



# Captain Kusto do we have the Power?

Azure Log Analytics, PowerShell, Power BI  
Kusto Query Language

# Logs as a Service

- Affordable

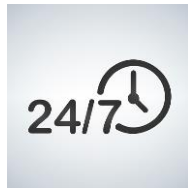


# Logs as a Service

- Affordable



- Always Available

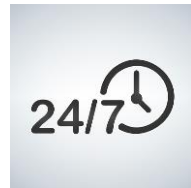


# Logs as a Service

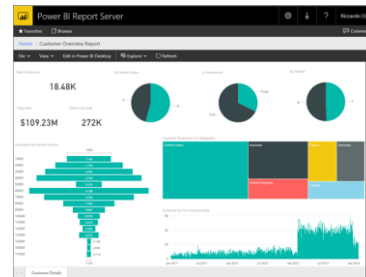
- Affordable



- Always Available



- 'Report-able'

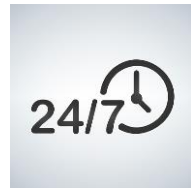


# Logs as a Service

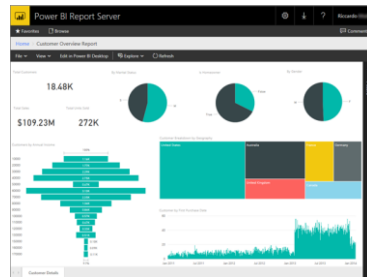
- Affordable



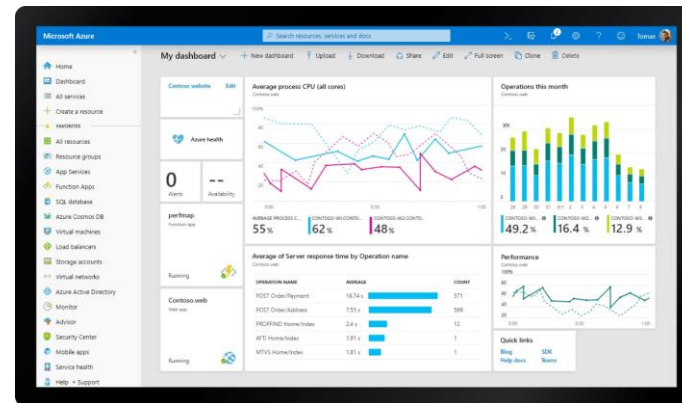
- Always Available



- 'Report-able'



## NOT SIEM














# 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...
15.10.2019 20:04:42 1035 Information     Windows Installer reconfigured the product. Product Name: Micros...
```

ProviderName: MsiInstaller			
TimeCreated	Id	LevelDisplayName	Message
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:44	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:43	1035	Information	Windows
15.10.2019 20:04:42	1035	Information	Windows









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

```

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...)

```

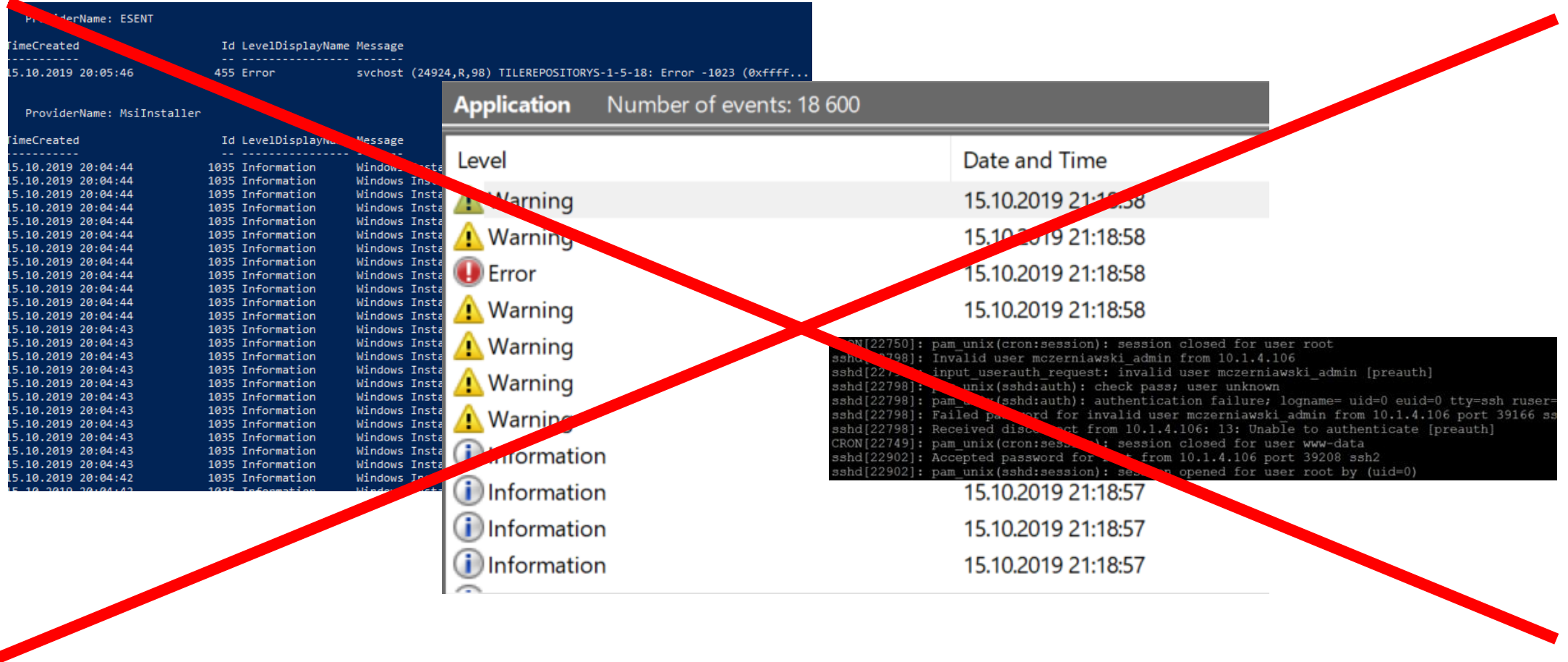
ProviderName: MsiInstaller				
TimeCreated	Id	Level	DisplayName	Message
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:44	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:43	1035	Information	Windows	Insta
15.10.2019 20:04:42	1035	Information	Windows	Insta
15.10.2019 20:04:42	1035	Information	Windows	Insta

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	<pre>CRON[22750]: pam_unix(cron:session): session closed for u sshd[22798]: Invalid user mczerniawski_admin from 10.1.4. sshd[22798]: input_userauth_request: invalid user mczerni sshd[22798]: pam_unix(sshd:auth): check pass; user unknow sshd[22798]: pam_unix(sshd:auth): authentication failure; sshd[22798]: Failed password for invalid user mczerniawsk sshd[22798]: Received disconnect from 10.1.4.106: 13: Un CRON[22749]: pam_unix(cron:session): session closed for u sshd[22902]: Accepted password for root from 10.1.4.106 p sshd[22902]: pam_unix(sshd:session): session opened for u</pre>
 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 mczeraniwski_admin from 10.1.4.106
sshd[22798]: input_userauth_request: invalid user mczeraniwski_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 mczeraniwski_admin from 10.1.4.106 port 39166 ssh
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)
```



# Logs



The image displays two screenshots of system logs, both of which are crossed out with a large red 'X'.

**Left Screenshot (Windows Event Viewer):**

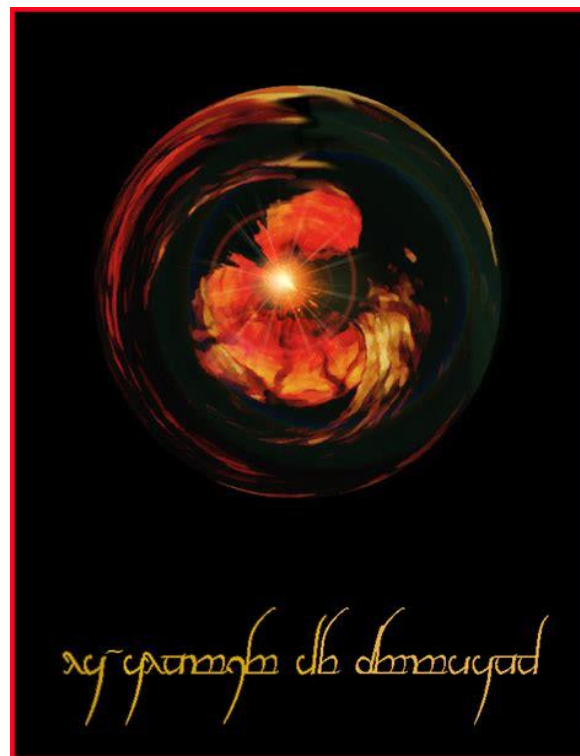
- ProviderName: ESENT**
- Table with columns: TimeCreated, Id, Level, DisplayName, Message.
- Entry: 15.10.2019 20:05:46, 455, Error, svchost (24924,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xffff...
- ProviderName: MsiInstaller**
- Table with columns: TimeCreated, Id, Level, DisplayName, Message.
- Multiple entries from 15.10.2019 20:04:44 to 20:04:42, mostly Information level (1035), related to Windows Installer.

**Right Screenshot (Application Log):**

- Application** Number of events: 18 600
- Table with columns: Level, Date and Time.
- Entries include: Warning (15.10.2019 21:18:58), Error (15.10.2019 21:18:58), and Information (15.10.2019 21:18:57).
- Below the table, a detailed log entry is shown:

```
CRON[22750]: pam_unix(cron:session): session closed for user root
sshd[22798]: Invalid user mczeraniawski_admin from 10.1.4.106
sshd[22798]: input userauth_request: invalid user mczeraniawski_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 mczeraniawski_admin from 10.1.4.106 port 39166 ssh
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)
```

# Logs



# 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 Passed_b == 'False'
| project Describe_s, Context_s,
    Passed_bFalse = Passed_b,
    TimeGeneratedFailed = TimeGenerated,
    Name_s, FailureMessage_s, Target_s
);
Passed | join kind=inner Failed on Name_s
| extend HowLongAgoH = ( now() - TimeGeneratedPassed ).Hours,
    HowLongAgoD = ( now() - TimeGeneratedPassed ).Days
| project Describe_s, Context_s, Name_s, FailureMessage_s, Target_s,
    TimeGeneratedPassed, TimeGeneratedFailed,
    ChecksTimeDifference = TimeGeneratedPassed - TimeGeneratedFailed,
    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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C
>	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 C

# Logs

```
let TimeG = 30d;  
let Passed = (  
pChecksAD_CL
```

```
| where TimeGenerated > ago(TimeG) and Passed_b == 'True'
```

project	Describe_s	Context_s	HowLongAgoH	HowLongAgoD	Describe_s	Context_s	Name_s
	Passed_bTrue=Passed_b						
	TimeGeneratedPassed = TimeGenerated						
	Name_s	FailureMessage_s	Target_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 Cc

 00:00:01.026



4,283 records

project	Describe_s	Context_s	Name_s	TimeGeneratedPassed	TimeGenerated	HowLongAgoH	HowLongAgoD	Describe_s	Context_s	Name_s
	Target_s	TimeGeneratedPassed	TimeGenerated							
	ChecksTimeDifference = TimeGeneratedPassed									
	HowLongAgoH	HowLongAgoD								
	sort by	HowLongAgoH	asc							
	> 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 Cc
	> 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 Cc
	> 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 Cc
	> 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 Cc
	> 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 Cc
	> 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 Cc
	> 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 Cc
	> 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 Cc

# Logs

Windows Events - All Events

Time Generated  
2019-05-27 2019-06-02

Event Action  
All

Number of Events  
642

Who performed action  
All

Object Affected  
All

Member Affected  
All

Details

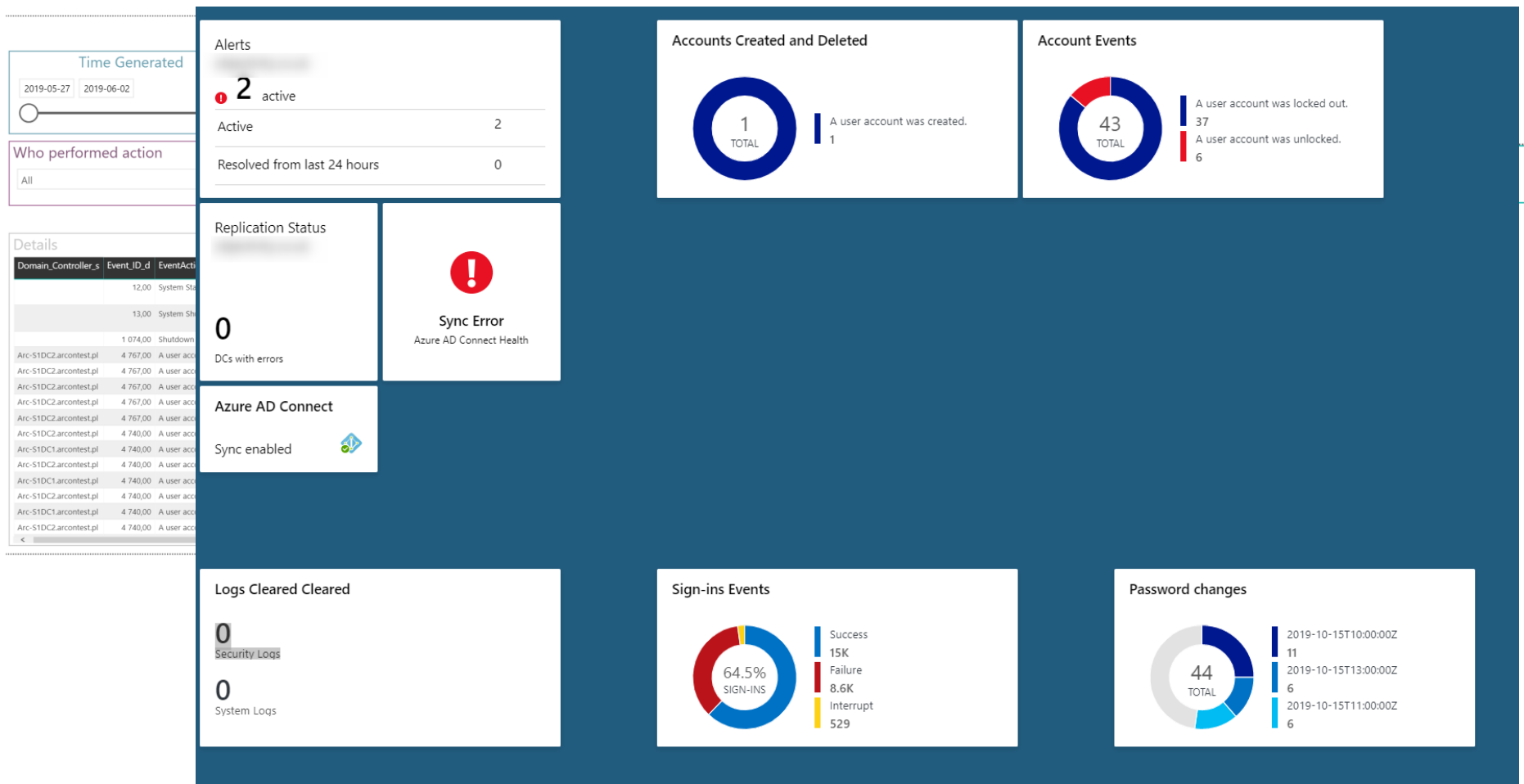
Domain_Controller_s	Event_ID_d	EventAction_s	EventActionDetails_s	Date_t	Who_s	ObjectAffected_s
	12,00	System Start	The operating system started at system time 2019-06-02T15:42:28.486044400Z.	2019-06-02 15:42:28		Arc-S2DHCPI.arcontest.pl
	13,00	System Shutdown	The operating system is shutting down at system time 2019-05-31T18:04:51.664907100Z.	2019-05-31 18:04:51		Arc-S2DHCPI.arcontest.pl
	1 074,00	Shutdown initiated	Shutdown Type: shutdown	2019-05-31 18:04:38		Arc-S2DHCPI.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\Kyp.Durron	ARCONTEST\Kyp.Durron
Arc-S1DC2.arcontest.pl	4 767,00	A user account was unlocked.	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-S1DC2S	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-S1DC1S	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-S1DC2S	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-S1DC1S	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-S1DC2S	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-S1DC1S	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-S1DC2S	ARC-MGMT\Luminara.Unduli

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 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

## Directory Checks

</

# Logs





# Logs





# Logs



# Interested?



# After this session

---

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

# WHO are you

---



# WHO are you

---



# WHO are you

---



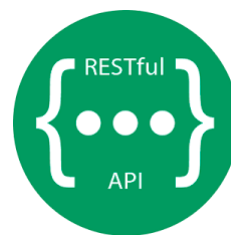
# WHO are you

---



# WHO are you

---





“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



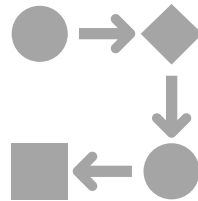
Analyze

“The Power of ♥”

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



Analyze



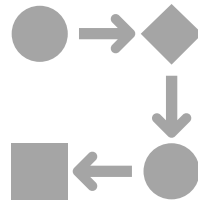
Visualize

“The Power of ♥”

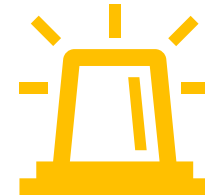
The True Power of Logs is what you can do with them



Analyze



Visualize



Alert

# A lil' bit of PowerShell

---

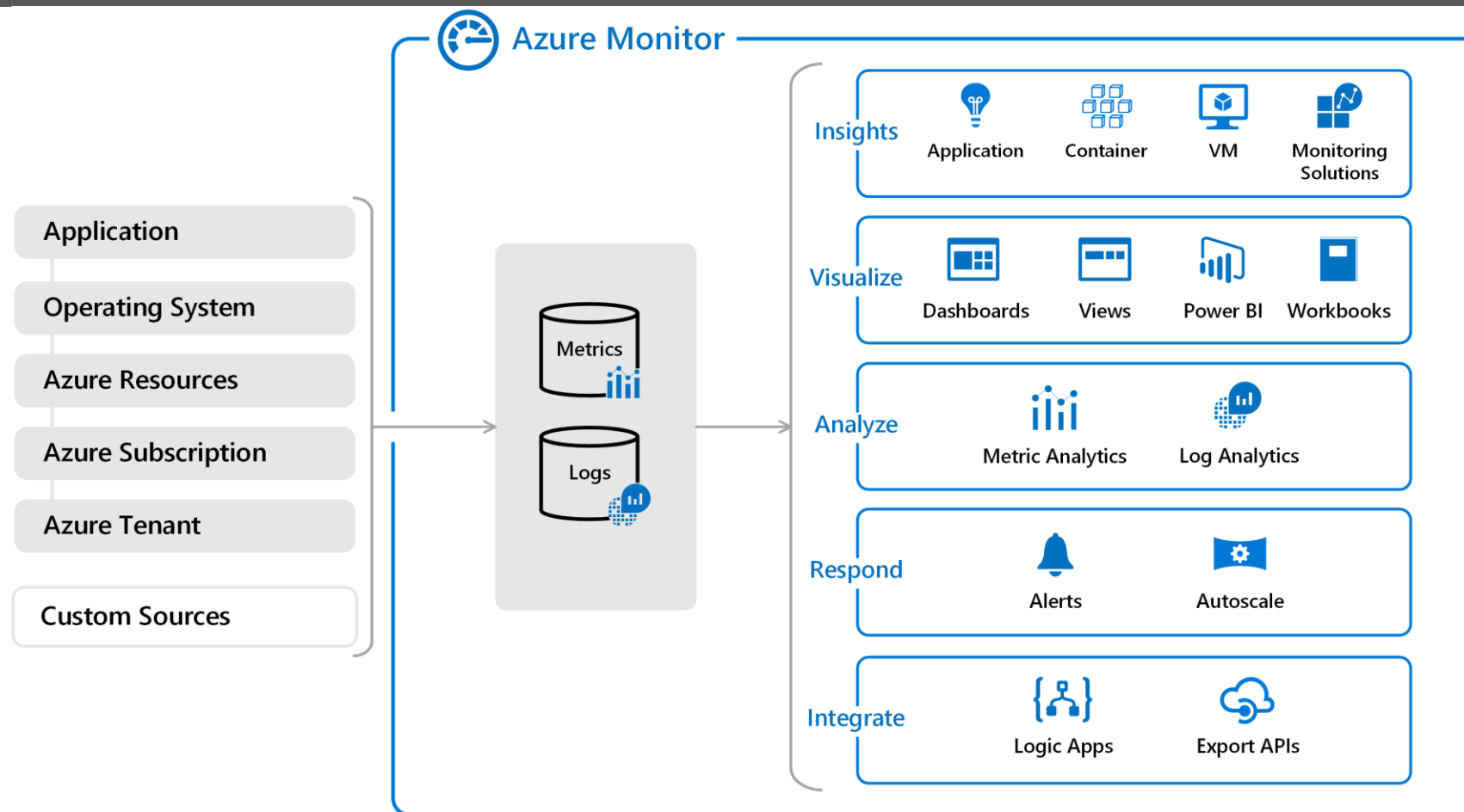


# Azure Monitor

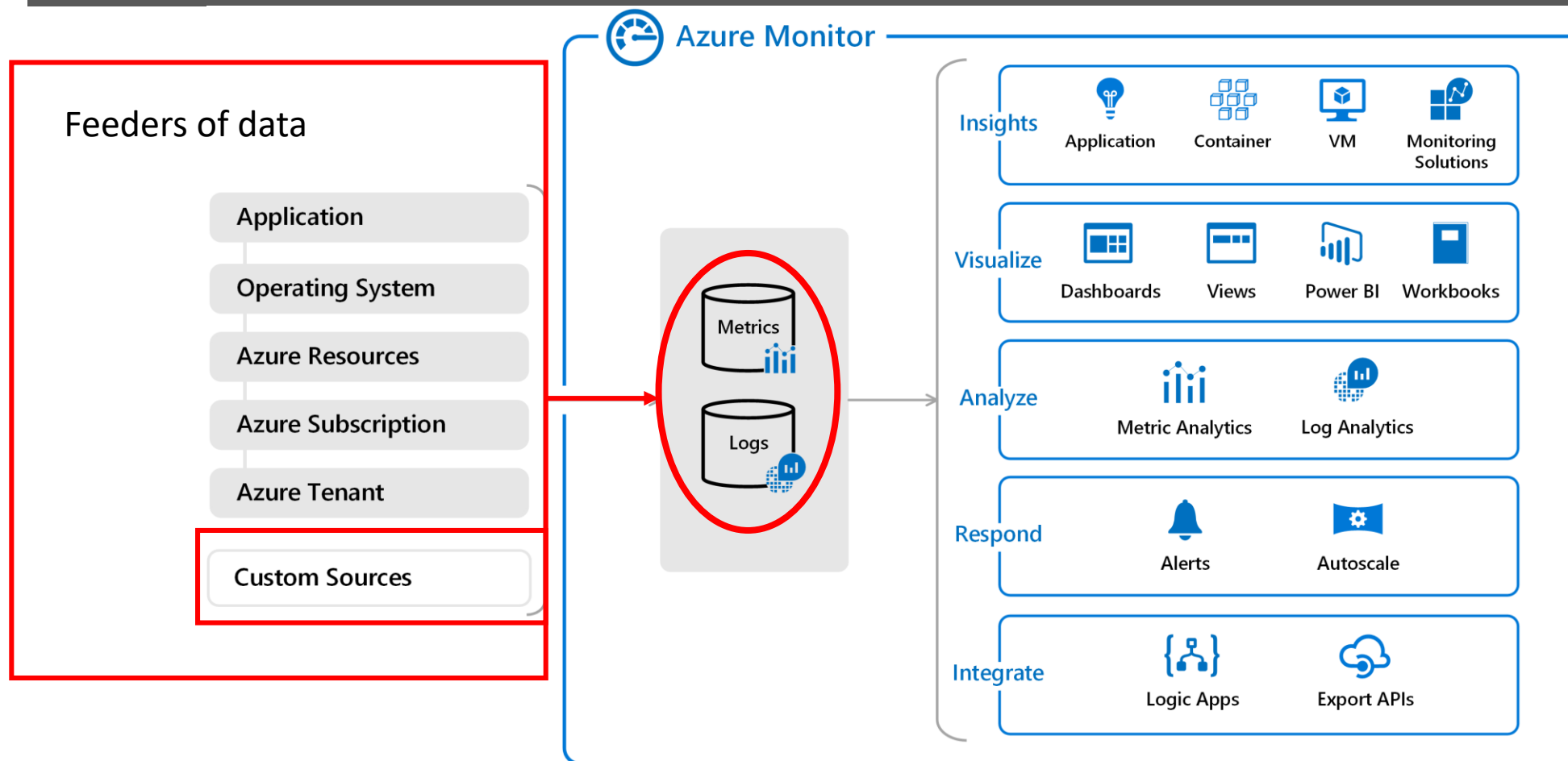
---



# Azure Monitor

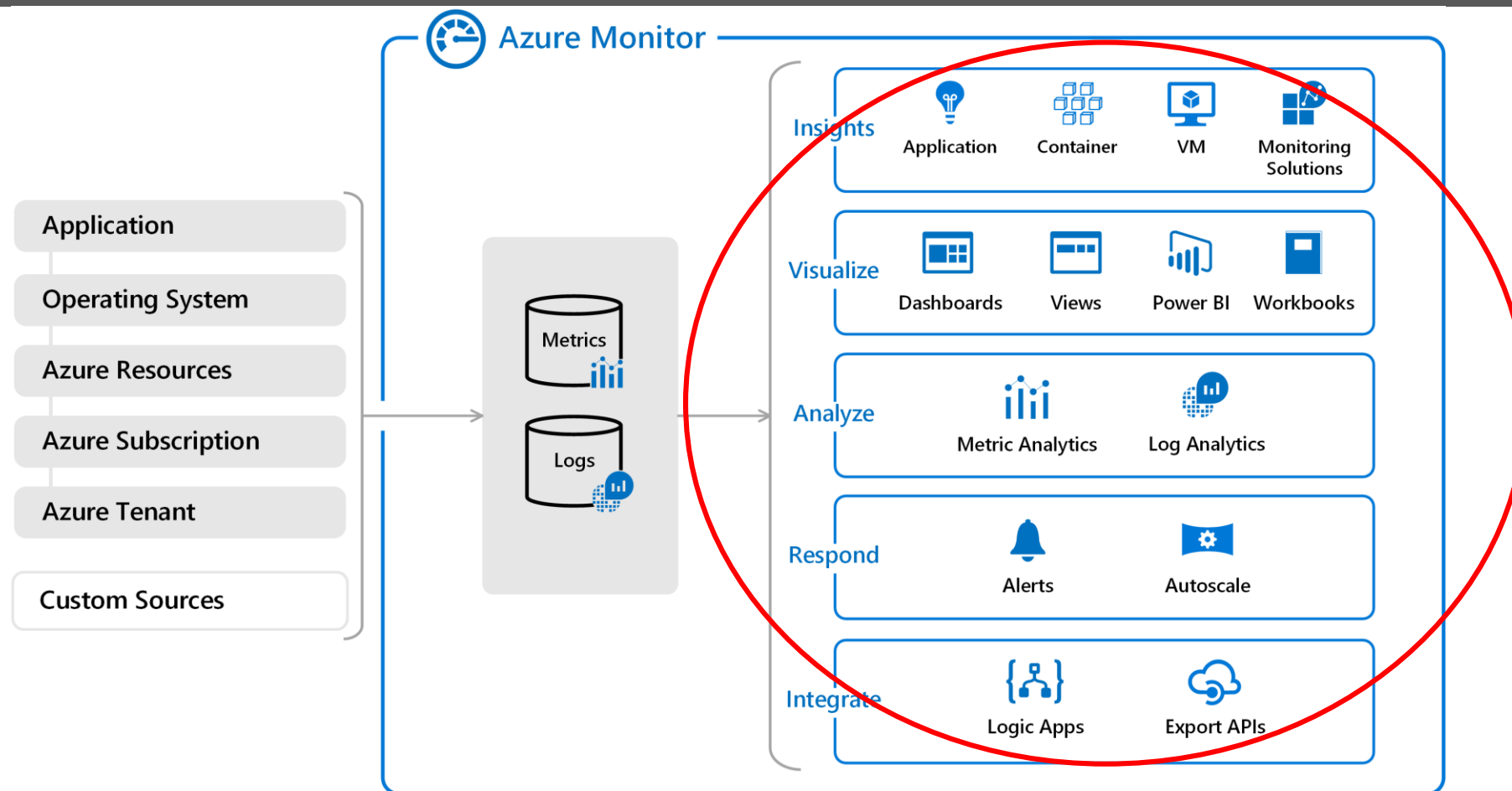


# Azure Monitor





# Azure Monitor



# 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
- Similar to SQL

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

# Kusto Query Language

---

- A Kusto query is a **read-only** request
- Similar to 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
- Similar to 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
```

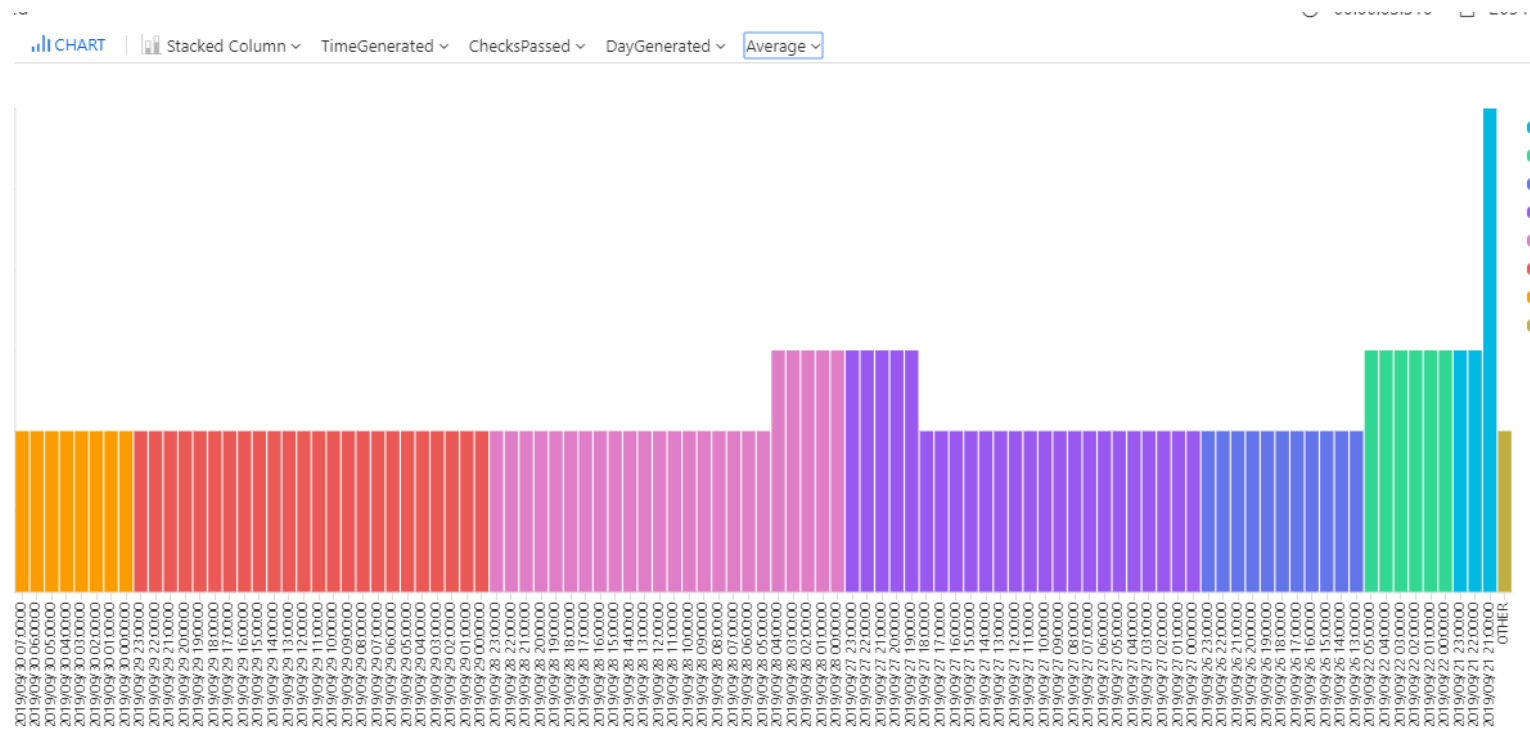
# Analyse - KQL Example

```
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
```

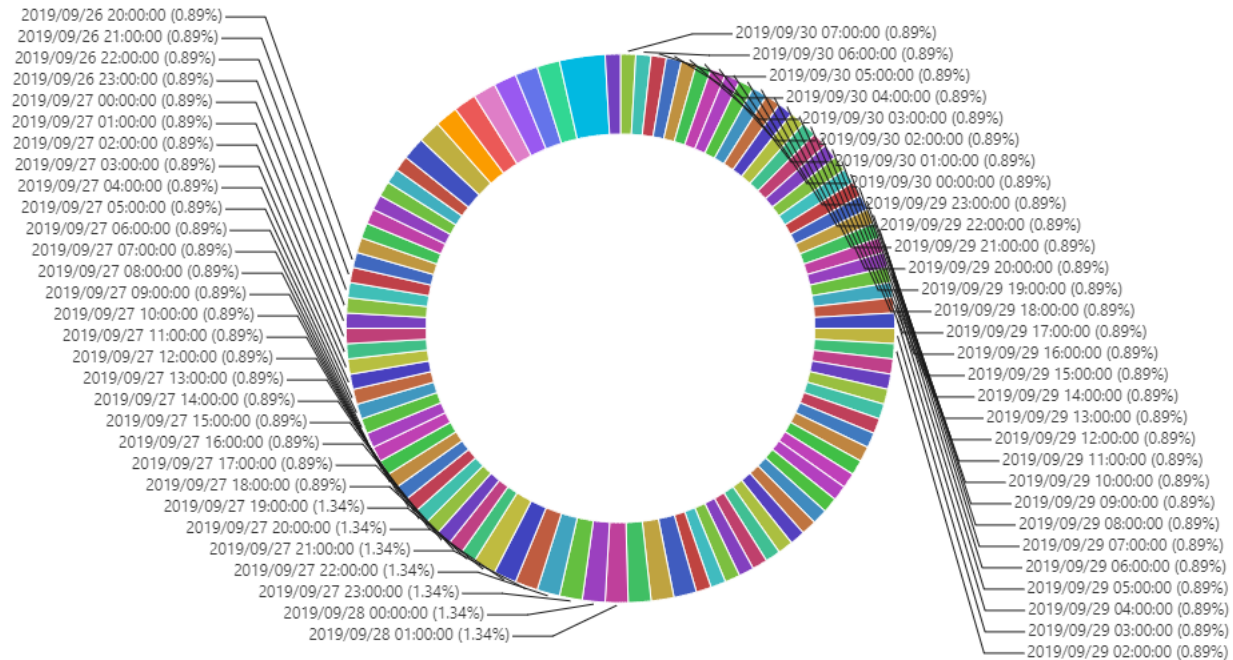
# Analyse - KQL Example

	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



# Analyse - KQL Example

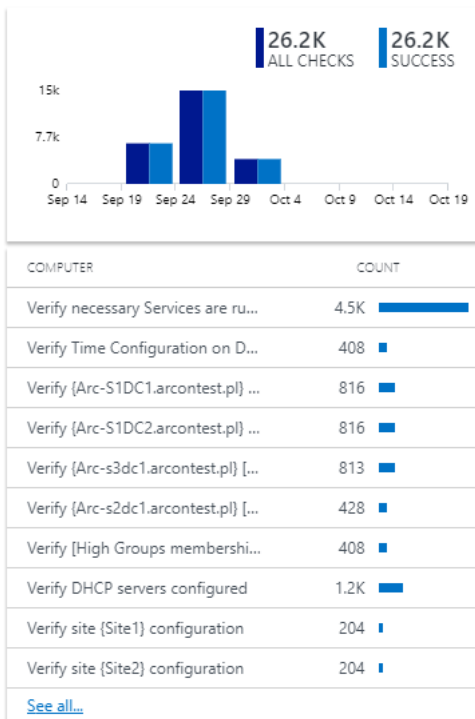


# Visualize – Azure Dashboards

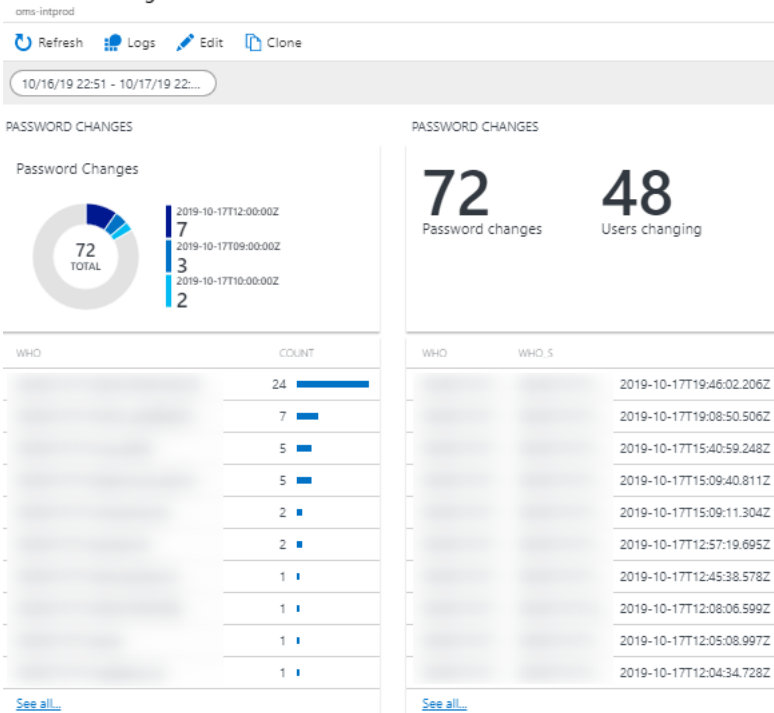


# Visualize – Azure Dashboards

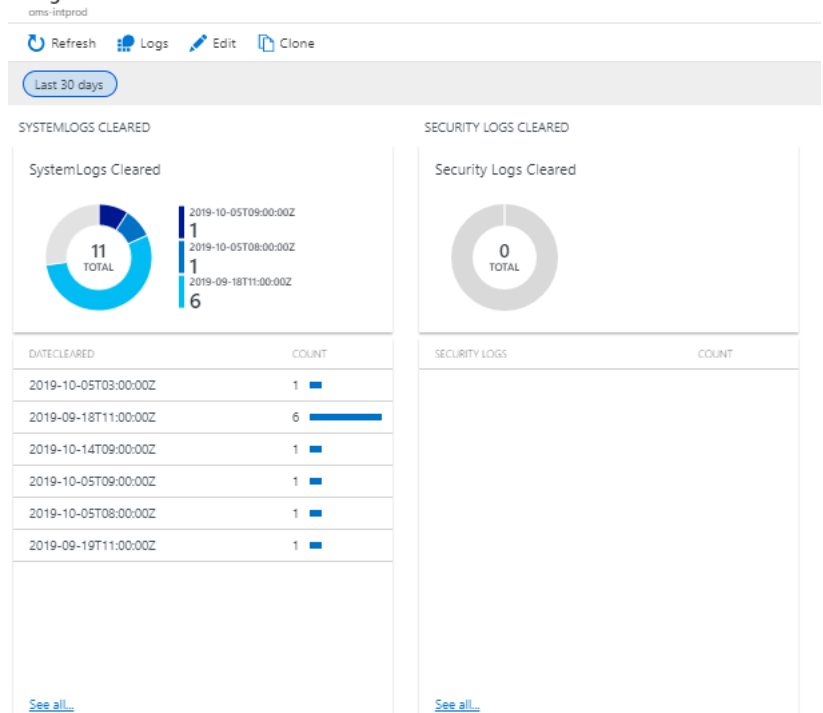
## PCHECKS SUCCESS



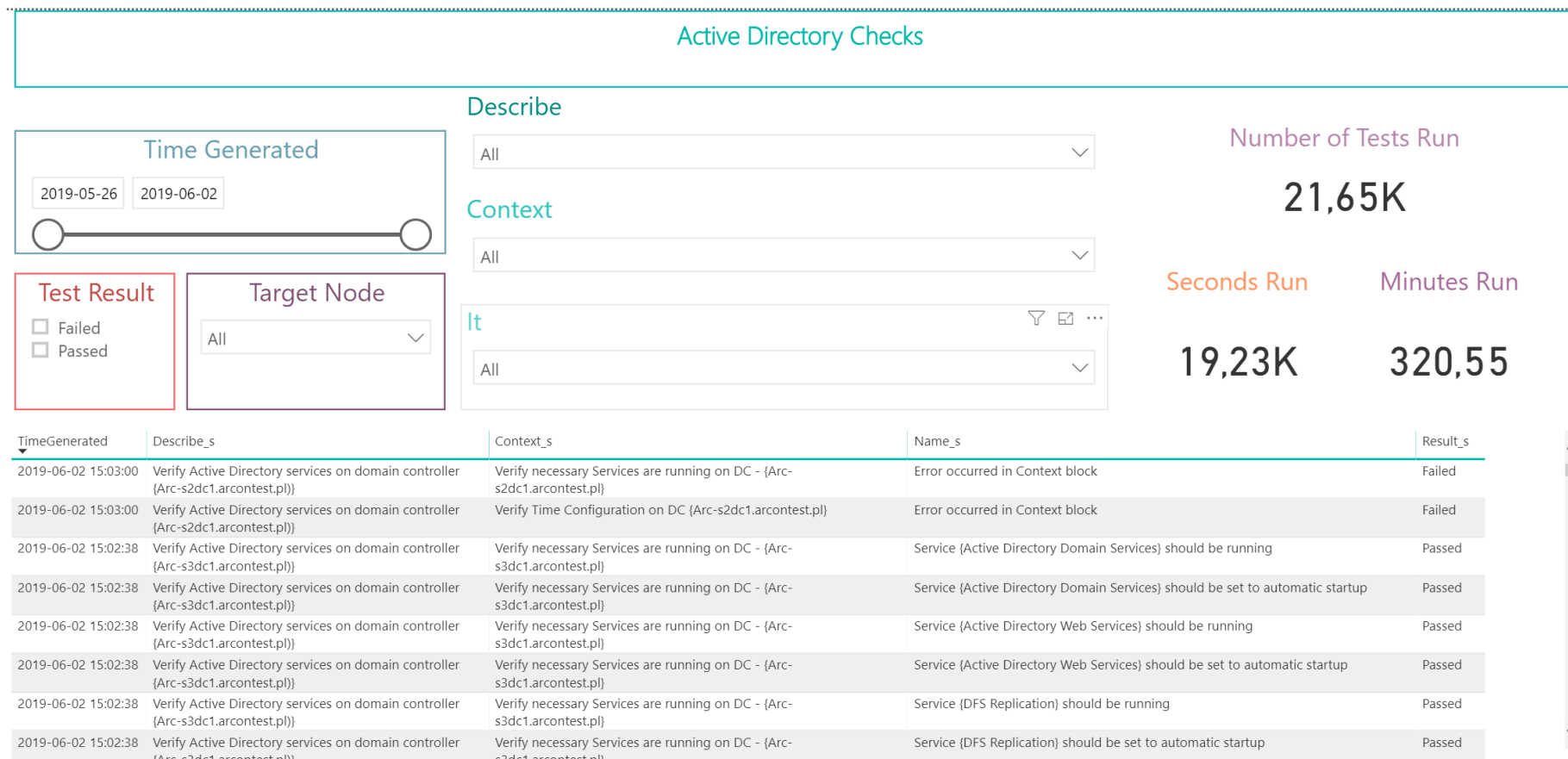
## Password changes



## Logs Cleared



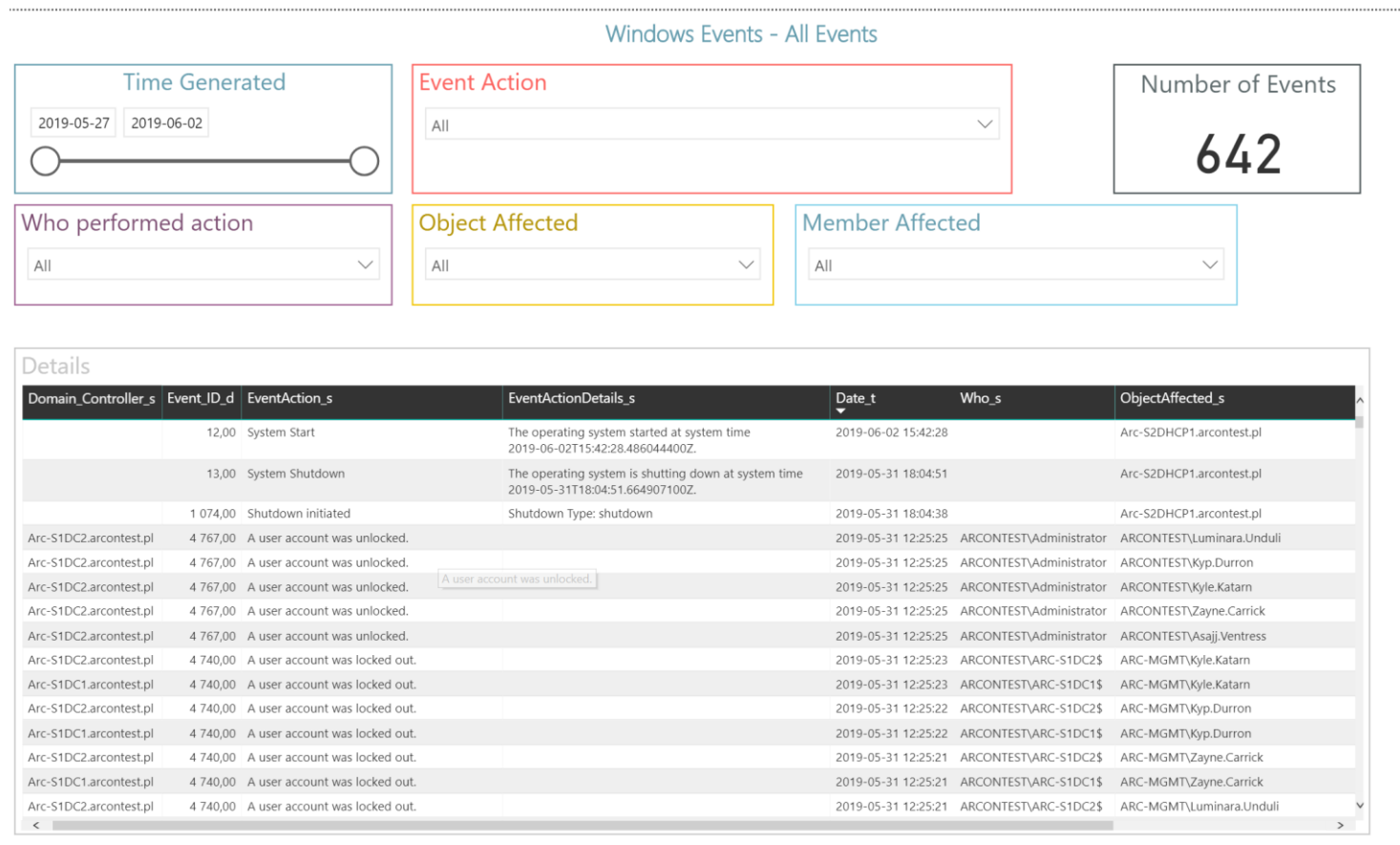
# Visualize – Power BI



<https://github.com/mczerniawski/pChecksAD>



# Visualize – Power BI



<https://github.com/mczerniawski/WEFTools>

# Alerts

---

Alert is based on:

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

# Almost there



# 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

---

```
$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

---

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
```

# Demo

---

- Create workspace
- Send logs
- Get logs

With PowerShell

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

# Demo

---





# Pricing

---



# 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

$10 * 30\text{MB} = 300\text{MB/day} = 9\text{GB a month}$

$9\text{GB} - 5\text{GB (free)} = 4\text{GB} * € 2,522 = € 10,088 \text{ per month}$

# Pricing - Example

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

## Ingestion

$10 * 30\text{MB} = 300\text{MB/day} = 9\text{GB a month}$

$9\text{GB} - 5\text{GB (free)} = 4\text{GB} * € 2,522 = € 10,088 \text{ per month}$

## Retention

1<sup>st</sup> Month – 9GB - **FREE**

2<sup>nd</sup> Month – 18GB (9GB Free)       $9 * € 0,110$       = € 0,88

3<sup>rd</sup> 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

$10 * 30\text{MB} = 300\text{MB/day} = 9\text{GB a month}$

$9\text{GB} - 5\text{GB (free)} = 4\text{GB} * € 2,522 = € 10,088 \text{ per month}$

## Retention

1<sup>st</sup> Month – 9GB - **FREE**

2<sup>nd</sup> Month – 18GB (9GB Free)       $9 * € 0,110$       = € 0,88

3<sup>rd</sup> Month – 27 GB (9GB free)       $18 * € 0,110$       = € 1,98



**€13 / per month!**

# 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



# 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 🕒 !!

# But it 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



# POWER Shell

---



# Questions

---



# Thank you

---

## [WRO] 17 spotkanie Microsoft Azure User Group Poland we Wrocławiu



# about\_Speaker

---



## Mateusz Czerniawski

Arcontar



[mczerniawski@arcon.net.pl](mailto:mczerniawski@arcon.net.pl)



@Arcontar



[www.mczerniawski.pl](http://www.mczerniawski.pl)



mczerniawski

