PowerShell Conference Europe 2020

Internet, World

June 2-3, 2020

CAPTAIN KUSTO
DO WE HAVE THE POWER

Mateusz Czerniawski

PSCONF.EU 2020 WOULDN'T BE POSSIBLE WITHOUT OUR AWESOME SPONSORS

Microsoft

ScriptRunner®

powershell.one

@Arcontar

PowerShell Conference Europe 2020

Internet, World

June 2-3, 2020

CAPTAIN KUSTO
DO WE HAVE THE POWER

Mateusz Czerniawski

LOGS AS A SERVICE

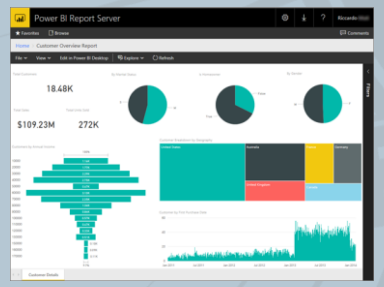
- Affordable 

LOGS AS A SERVICE

- Affordable 
- Always Available 

LOGS AS A SERVICE

- Affordable 
- Always Available 

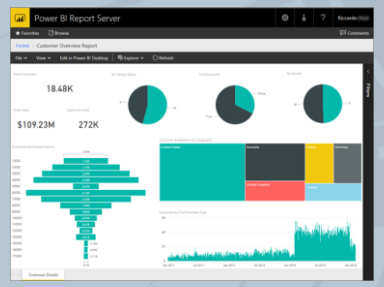
- ‘Report-able’ 

LOGS AS A SERVICE

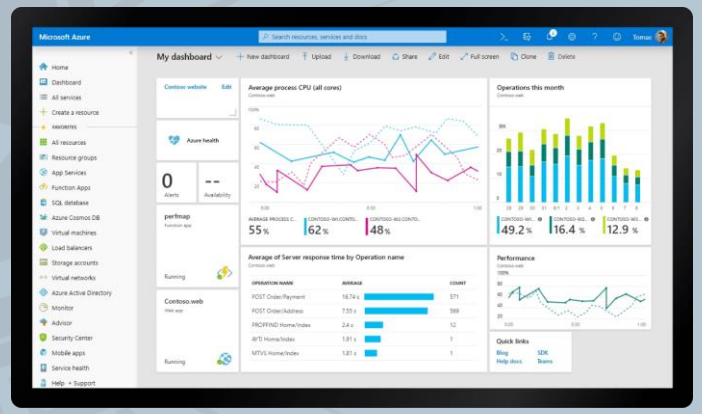
- Affordable

- Always Available

- ‘Report-able’



NOT SIEM



@Arcontar

LOGS

```
   ProviderName: ESENT

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
15.10.2019 20:05:46             455 Error            svchost (24924,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xffff...


   ProviderName: MsiInstaller

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Java A...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Node.j...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Slack ...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Tortoi...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Slack....
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Mozill...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Google...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: 7-Zip ...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Graphv...
15.10.2019 20:04:44            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Surfac...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Cisco ...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Adobe ...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Adobe ...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Local ...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Tortoi...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Micros...
15.10.2019 20:04:43            1035 Information      Windows Installer reconfigured the product. Product Name: Java 8...
15.10.2019 20:04:42            1035 Information      Windows Installer reconfigured the product. Product Name: Java 8...
```

LOGS

```
  ProviderName: ESENT

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
15.10.2019 20:05:46            455 Error            svchost (24924,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xffff...


  ProviderName: MsiInstaller

TimeCreated                     Id LevelDisplayName Messag
-----------                     -- ---------------- ------
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:42           1035 Information      Window
```

Application Number of events: 18 600

Level	Date and Time
Warning	15.10.2019 21:18:58
Warning	15.10.2019 21:18:58
Error	15.10.2019 21:18:58
Warning	15.10.2019 21:18:58
Warning	15.10.2019 21:18:58
Warning	15.10.2019 21:18:58
Warning	15.10.2019 21:18:57
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57

LOGS

```
  ProviderName: ESENT

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
15.10.2019 20:05:46            455 Error            svchost (24924,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xffff...


  ProviderName: MsiInstaller

TimeCreated                     Id LevelDisplayName Messag
-----------                     -- ---------------- ------
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:44           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:43           1035 Information      Window
15.10.2019 20:04:42           1035 Information      Window
```

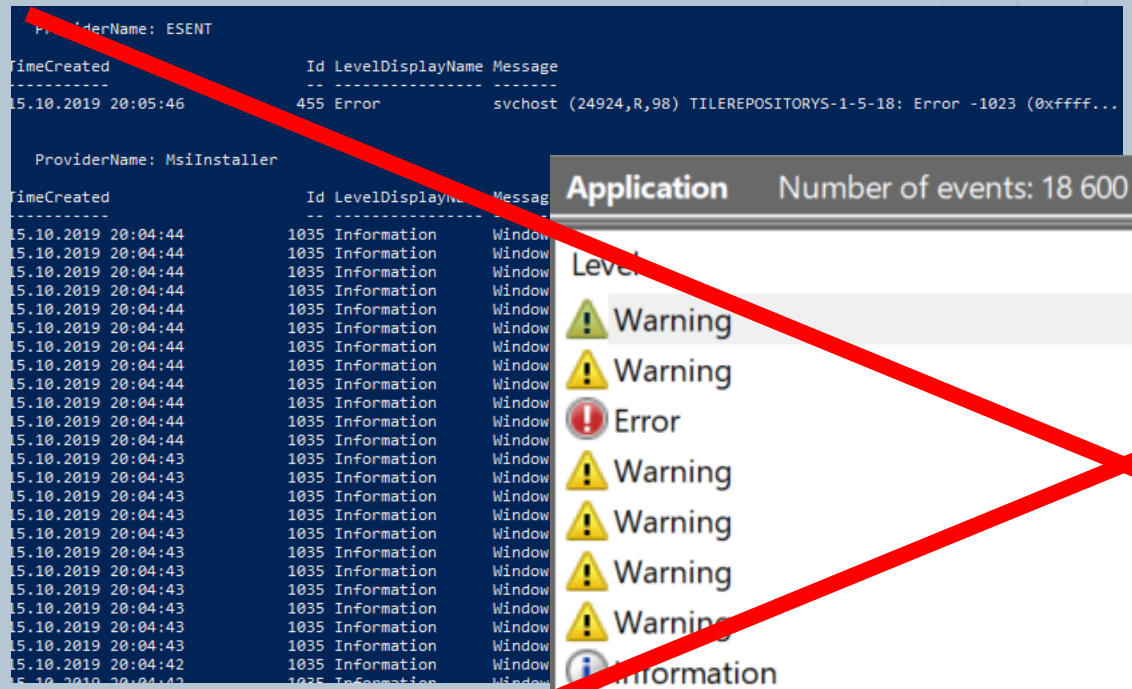
Application Number of events: 18 600

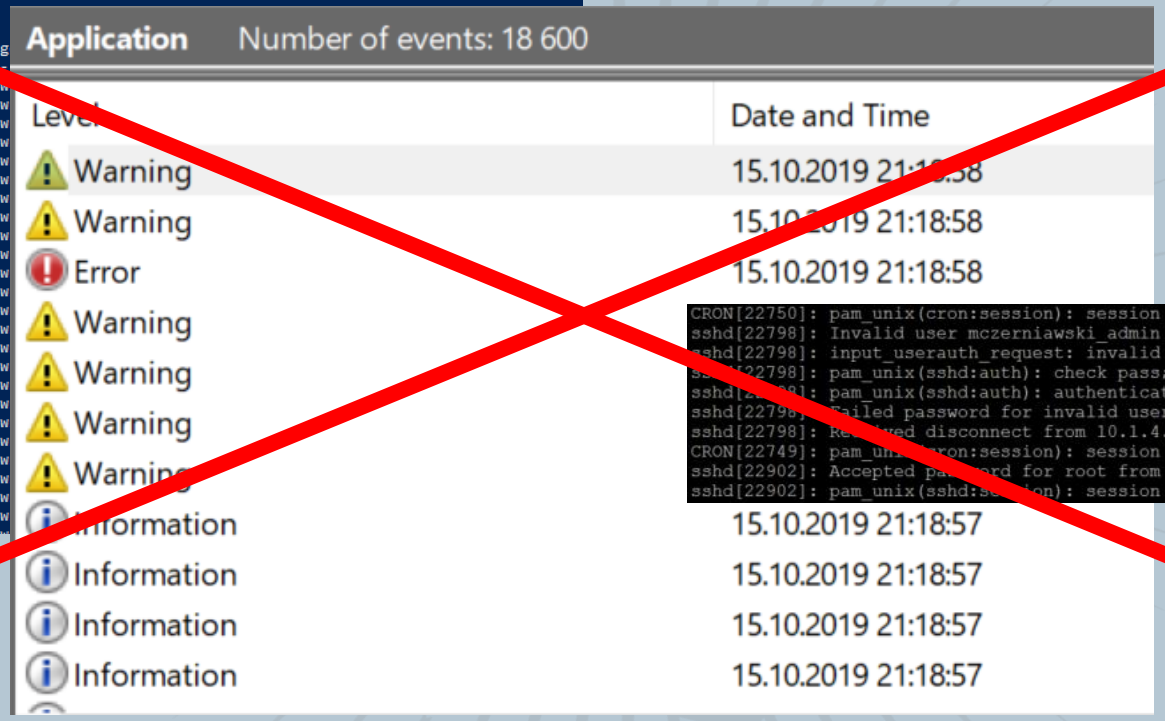
Level	Date and Time
Warning	15.10.2019 21:18:58
Warning	15.10.2019 21:18:58
Error	15.10.2019 21:18:58
Warning	
Warning	
Warning	
Warning	
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57
Information	15.10.2019 21:18:57

```
CRON[22750]: pam_unix(cron:session): session closed for user root
sshd[22798]: Invalid user mczerniawski_admin from 10.1.4.106
sshd[22798]: input_userauth_request: invalid user mczerniawski_admin [preauth]
sshd[22798]: pam_unix(sshd:auth): check pass; user unknown
sshd[22798]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
sshd[22798]: Failed password for invalid user mczerniawski_admin from 10.1.4.106 port 39166 ss
sshd[22798]: Received disconnect from 10.1.4.106: 13: Unable to authenticate [preauth]
CRON[22749]: pam_unix(cron:session): session closed for user www-data
sshd[22902]: Accepted password for root from 10.1.4.106 port 39208 ssh2
sshd[22902]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

@Arcontar

LOGS





@Arcontar

LOGS

@Arcontar

LOGS

```
let TimeG = 30d;
let Passed = (
pChecksAD_CL
| where TimeGenerated  > ago(TimeG) and Passed_b == 'True'
| project Describe_s, Context_s ,
          Passed_bTrue=Passed_b  ,
          TimeGeneratedPassed = TimeGenerated ,
          Name_s , FailureMessage_s , Target_s
);
let Failed = (
pChecksAD_CL
   | where TimeGenerated  > ago(TimeG) and Passed_b == 'False'
   | project Describe_s, Context_s ,
             Passed_bFalse = Passed_b ,
             TimeGeneratedFalse = TimeGenerated,
             Name_s , FailureMessage_s , Target_s
);
Passed | join kind=inner Failed on Name_s
| extend HowLongAgoH = ( now() - TimeGeneratedPassed )/ 1h,
         HowLongAgoD = ( now() - TimeGeneratedPassed )/ 1d
| project Describe_s, Context_s ,  Name_s , FailureMessage_s ,Passed_bTrue , Passed_bFalse,
          Target_s, TimeGeneratedPassed, TimeGeneratedFalse,
          ChecksTimeDifference = TimeGeneratedPassed - TimeGeneratedFalse,
          HowLongAgoH, HowLongAgoD
| sort by HowLongAgoH asc
```

LOGS

```
let TimeG = 30d;
let Passed = (
pChecksAD_CL
| where TimeGenerated  > ago(TimeG) and Passed_b == 'True'
| project Describe_s, Context_s ,
          Passed_bTrue=Passed_b  ,
          TimeGeneratedPassed = TimeGenerated ,
          Name_s , FailureMessage_s , Target_s
);
let Failed = (
pChecksAD_CL
   | where TimeGenerated  > ago(TimeG) and Pass
   | project Describe_s, Context_s ,
             Passed_bFalse = Passed_b ,
             TimeGeneratedFalse = TimeGenerated,
             Name_s , FailureMessage_s , Target_
);
Passed | join kind=inner Failed on Name_s
| extend HowLongAgoH = ( now() - TimeGeneratedP
         HowLongAgoD = ( now() - TimeGeneratedP
| project Describe_s, Context_s ,  Name_s , Fai
          Target_s, TimeGeneratedPassed, TimeGe
          ChecksTimeDifference = TimeGeneratedP
          HowLongAgoH, HowLongAgoD
| sort by HowLongAgoH asc
```

HowLongAgoH	HowLongAgoD	Describe_s	Context_s	Name_s
372.721	15.53	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
372.721	15.53	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
372.721	15.53	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
373.715	15.571	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
373.715	15.571	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
373.715	15.571	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
374.726	15.614	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
374.726	15.614	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
374.726	15.614	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
375.724	15.655	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
375.724	15.655	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
375.724	15.655	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co

@Arcontar

LOGS

```
let TimeG = 30d;
let Passed = (
pChecksAD_CL
| where TimeGenerated  > ago(TimeG) and Passed_b == 'True'
| project Describe_s, Context_s ,
          Passed_bTrue=Passed_b  ,
          TimeGeneratedPassed = TimeGenerated ,
          Name_s , FailureMessage_s , Target_s
);
let Failed = (
pChecksAD_CL
```

00:00:01.026

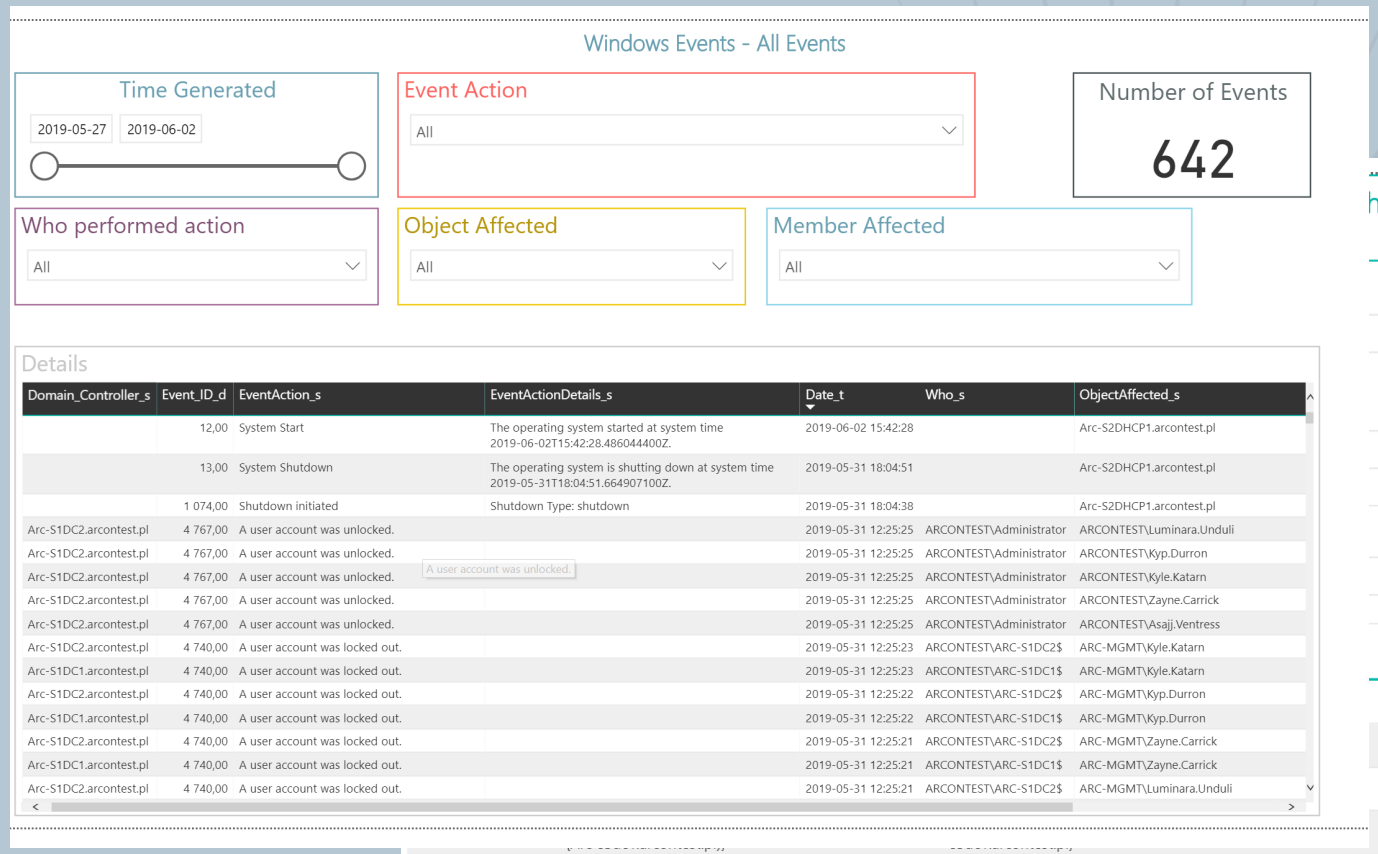
4,283 records

```
| sort by HowLongAgoH asc
```

HowLongAgoH	HowLongAgoD	Describe_s	Context_s	Name_s
372.721	15.53	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
372.721	15.53	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
375.724	15.655	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
376.722	15.697	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co
377.723	15.738	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s3dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}	Verify Domain Co

@Arcontar

LOGS



@Arcontar

LOGS

@Arcontar

LOGS

@Arcontar

LOGS

@Arcontar

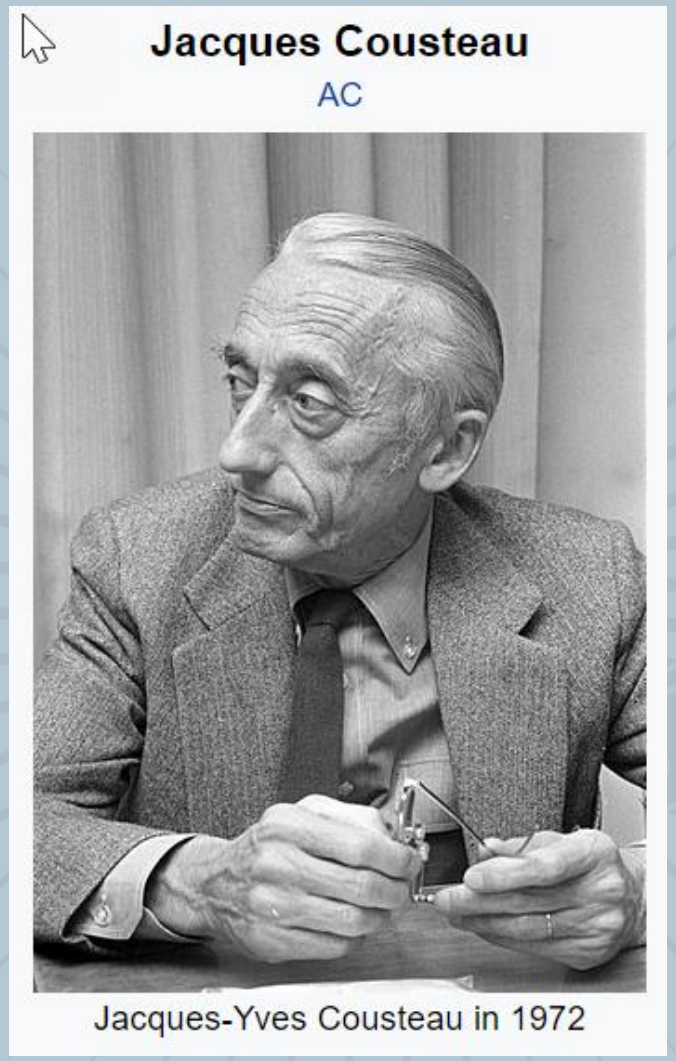
INTERESTED?

@Arcontar

AGENDA

- Azure Monitor
- Kusto Query Language (KQL)
- Working with RestAPI
- Power BI reports
- Azure Dashboards
- Alert rules

KUSTO



Jacques-Yves Cousteau in 1972

https://en.wikipedia.org/wiki/Jacques_Cousteau

@Arcontar

WHO ARE YOU

@Arcontar

WHO ARE YOU

WHO ARE YOU

WHO ARE YOU

WHO ARE YOU

MOTIVATION

@Arcontar

"THE POWER OF ♥"

The True Power of Logs is what you can do with them

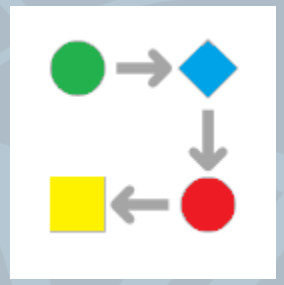
"THE POWER OF ♥"

The True Power of Logs is what you can do with them

Analyse

"THE POWER OF ♥"

The True Power of Logs is what you can do with them

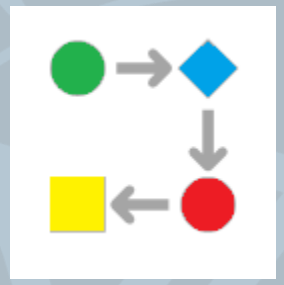


Analyse

Visualize

"THE POWER OF ♥"

The True Power of Logs is what you can do with them



Analyse

Visualize

Alert

A LIL' BIT OF POWERSHELL

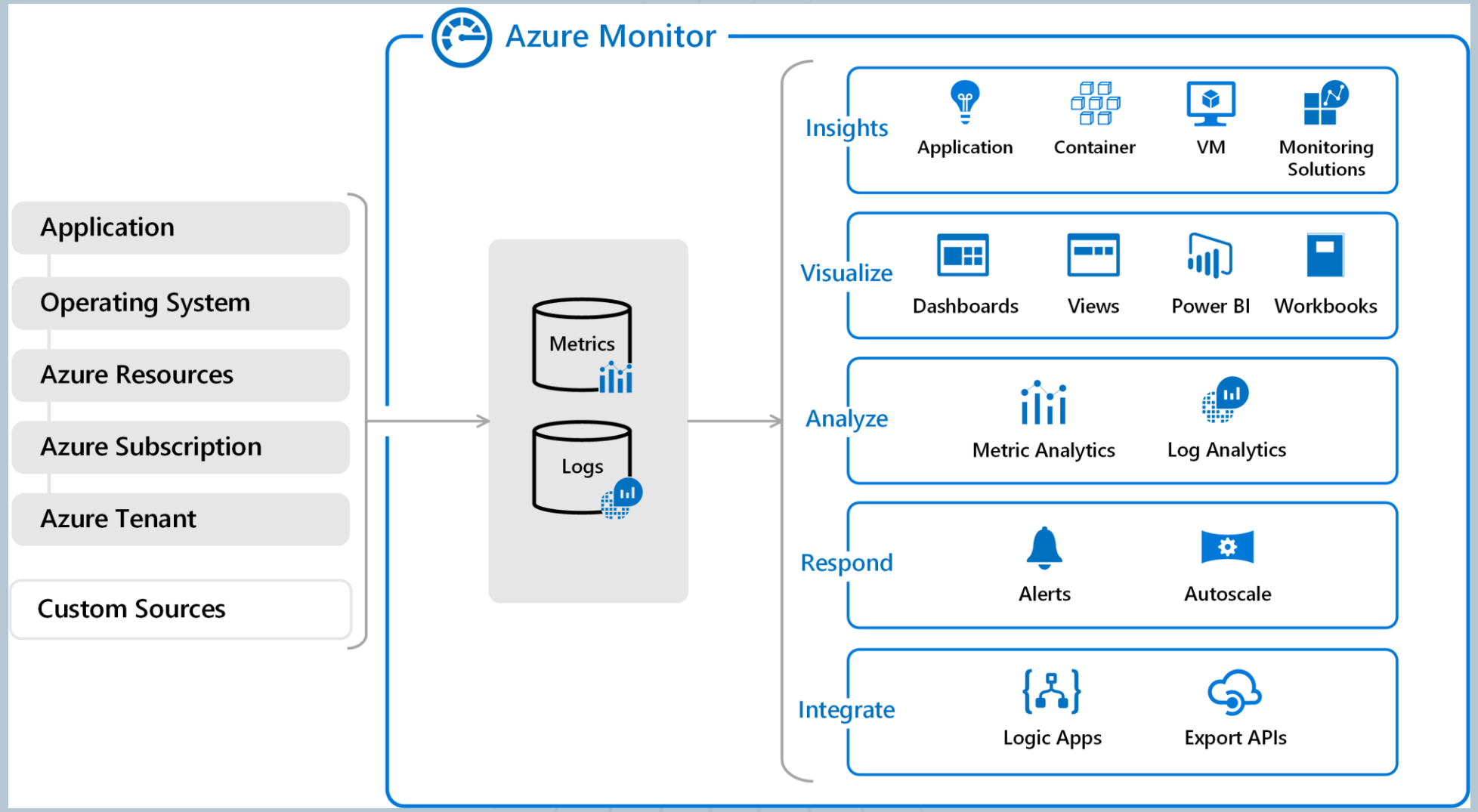
A LIL' BIT OF POWERSHELL

@Arcontar

AZURE MONITOR

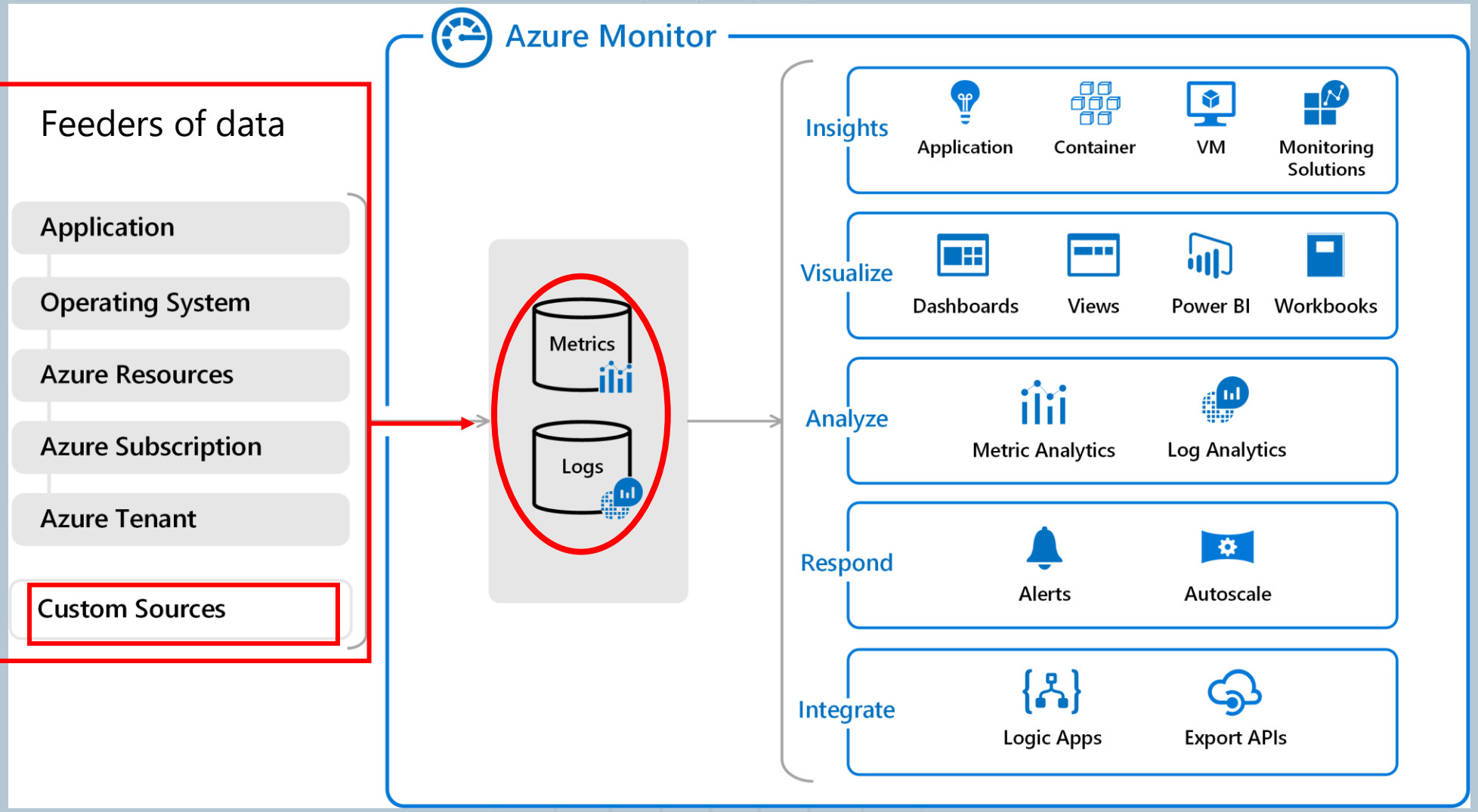
?

AZURE MONITOR

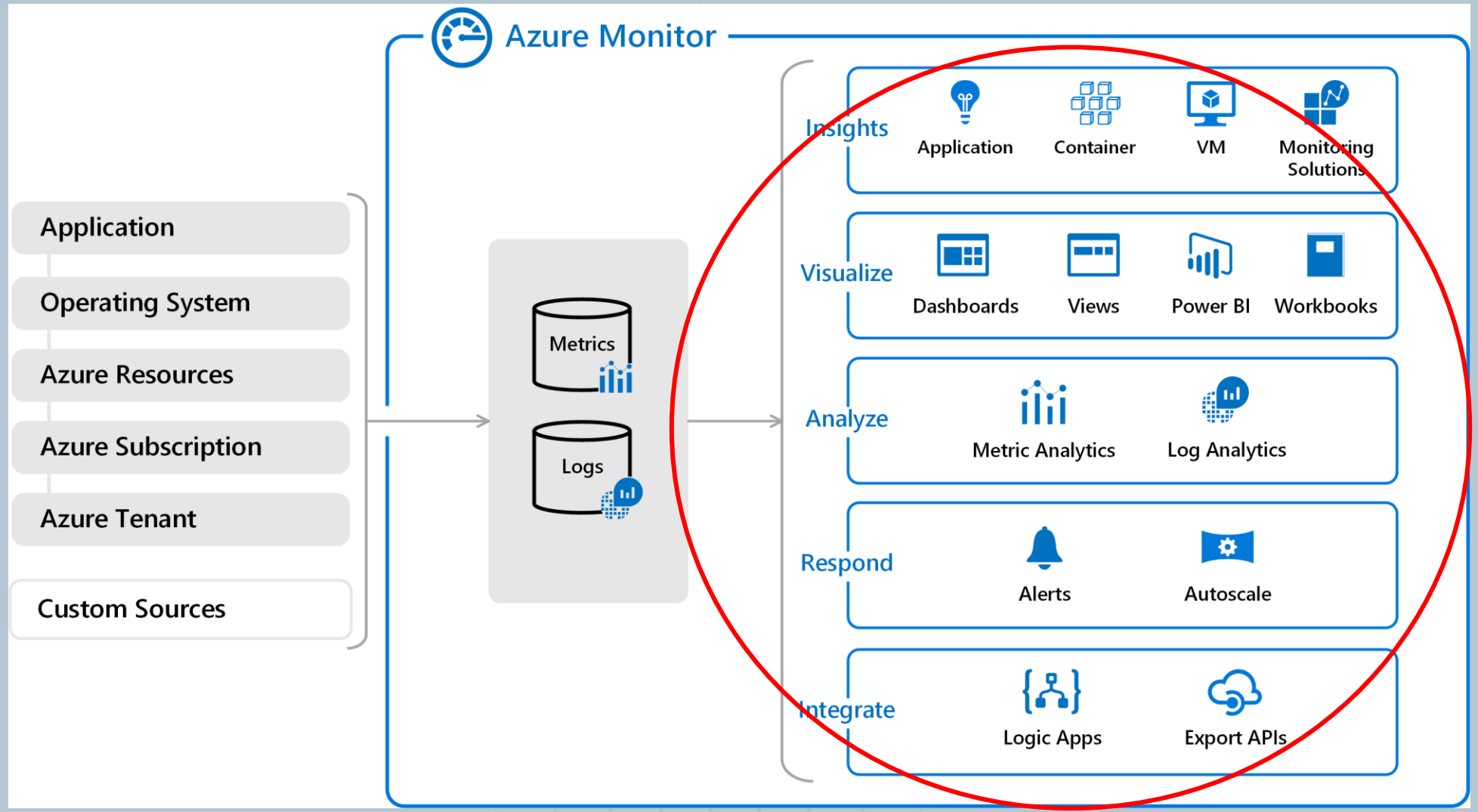


@Arcontar

AZURE MONITOR



AZURE MONITOR



@Arcontar

AZURE LOG

- Data collected and stored as **Metrics** or **Logs**
- Azure Log is a part of Azure Monitor solution
- Logs are records with custom properties

AZURE LOG

- Data collected and stored as **Metrics** or **Logs**
- Azure Log is a part of Azure Monitor solution
- Logs are records with custom properties

Accessible through

- **KQL Queries**
- **Rest API**
- **M Query**

KUSTO QUERY LANGUAGE

- A Kusto query is a **read-only** request

KUSTO QUERY LANGUAGE

- A Kusto query is a **read-only** request

- Like SQL

https://docs.microsoft.com/en-us/azure/kusto/query/sqlcheatsheet

KUSTO QUERY LANGUAGE

- A Kusto query is a **read-only** request

- Like SQL

https://docs.microsoft.com/en-us/azure/kusto/query/sqlcheatsheet

- KQL for Azure services = PowerShell for Automation

KUSTO QUERY LANGUAGE

- A Kusto query is a **read-only** request

- Like SQL

https://docs.microsoft.com/en-us/azure/kusto/query/sqlcheatsheet

- KQL for Azure services = PowerShell for Automation

- Pluralsight course

https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch

ANALYSE - KQL EXAMPLE

```
VMInventory_CL
| where DynamicMemoryEnabled_b == 'true' and MemoryStatus_s != 'OK’
```

ANALYSE - KQL EXAMPLE

VMInventory_CL

| where DynamicMemoryEnabled_b == 'true' and MemoryStatus_s != 'OK’

```
pChecksAD_CL
| where TimeGenerated > ago(7d)
| summarize ChecksPassed = (count(Passed_b == 'True')),
            ChecksFailed = (count(Passed_b == 'False'))
            by Describe_s
| sort by ChecksFailed
```

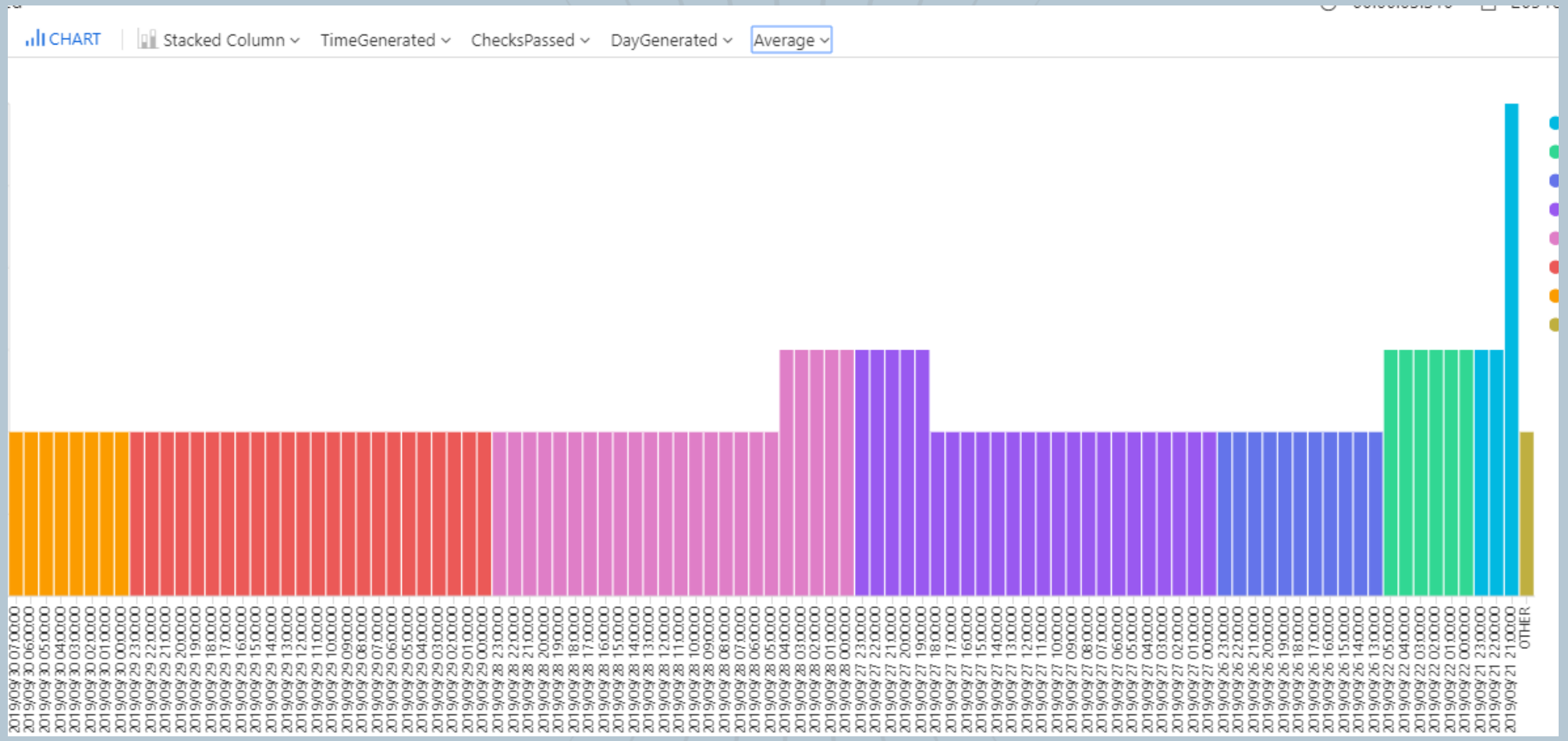
ANALYSE - KQL EXAMPLE

```
pChecksAD_CL
| where TimeGenerated > ago(7d)
| extend DayGenerated = startofday(TimeGenerated)
| summarize ChecksPassed = count(Passed_b=='True') ,
            ChecksFailed = count(Passed_b=='False')
            by DayGenerated, bin(TimeGenerated,1h) ,
            Describe_s, Context_s
| sort by bin(TimeGenerated,1h) desc, ChecksPassed, ChecksFailed
| where ChecksPassed  <> 0 and
      ChecksFailed  <> 0
| project ChecksPassed, ChecksFailed ,
          format_datetime(DayGenerated, 'yyyy/MM/dd') ,
          format_datetime(TimeGenerated, 'yyyy/MM/dd HH:mm:ss') ,
          Describe_s , Context_s
```

ANALYSE - KQL EXAMPLE

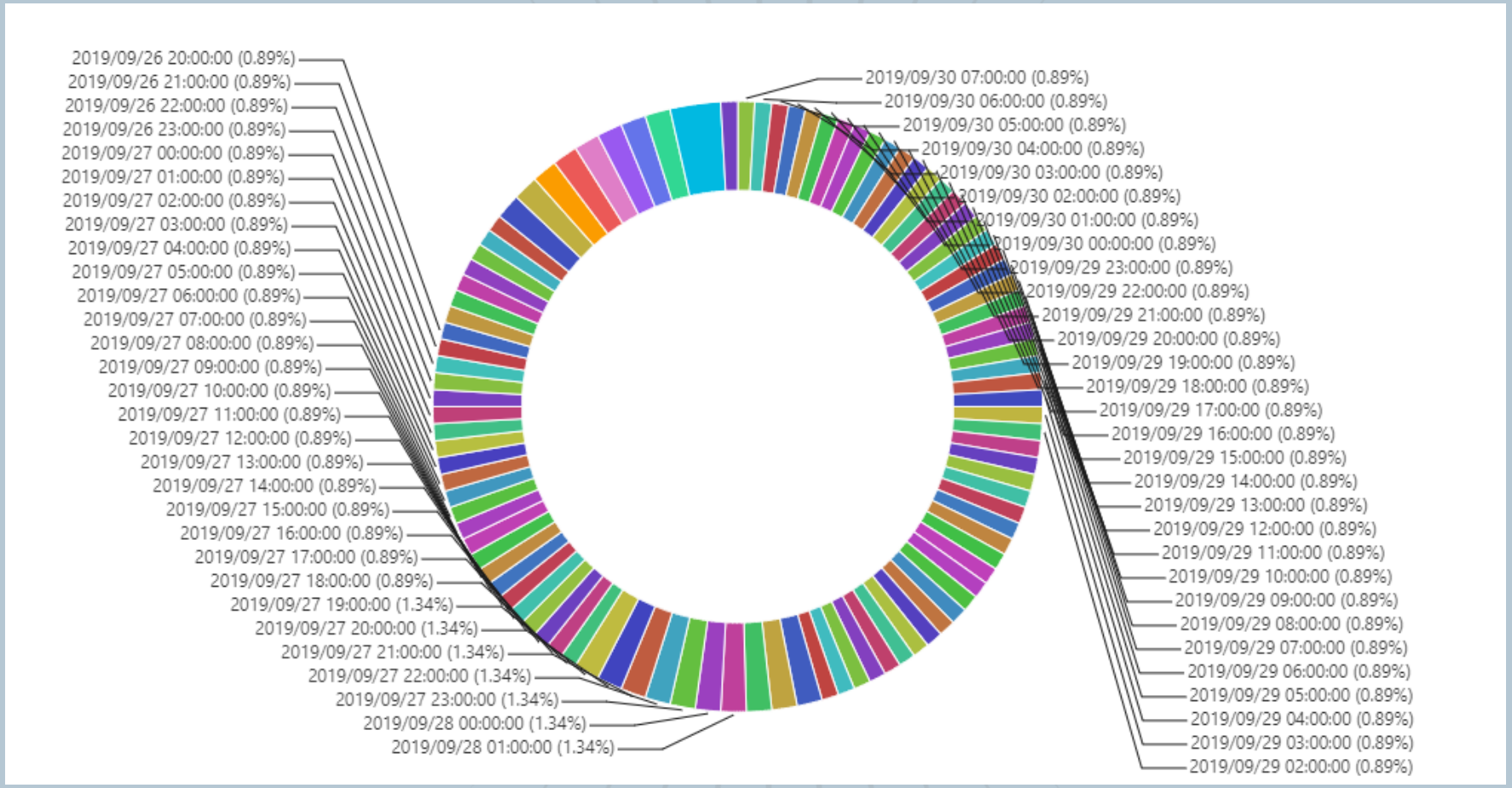
TimeGenerated	DayGenerat...	ChecksPassed	Check...	Describe_s	Context_s
2019/09/30 07:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 06:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 05:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 04:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 03:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 02:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 01:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/30 00:00:00	2019/09/30	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/29 23:00:00	2019/09/29	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/29 22:00:00	2019/09/29	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/29 21:00:00	2019/09/29	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/29 20:00:00	2019/09/29	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}
2019/09/29 19:00:00	2019/09/29	2	2	Verify Active Directory [Services] from domain controller {arcontest.pl}	Verify {Arc-s2dc1.arcontest.pl} [Connectivity] in forest {arcontest.pl}

ANALYSE - KQL EXAMPLE



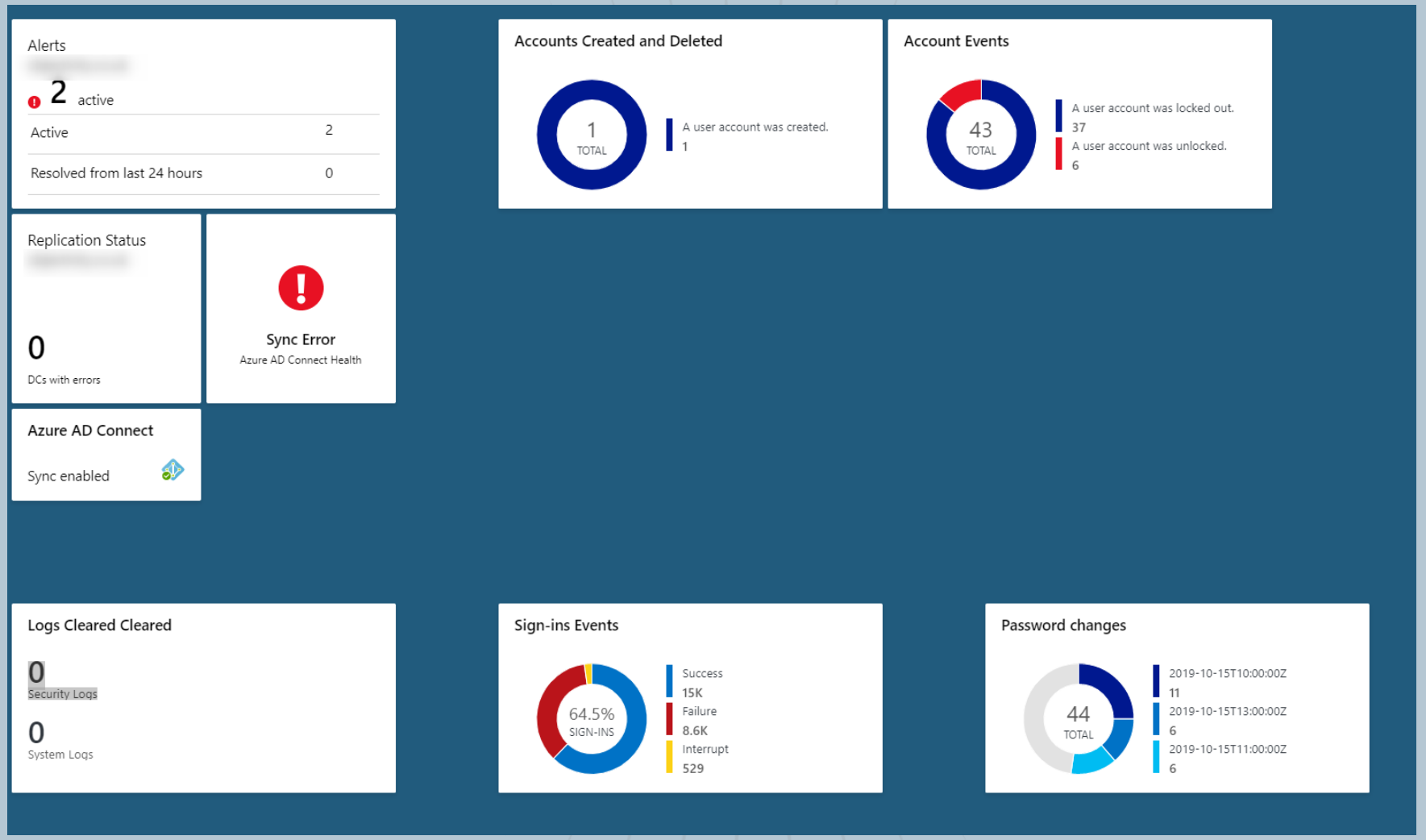
@Arcontar

ANALYSE - KQL EXAMPLE



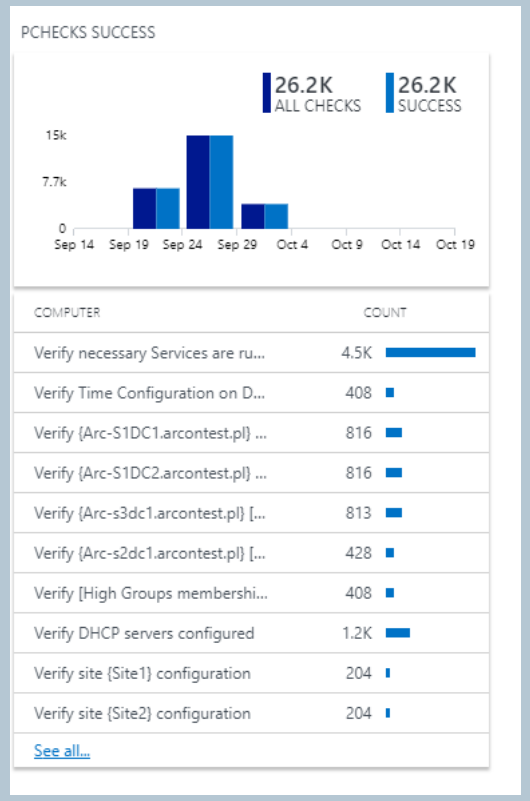
@Arcontar

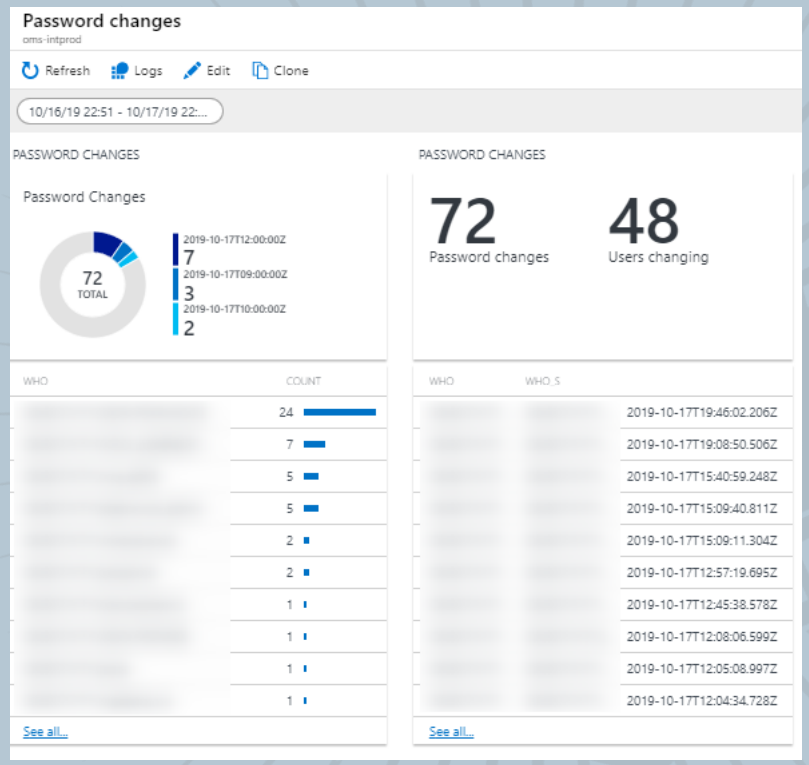
VISUALIZE - AZURE DASHBOARDS

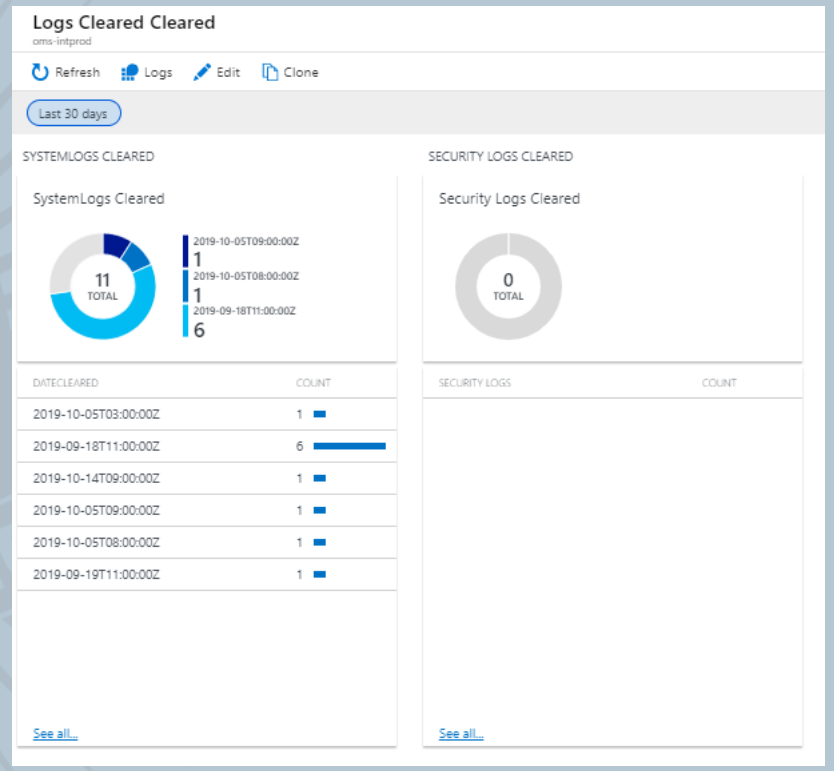


@Arcontar

VISUALIZE - AZURE DASHBOARDS

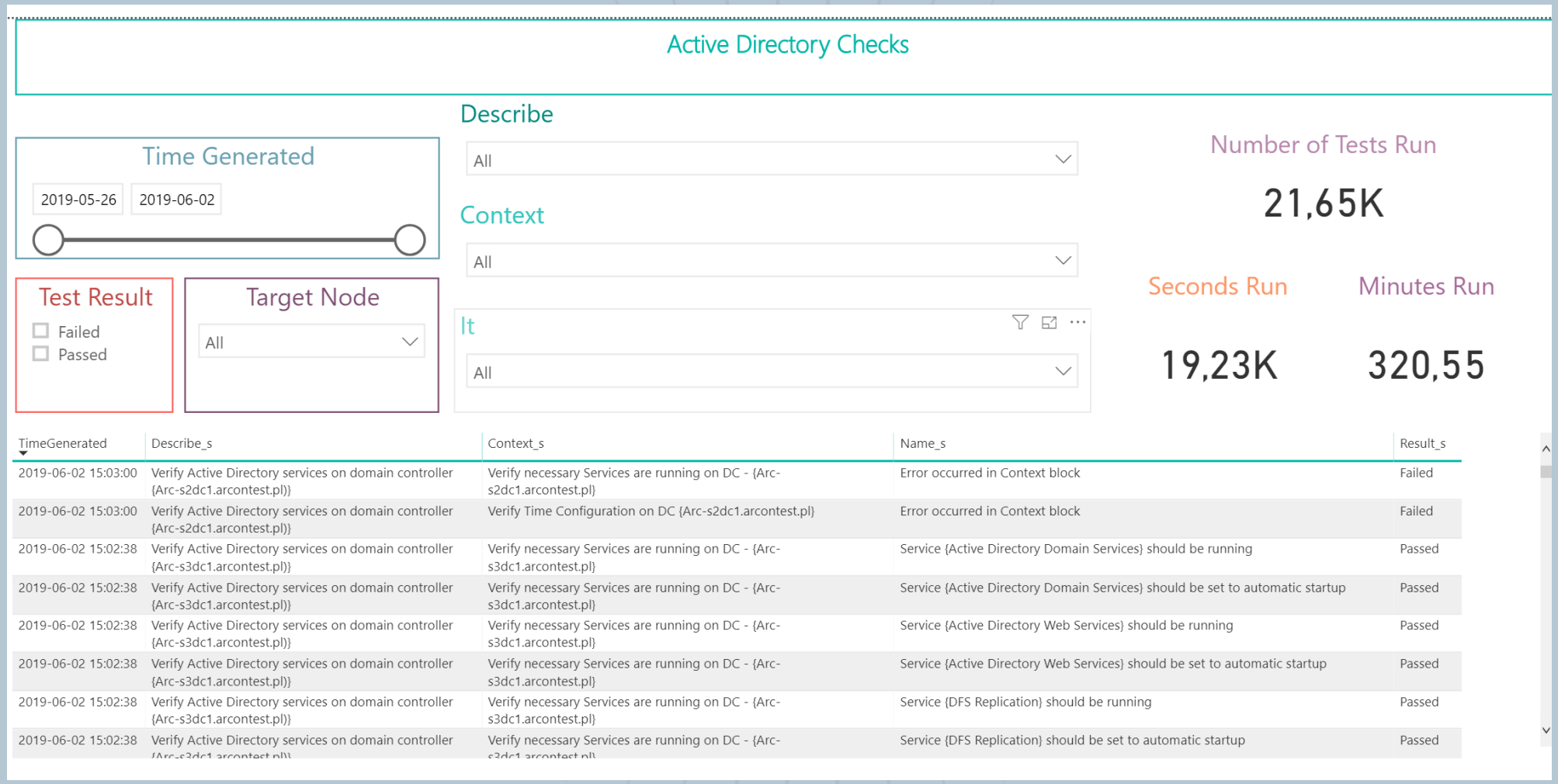






@Arcontar

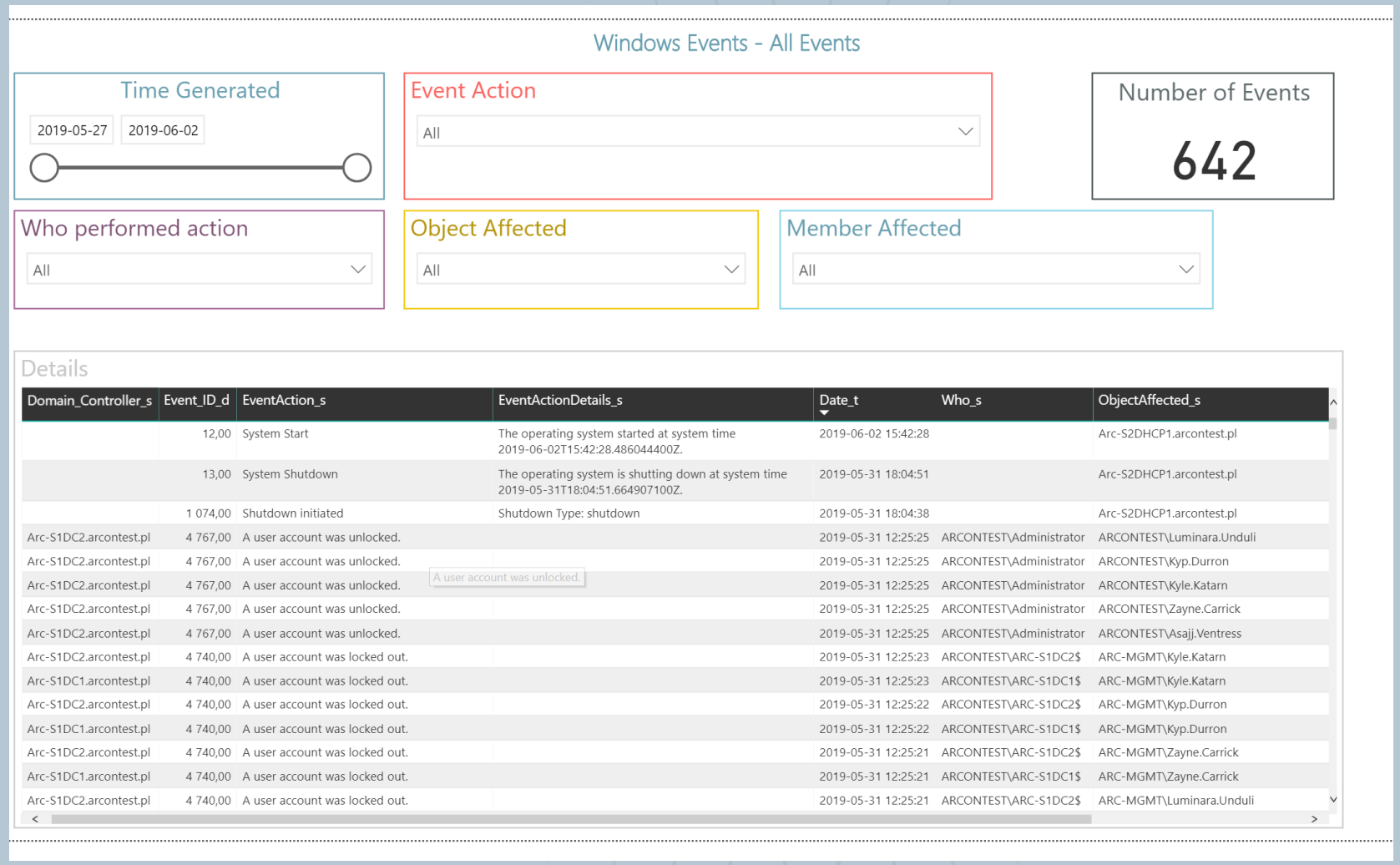
VISUALIZE - POWER BI



TimeGenerated	Describe_s	Context_s	Name_s	Result_s
2019-06-02 15:03:00	Verify Active Directory services on domain controller {Arc-s2dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s2dc1.arcontest.pl}	Error occurred in Context block	Failed
2019-06-02 15:03:00	Verify Active Directory services on domain controller {Arc-s2dc1.arcontest.pl)}	Verify Time Configuration on DC {Arc-s2dc1.arcontest.pl}	Error occurred in Context block	Failed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {Active Directory Domain Services} should be running	Passed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {Active Directory Domain Services} should be set to automatic startup	Passed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {Active Directory Web Services} should be running	Passed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {Active Directory Web Services} should be set to automatic startup	Passed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {DFS Replication} should be running	Passed
2019-06-02 15:02:38	Verify Active Directory services on domain controller {Arc-s3dc1.arcontest.pl)}	Verify necessary Services are running on DC - {Arc-s3dc1.arcontest.pl}	Service {DFS Replication} should be set to automatic startup	Passed

@Arcontar

VISUALIZE – POWER BI



Domain_Controller_s	Event_ID_d	EventAction_s	EventActionDetails_s	Date_t	Who_s	ObjectAffected_s
	12,00	System Start	The operating system started at system time 2019-06-02T15:42:28.486044400Z.	2019-06-02 15:42:28		Arc-S2DHCP1.arcontest.pl
	13,00	System Shutdown	The operating system is shutting down at system time 2019-05-31T18:04:51.664907100Z.	2019-05-31 18:04:51		Arc-S2DHCP1.arcontest.pl
	1 074,00	Shutdown initiated	Shutdown Type: shutdown	2019-05-31 18:04:38		Arc-S2DHCP1.arcontest.pl
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.		2019-05-31 12:25:25	ARCONTEST\Administrator	ARCONTEST\Luminara.Unduli
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.		2019-05-31 12:25:25	ARCONTEST\Administrator	ARCONTEST\Kyp.Durron
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.		2019-05-31 12:25:25	ARCONTEST\Administrator	ARCONTEST\Kyle.Katarn
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.		2019-05-31 12:25:25	ARCONTEST\Administrator	ARCONTEST\Zayne.Carrick
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.		2019-05-31 12:25:25	ARCONTEST\Administrator	ARCONTEST\Asajj.Ventress
Arc-S1DC2.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:23	ARCONTEST\ARC-S1DC2$	ARC-MGMT\Kyle.Katarn
Arc-S1DC1.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:23	ARCONTEST\ARC-S1DC1$	ARC-MGMT\Kyle.Katarn
Arc-S1DC2.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:22	ARCONTEST\ARC-S1DC2$	ARC-MGMT\Kyp.Durron
Arc-S1DC1.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:22	ARCONTEST\ARC-S1DC1$	ARC-MGMT\Kyp.Durron
Arc-S1DC2.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:21	ARCONTEST\ARC-S1DC2$	ARC-MGMT\Zayne.Carrick
Arc-S1DC1.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:21	ARCONTEST\ARC-S1DC1$	ARC-MGMT\Zayne.Carrick
Arc-S1DC2.arcontest.pl	4 740,00	A user account was locked out.		2019-05-31 12:25:21	ARCONTEST\ARC-S1DC2$	ARC-MGMT\Luminara.Unduli

ALERTS

Alert is based on:

- Conditions – Kusto Query
- Violated Threshold – Time Period & Frequency
- Target Notification – User, Group,
  Mail, WebHook, Azure Automation

ALMOST THERE

@Arcontar

ALTOOLS

- Microsoft's example

  https://docs.microsoft.com/en-nz/azure/azure-monitor/platform/data-collector-api#powershell-sample

- My micromodule – AL Tools

  https://www.mczerniawski.pl/powershell/altools-initial-version/

  https://www.powershellgallery.com/packages/ALTools/

ALTOOLS

```powershell
$invocationStartTime = [DateTime]::UtcNow
$object = Get-VMInventory -ComputerName 'HVHost1'
$invocationEndTime = [DateTime]::UtcNow

$writeToLogAnalyticsSplat = @{
    ALWorkspaceID        = 'c7eae394-xxxx-yyyy-zzzz-2bbccd85e0a4'
    invocationStartTime  = $invocationStartTime
    PSObject             = $object
    ALTableIdentifier    = 'VMInventory'
    invocationEndTime    = $invocationEndTime
    WorkspacePrimaryKey  = 'sSwhziHxeeR.....LOULHg+PNbsV9qf68CuRymn3z0coD6BA=='
}
Write-ToLogAnalytics @writeToLogAnalyticsSplat
```

AZURERM WITH REST API

```
Login-AzureRmAccount -Credential $creds -ServicePrincipal -Tenant ’…’
```

https://dev.loganalytics.io/

```
$query = @”
VMInventory_CL
| where DynamicMemoryEnabled_b == 'true' and MemoryStatus_s != ’OK’
“@

$queryResults = Invoke-AzureRmOperationalInsightsQuery  -
WorkspaceId ’…’ -Query $query
```

REMOVE DATA FROM LOG ANALYTICS

Deleting data from Log Analytics has no GUI option!

- Need to add an AAD Application the Role ‘Data Purger’
  - It is resource consuming
  - Destructive and non-reversible

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/personal-data-mgmt#how-to-export-and-delete-private-data

REMOVE DATA FROM LOG ANALYTICS

Deleting data from Log Analytics has no GUI option!

- Need to add an AAD Application the Role 'Data Purger'
  - It is resource consuming
  - Destructive and non-reversible

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/personal-data-mgmt#how-to-export-and-delete-private-data

That is why I'm not adding this to AL Tools module

Instead – use custom retention policy per tables

https://azure.microsoft.com/en-us/updates/retention-by-type/

DEMO

- Create workspace
- Send logs
- Get logs

With PowerShell

DEMO

- Create workspace
- Send logs
- Get logs

With PowerShell

- Query with KQL
- Azure Dashboards
- Power BI – examples WEFTools & pChecksAD

DEMO

PRICING

@Arcontar

PRICING

- per GB
  - Data Ingestion - €2,522 for each GB
  - Data Retention - €0,110 for each GB/month

PRICING

- per GB
  - Data Ingestion - €2,522 for each GB
  - Data Retention - €0,110 for each GB/month

BUT

- Data ingestion – 5GB per month FREE
- Data Retention – first 31 days FREE

https://azure.microsoft.com/en-gb/pricing/details/monitor/

PRICING - EXAMPLE

- 10 servers – 30MB of custom logs (text) per day
- Retention for 3 months

PRICING - EXAMPLE

- 10 servers – 30MB of custom logs (text) per day
- Retention for 3 months

Ingestion

10 * 30MB = 300MB/day = 9GB a month

9GB – 5GB (free) = 4GB * € 2,522 = € 10,088 per month

PRICING - EXAMPLE

- 10 servers – 30MB of custom logs (text) per day
- Retention for 3 months

Ingestion

10 * 30MB = 300MB/day = 9GB a month

9GB – 5GB (free) = 4GB * € 2,522 = € 10,088 per month

Retention

1st Month – 9GB - FREE

2nd Month – 18GB (9GB Free) 9 * € 0,110 = € 0,88

3rd Month – 27 GB (9GB free) 18 * € 0,110 = € 1,98

PRICING - EXAMPLE

- 10 servers – 30MB of custom logs (text) per day
- Retention for 3 months

Ingestion

10 * 30MB = 300MB/day = 9GB a month

9GB – 5GB (free) = 4GB * € 2,522 = € 10,088 pe

Retention

1st Month – 9GB - FREE

2nd Month – 18GB (9GB Free) 9 * € 0,110 = € 0,88

3rd Month – 27 GB (9GB free) 18 * € 0,110 = € 1,98

SUMMARY - AZURE LOGS

- It comes with an acceptable intro cost
- It requires NO maintenance time (as it's a service)
- It's scalable with reasonable cost
- It comes with NO `out of the box` queries

SUMMARY - AZURE LOGS

- It comes with an acceptable intro cost
- It requires NO maintenance time (as it's a service)
- It's scalable with reasonable cost
- It comes with NO `out of the box` queries
- but with an addition of Power BI and Azure Dashboards

allows YOU to build what YOU need in minutes 🕐 !!

SUMMARY - AZURE LOGS - IS NOT

- a SIEM solution

  Instead look for Azure Sentinel

  https://azure.microsoft.com/en-in/services/azure-sentinel

- an SQL database

  Build your own ‘relations’ on-the-fly

- an ELK replacement

  a subset of Logs is stored

YET ANOTHER TOOL INC.

@Arcontar

POWER SHELL

@Arcontar

SLIDES + DEMO CODE

```
Start-Process -FilePath https://github.com/psconfeu/2020
```

@Arcontar

QUESTIONS

@Arcontar

ABOUT_SPEAKER

Mateusz Czerniawski

Arcontar

mczerniawski@arcon.net.pl

@Arcontar

www.mczerniawski.pl

mczerniawski

PowerShell Conference Europe 2021
Hannover, Germany
June 1-4, 2021

Delegate sign-up opens November 2020 at https://psconf.eu