255')) or (parse_ipv4(Destinationlp) parse_ipv4('23.103.175.255')) or (parse_ipv4(Destinationlp) parse_ipv4('40.103.255.255')) or (parse_ipv4(Destinationlp) parse_ipv4('52.99.255.255')) or (parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) == p or (parse_ipv4(Destinationlp) == p	>= >= >= >= >= parse_	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0') parse_ipv4('52.96.0.0') ipv4('131.253.33.215')) parse_ipv4('132.245.0.0')	and and and and and	parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp) parse_ipv4(Destinationlp)	< = < = < = < =
or (parse_ipv4(bestinationip) parse_ipv4('13.107.131.255')) or (parse_ipv4(Destinationlp) parse_ipv4('23.103.175.255')) or (parse_ipv4(Destinationlp) parse_ipv4('40.103.255.255')) or (parse_ipv4(Destinationlp) parse_ipv4('40.105.255.255')) or (parse_ipv4(Destinationlp) parse_ipv4('132.245.255')) or (parse_ipv4(Destinationlp) == p	>= >= >= >= >= parse_ >=	parse_ipv4('13.107.128.0') parse_ipv4('23.103.160.0') parse_ipv4('40.96.0.0') parse_ipv4('40.104.0.0') parse_ipv4('52.96.0.0') ipv4('131.253.33.215')) parse_ipv4('132.245.0.0')	and and and and and and	parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)parse_ipv4(Destinationlp)	<= <= <= <=

or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('150.171.32.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('150.171.35.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('191.234.140.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('191.234.143.255'))					
or (p	parse_ipv4(DestinationIp) ==	parse_	ipv4('204.79.197.215'))			
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.64.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('13.107.127.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('52.112.0.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('52.115.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.136.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('13.107.139.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('40.108.128.0')	and	parse_ipv4(DestinationIp)	<=
pars	e_ipv4('40.108.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('52.104.0.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('52.107.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('104.146.128.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('104.146.255.255'))					
or	(parse_ipv4(DestinationIp)	>=	parse_ipv4('150.171.40.0')	and	parse_ipv4(Destinationlp)	<=
pars	e_ipv4('150.171.43.255'))					
sur	mmarize TotalSentMB = sum	(Bytes	Sent)/1024/1024, TotalReceiv	vedMB =	= sum(BytesReceived)/1024/	1024
by C	Computer					
) on	Computer					
pro	oject Computer, Percentile95S	entKb	ps, Percentile95ReceivedKbp	s, Totals	SentMB, TotalReceivedMB	

Please note that the following filter for computer name is optional, comment it or remove it if you want to view the results for all computers connected to your workspace.

Computer contains "XXXX"

The highlighted section in orange may need to be replaced if the IP ranges used for Optimize category changes, the ranges are published in https://aka.ms/o365ip

You can use the Powershell script Generate-LAQuery-optimize-category-v3.ps1 in <u>Github</u> to generate the query with up to date IP ranges for the highlighted orange section only (copy/paste the output from Generate-LAQuery-optimize-category-v3.ps1 into your log analytics query). Syntax examples for Generate-LAQuery-optimize-category-v3.ps1 are available in the comments section of the file.



Query for LinksLive (TCP Connections) per Process

This query is useful when you would like to measure the number of TCP connections that were used by a specific process during the defined time period. The query is set to use 95th percentile function you can modify (increase/decrease) this as per your requirement.

let startTime=datetime(2019-12-01T00:01:00); let endTime=datetime(2019-12-23T23:59:00); VMConnection | where TimeGenerated > startTime and TimeGenerated < endTime | where Direction == "outbound" | where Protocol == "tcp" | where ProcessName == "OUTLOOK" | summarize sum(LinksLive) by TimeGenerated, Computer | summarize percentile(sum_LinksLive, 95) by Computer

Query for LinksLive (TCP Connections) for Optimize category endpoints

This query is useful when you would like to measure the number of TCP connections that were used by any process connecting to an IP endpoint part of 'Optimize' category during the defined time period. The query is set to use 95th percentile function you can modify (increase/decrease) this as per your requirement.

let startT	Time=datetime(2019-12-0	1T00:(01:00);			
let endTi	ime=datetime(2019-12-23	3T23:5	9:00);			
VMConn	nection					
where 1	TimeGenerated > startTim	e and	TimeGenerated < endTime			
where	e (parse_ipv4(Destination	nlp) :	>= parse_ipv4('13.107.6.15	2') and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('13.107.6.153'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.18.10')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('13.107.18.11'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.128.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('13.107.131.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('23.103.160.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('23.103.175.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('40.96.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ip	v4('40.103.255.255'))					
or (pa	arse_ipv4(Destinationlp)	>=	parse_ipv4('40.104.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ip	v4('40.105.255.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('52.96.0.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('52.99.255.255'))					
or (parse	e_ipv4(Destinationlp) == p	oarse_i	pv4('131.253.33.215'))			
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('132.245.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ip	v4('132.245.255.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('150.171.32.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('150.171.35.255'))					
or (pa	rse_ipv4(DestinationIp)	>=	parse_ipv4('191.234.140.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('191.234.143.255'))					
or (parse	e_ipv4(Destinationlp) == p	oarse_i	pv4('204.79.197.215'))			
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.64.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('13.107.127.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('52.112.0.0')	and	parse_ipv4(DestinationIp)	<=
parse_ip	v4('52.115.255.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('13.107.136.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('13.107.139.255'))					
or (pa	arse_ipv4(DestinationIp)	>=	parse_ipv4('40.108.128.0')	and	parse_ipv4(Destinationlp)	<=
parse_ip	v4('40.108.255.255'))					

or	(parse_ipv4(Destinationlp)	>=	parse_ipv4('52.104.0.0')	and	parse_ipv4(Destinationlp)	<=
parse	e_ipv4('52.107.255.255'))					
or	(parse_ipv4(Destinationlp)	>=	parse_ipv4('104.146.128.0')	and	parse_ipv4(DestinationIp)	<=
parse	e_ipv4('104.146.255.255'))					
or	(parse_ipv4(Destinationlp)	>=	parse_ipv4('150.171.40.0')	and	parse_ipv4(Destinationlp)	<=
parse	e_ipv4('150.171.43.255'))					
sum	nmarize sum(LinksLive) by Tin	neGen	erated, Computer			
summarize percentile(sum_LinksLive, 95) by Computer						

The highlighted section in orange may need to be replaced if the IP ranges used for Optimize category changes, the ranges are published in <u>https://aka.ms/o365ip</u>

You can use the Powershell script Generate-LAQuery-optimize-category-v3.ps1 in <u>Github</u> to generate the query with up to date IP ranges for the highlighted orange section only (copy/paste the output from Generate-LAQuery-optimize-category-v3.ps1 into your log analytics query). Syntax examples for Generate-LAQuery-optimize-category-v3.ps1 are available in the comments section of the file.

```
PS C:\temp> .\Generate-LAQuery-optimize-category-v3.ps1
cmdlet Generate-LAQuery-optimize-category-v3.ps1 at command pipeline position 1
Supply values for the following parameters:
Category: optimize
startdate: 2019-12-01T09:00
enddate: 2019-12-23T09:00
Log Analytics query written to 'C:\Users\meehomp\AppData\Local\Temp\LogAnalyticsquery_optimize_25-12-2019_15-48.txt'
PS C:\temp> _
```

4.7 Adding graphs to an Azure Dashboard

With each of the above queries, when you create a graph to show the information, you have the option to pin the graph to an Azure dashboard

Once the table is displayed, click 'Chart' then select the view you wish. Once the graph is displayed, simply click on the pin icon in the top right-hand corner of the graph



You can add multiple graphs to create a dashboard to show the data you need to view as soon as you log into Azure. These graphs can easily be refreshed to keep them current without having to run the query in Azure Analytics again.

Bandwidth Measurement \checkmark + New dashboard \clubsuit Upload \bigstar	townload ∥ Edit Q Unshare ∥ Fullscreen 🗗 Clone ij Delete		
		Non-state Non-state 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1 20 1 20 1	Окловска Расказа таки, в таки и кака рака на кака в ма у таки, в на кака рака еко в ма еко в ма
Outlook process the connection count ones as soons the count of the co	Machine Bandwisth: Usage		

4.8 Building a Dashboard in Power BI

Whilst Azure Analytics provides some great features to quickly analyse the data, it does have some limitations as it is not intended for extensive analysis. Firstly the number of rows returned in a query is limited to 10000 which may cause issues with larger sample sets.

Also, the graph options are fairly limited so may not contain the type you require.

Thankfully the Analytics portal makes it easy to export the data for analysis elsewhere. Once you enter a query there is an option to export the data to CSV for loading into Microsoft Excel, or it will re-write the query into a Power BI ready version.

Here we'll walk through the steps to create a Power BI dashboard and use the Outlook process as an example.

1. Install Power BI Desktop

Firstly, you'll need to install Power BI desktop from <u>here</u>. Power BI desktop is the place where we'll create our dashboard which can then be published for viewing via a browser.

2. Obtain the Power BI query from Azure Log Analytics

Once Power BI Desktop is installed we'll first have to obtain a query to use from Azure Log Analytics. To export a query, we simply enter the query as normal into Azure Analytics, and click the page icon with an arrow pointing to the right, then click on 'Export to Power BI (M Query)

Run Time range: Set in query	🚽 Save 🐵 Copy link 🔁 Export 🕂 New alert rule 🖈 Pin
<pre>let startTime=datetime(2018-11-14T00:01:00); let endTime=datetime(2018-11-14T11:59:59):</pre>	Export to CSV - All Columns
VMConnection where Computer contains "roshwork"	Export to CSV - Displayed Columns
<pre>where ProcessName contains "outlook" where TimeGenerated > startTime and TimeGenerated < endTime</pre>	Export to Power BI (M Query)
<pre> summarize SentKbps = (sum(BytesSent)/1024*8/60), ReceivedK (TimeGenerated, 1m), Computer summarize Percentile95SentKbps = round(percentile(SentKbps (percentile(ReceivedKbps, 95),2) by Computer</pre>	<pre>Export to Power BI (M Query) ps = (sum(BytesReceived)/1024*8/60) by bin 95),2), Percentile95ReceivedKbps = round</pre>

In this instance, to build an Outlook dashboard we don't have to be very specific, the following query will export <u>all</u> data related to Outlook for all users. For a specific machine uncomment the bottom line and add the machine name.

let startTime=datetime(2018-11-14T00:01:00); let endTime=datetime(2018-11-14T11:59:59); VMConnection | where ProcessName contains "outlook" | where TimeGenerated > startTime and TimeGenerated < endTime</pre>

By exporting all the data, we can choose what to display from within Power BI in different graphs in the same dashboard. Ensure the timeframe set at the top is what you wish to view in Power BI e.g. 24 Hours.

- 2. Create a new Dashboard in Power BI Desktop
- a. Open Power BI Desktop and you should see a start-up screen displayed. Select 'Get Data' from the options on the left
- b. On the next window which opens, scroll to the bottom of the options and select 'Blank Query' then click 'Connect'

Get Data		×
Search	All	
All	Planview Enterprise One - CTM (Beta)	~
File	(E) Twilio (Beta)	
Database	G tyGraph (Beta)	
Power BI	Webtrends (Beta)	
Azure	💸 Zendesk (Beta)	
Online Services	Web	
Other	S SharePoint list	
	🔁 OData Feed	
	S Active Directory	
	Microsoft Exchange	
	+ Hadoop File (HDFS)	
	😭 Spark (Beta)	
	R script	
	♦ ODBC	
	OLE DB	
	🗐 Blank Query	~
		Write a que
Certified Connectors	Connect	Cancel

- c. In the window which opens we'll import the Power BI query we exported from Azure Log Analytics. Click 'Get Data' from the menu at the top, then 'Blank Query'.
- In the new window which opens, click 'Advanced Editor' delete what is in the window and paste your query from Log Analytics. If all is well, a green tick should appear showing no syntax errors. If this does not occur, it's likely the copy/paste has copied some of the instructions at the top of the export.
- e. This will load the table of data into the window and when complete, click "Close and Apply" at the top to import into our blank dashboard.

Tip: Ensure you are logged in to PowerBI with the same Organizational account that you used to login to Azure and Log Analytics. Otherwise PowerBI will throw an Authentication warning since you won't have permissions to access the workspace.

f. Now we have the data loaded into the dashboard we can begin to create graphs showing the data we wish to see.

3. Create graphs in the Power BI Dashboard

You can create your own graphs/visuals in Power BI if you are familiar within otherwise, we have provided example templates for EXO, SPO, SFBO and Teams to help you with getting started. Dashboard templates (Dashboards-v2.zip) is available for download at <u>Github</u>



4.9 Publish a Power BI Dashboard

Once you're happy with your dashboard it's time to publish it. Simply click the Publish button on the top taskbar.

```
OutlookDashboard - Power BI Desktop
```



Once saved, you'll be presented a list of possible places to publish the dashboard. Select wherever you wish, and you should receive confirmation it's been published.

Once complete, login to <u>https://powerbi.com</u> via a browser and navigate to where you published the dashboard and you should see what you created in Power BI Desktop.

When logged in, to share the dashboard, simply click share in the top right-hand corner and enter the users or groups you wish to share it with.

4.10 AutoRefresh Power BI Dashboard

To refresh the dashboard with new data every day, we need to follow these steps. In the browser, when in your Power BI dashboard:

- Click on 'My Workspace' if this is where you published it.
- Next select the workspace under 'DATASETS'.
- Click the three dots to launch the menu then select "schedule refresh' from the list.

REPORTS MachineWorkspace	$\operatorname{OutlookDashboard}$
NWA_Results_Analyzer with th	LAST REFRESH FAILED:
OutlookDashboard ····	⊗ <u>Wed May 16 2018 00:18:24 GMT+0100 (GMT</u> Summer Time)
WORKBOOKS	
	Next refresh : Thu May 17 2018 00:00:00 GMT+0100 (GMT Summer Time)
DATASETS	
MachineWorkspace	
NWA_Results_Analyzer with th	RENAME
NWA_Results_Analyzer with th	REM
OutlookDashboard ···	SCHEDULE REFRESH
	SCHEDULE REFRESH
	REFRESH NOW
	ANALYZE IN EXCEL
	QUICK INSIGHTS
	DOWNLOAD .PBIX

• Select 'Schedule Refresh' (again) from the next menu and enable and configure the feature to your requirements.

5 Summary

The approach in this document can be used for:

- 3. Measuring network bandwidth usage for pilot users on-boarded to Office 365 or network bandwidth usage of on-premises users.
- 4. Endpoint monitoring dashboards post on-boarding users to Office 365

You can apply this concept for measuring any SaaS/PaaS traffic, not just Office 365. Future improvements to this project can be tracked at <u>Github</u>