

MVP Global Summit

March 29 – April 1, 2021



Microsoft confidential

Everything is confidential unless otherwise stated.



Inclusive Session Guidelines

Please practice these tips while in Summit sessions.

Voice Guidance

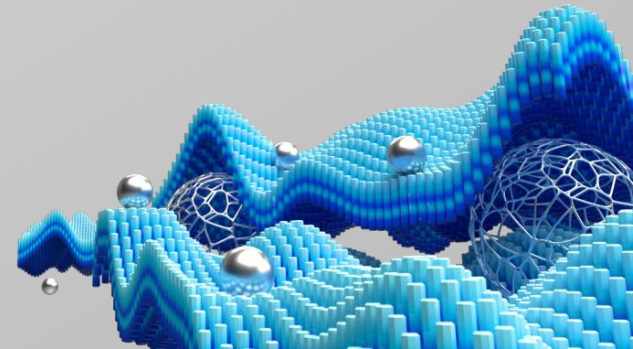
- Raise hand so the moderator can call on you
- State your name when speaking
- Return to mute when not talking

Chat Guidance

- **Q:** to preface questions
- **@mention** to respond to an individual
- Stay on topic
- Use alt-text for images and gifs

Allyship

- Seek to understand, not drive agreement
- Focus on ideas, not people
- Support and amplify peers
- Avoid acronyms



KQL: From Hero to Superhero



Ramiro Calderon

 [@ramirocd](#)



Corissa Koopmans

 [@corissalea](#)

Program Managers | **Microsoft Identity**



Agenda

- Digital Venue
- Walk-through Scenarios and Requirements
- Illustrate the power of KQL to produce insights
- Learnings
- Resources



Digital Venue

Event Requirements

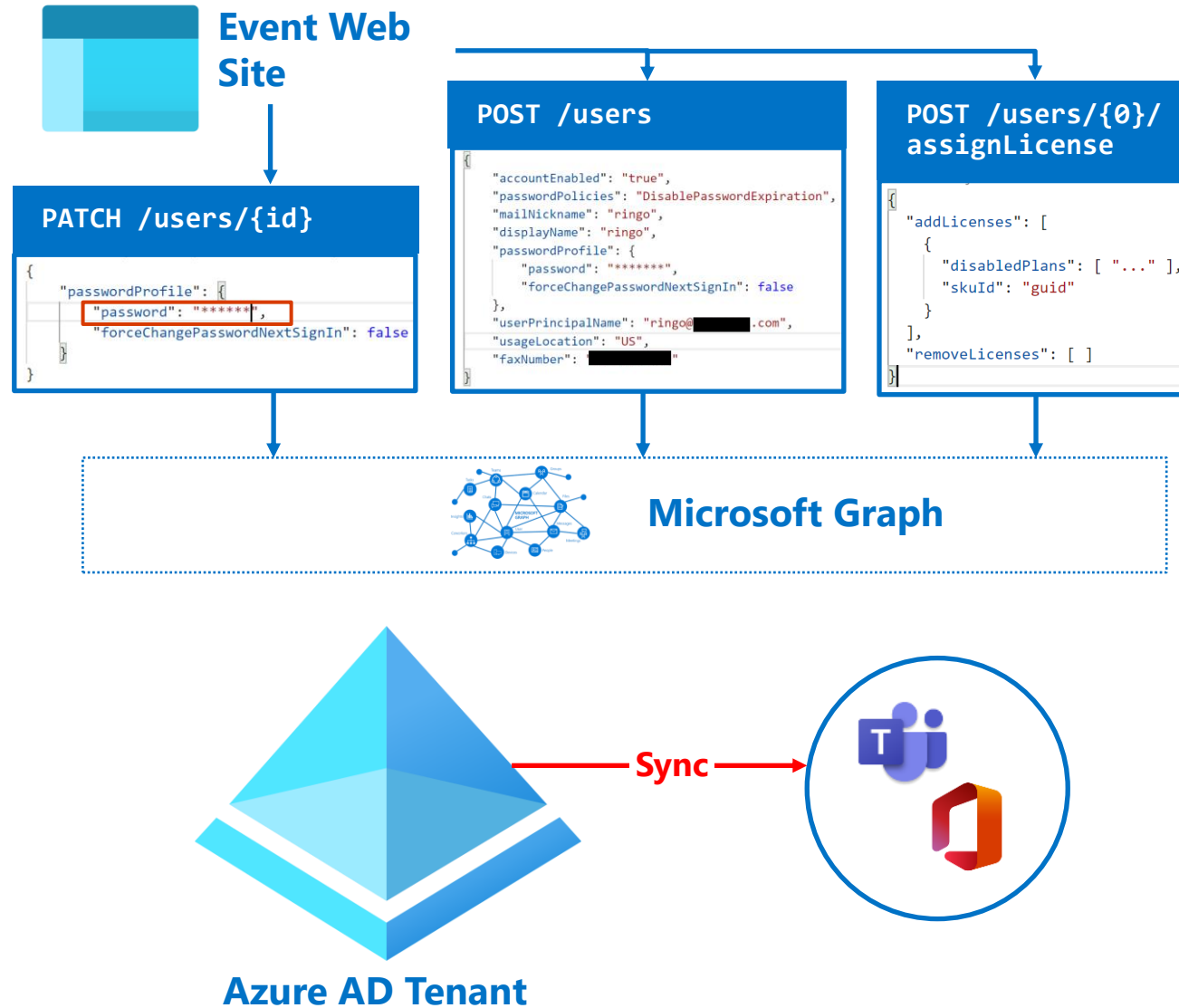
- Users between 1k-1 MM 😊
- Teams Live Events for sessions
- Teams for attendee-to-attendee networking
- Basic usage and attendee reports

Goals for us

- Learn from this to apply in future events



Digital Venue – Technical Design



Scenario: Attendee Registration

Business Questions

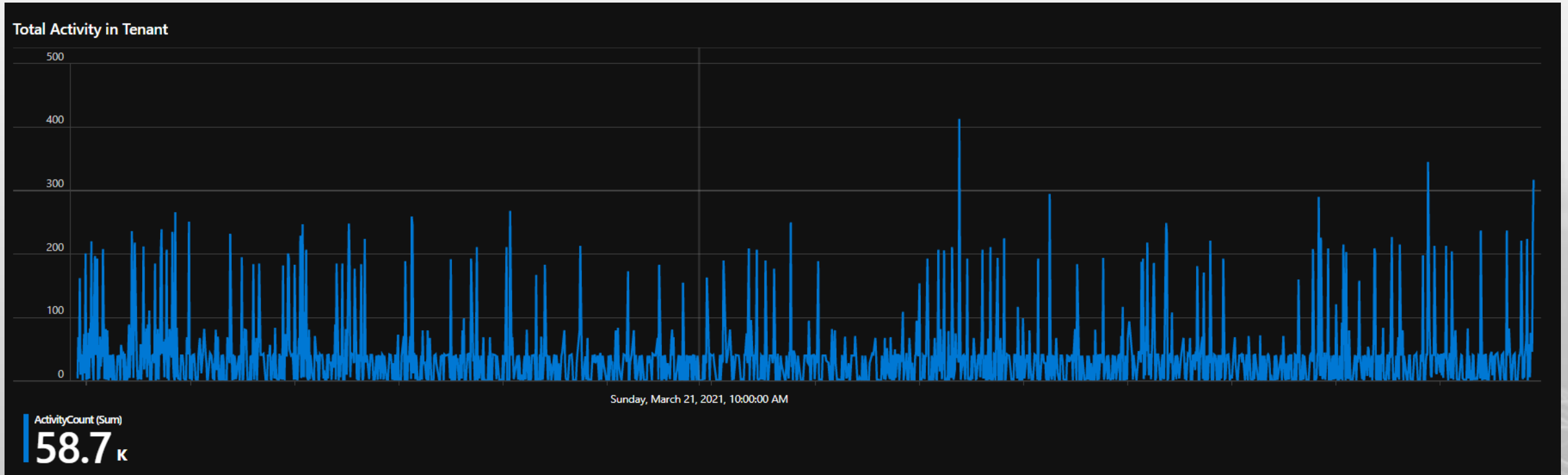
- How many users register before the event?
- Are they succeeding?

Translates to..

- Monitor user provisioning activity before the event
- Measure trends towards [throttling](#)

Limit type	Resource unit quota	Write quota
application+tenant pair	S: 3500, M:5000, L:8000 per 10 seconds	3000 per 2 minutes and 30 seconds
application	150,000 per 20 seconds	70,000 per 5 minutes
tenant	Not Applicable	18,000 per 5 minutes

Activity Count in Tenant



Auditlogs

```
| summarize AggregatedValue = count() by bin(TimeGenerated, 5m)
```

Configure signal logic

Search query * ⓘ

AuditLogs

| where TimeGenerated > ago(5m)

| summarize AggregatedValue = count() by bin(TimeGenerated, 5m)

[View result of query in Azure Monitor - Logs](#)

Query to be executed : *AuditLogs | where TimeGenerated > ago(5m) | summarize AggregatedValue = count() by bin_at(TimeGenerated, 5m, now())*

For time window : *3/26/2021, 4:26 PM - 3/26/2021, 5:26 PM*

ⓘ

It may take in the range of 6 minutes, to have the logs available for provided query [Learn more](#)

Alert logic

Based on ⓘ

Operator ⓘ

Threshold value * ⓘ

Metric measurement

Greater than

4000



engage identity owners

Edit action group

Save changes

Delete action group

This is a summary of your action group. Please review to ensure the information is correct and consider [Azure Alerts Pricing](#) and the [Azure Privacy Statement](#).

Basics

Subscription

Visual Studio Ultimate with MSDN

Resource group

Action group name

Engage Identity Owners

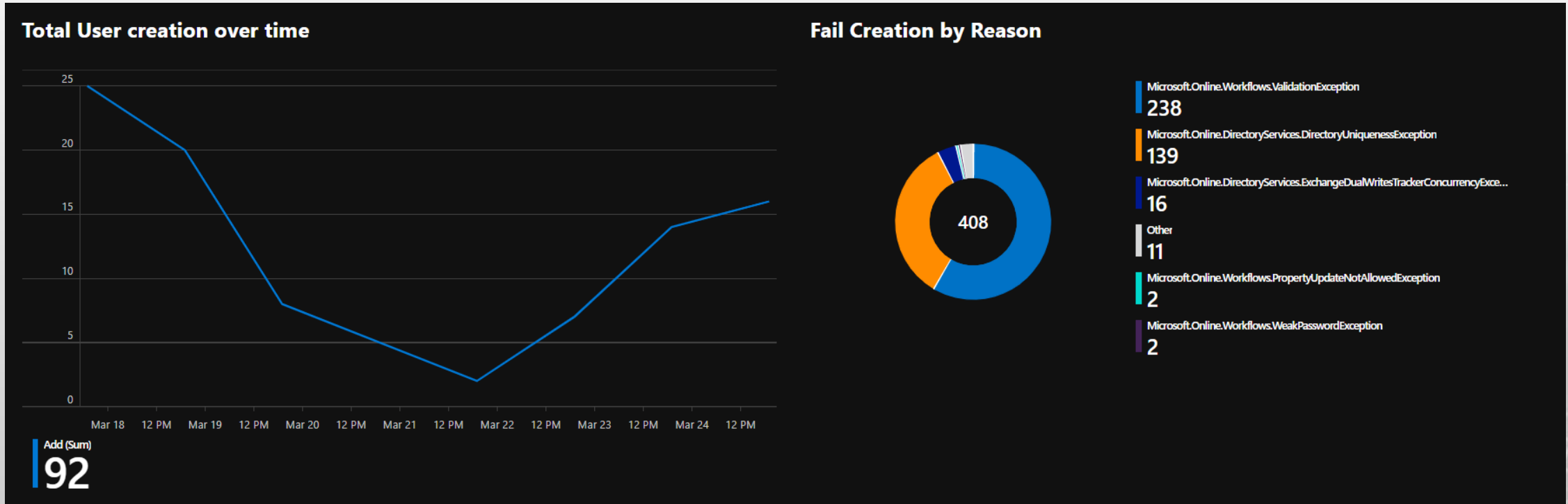
Display name *

pingidowners

Notifications

Notification type	Name	Status	Selected
Email/SMS message/Push/Voice	ramical	Subscribed	Email, SMS message

User Creation and Failed Creation by Reason



AuditLogs

```
| where AADOperationType == "Add"  
| where Category == "UserManagement"  
| where Result == "success"  
| summarize count() by bin (TimeGenerated,1d)
```

AuditLogs

```
| where AADOperationType == "Add" or AADOperationType =  
= "Update"  
| where Category == "UserManagement"  
| where Result == "failure"  
| summarize count() by ResultReason
```

```
AuditLogs  
| distinct AADOperationType, Category
```

Here's
a tip!

Scenario: Password Management

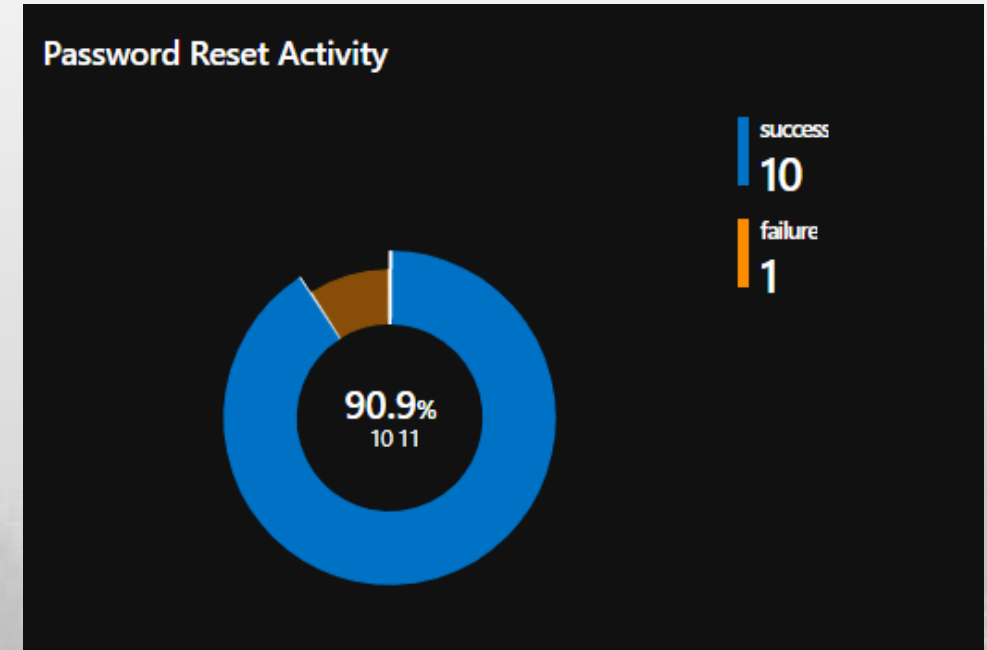
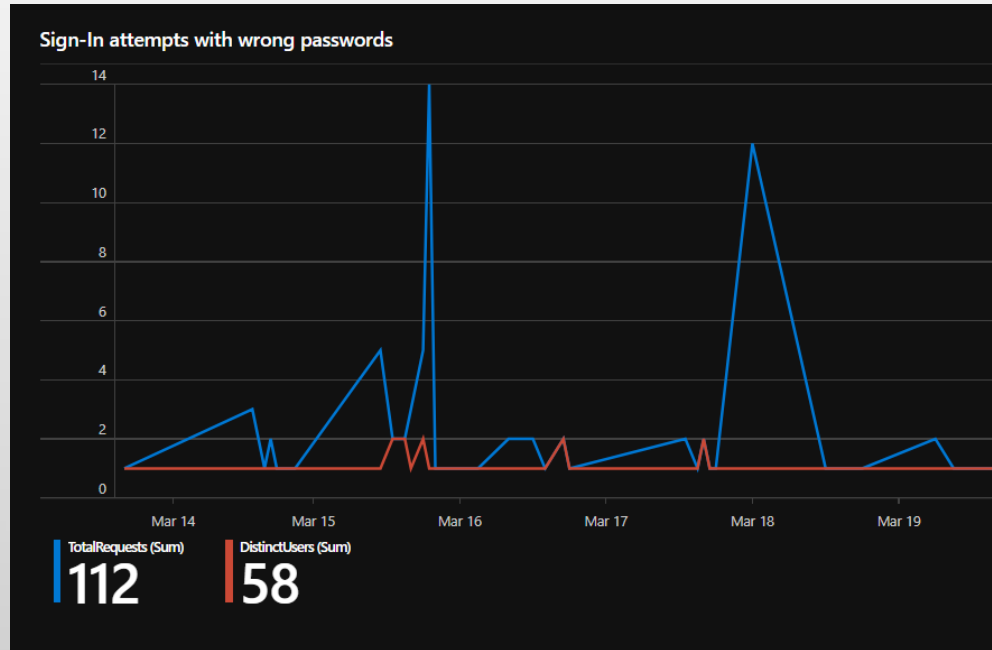
Business Questions

(none, we just saw this from the technical side proactively)

Translates to..

- Monitoring attempts to set weak passwords
- Monitoring people logging in with wrong passwords
- Monitoring people resetting their passwords

Sign-ins w/ Wrong Password and Password Resets



```
SigninLogs
| where ResultType == "50126" //invalid user name or password
| summarize TotalRequests=count(),DistinctUsers=dcount(UserId)
  by bin(TimeGenerated,1h)
```

```
AuditLogs
| where OperationName contains "Reset User Password"
| mv-expand TargetResources
| extend TRParsed = parse_json(TargetResources)
| extend UserId = tostring(TRParsed.id)
| summarize dcount(UserId) by Result
```

Here's
a tip!

```
AuditLogs
| summarize buildschema(TargetResources)
```

Monitoring for weak passwords

ResultReason	Count
Your Workday credentials are invalid. Either the user nam...	46
PasswordPolicyError	15
This run profile is being quarantined because of: Encount...	12
Microsoft.Online.Workflows.IncorrectPasswordException	6
UserIncorrectPassword	5
PasswordDoesnotComplyFuzzyPolicy	5
Microsoft.Online.Workflows.WeakPasswordException	2
FuzzyPolicyViolationInvalidPassword	1
The user selected a password that was automatically ban...	1
PolicyViolationWeakPassword	1
User submitted a password that did not meet the security...	1

AuditLogs

```
| where ResultReason contains "Password"  
| where Result == "failure"  
| mv-expand TargetResources  
| extend TRParsed = parse_json(TargetResources)  
| extend UserId = tostring(TRParsed.id)  
| summarize Count = count() by ResultReason  
| order by Count desc
```

Scenario: Monitor user behavior and experience during the event

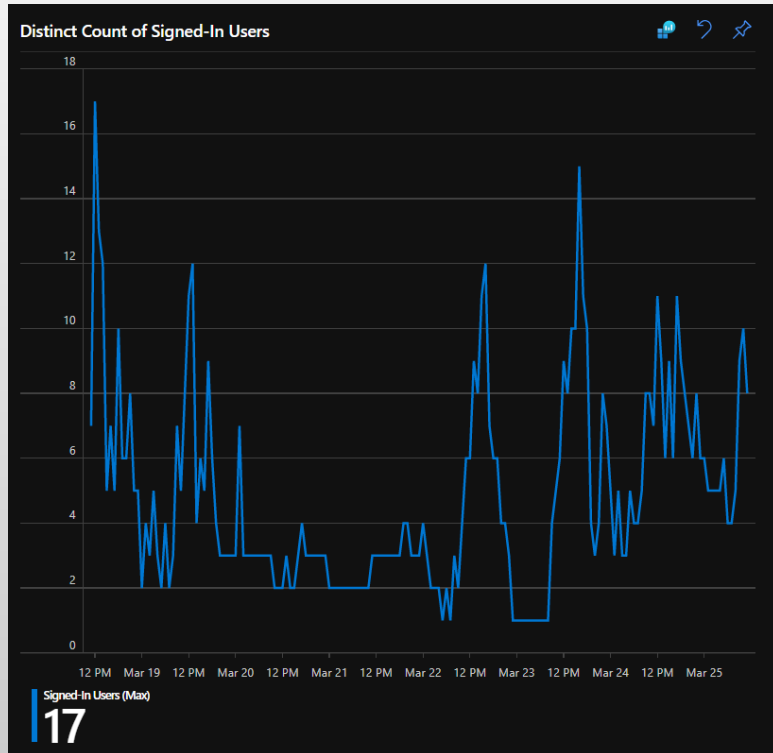
Business Questions:

- Can attendees get into digital venue smoothly?
- Where are the attendees coming from?

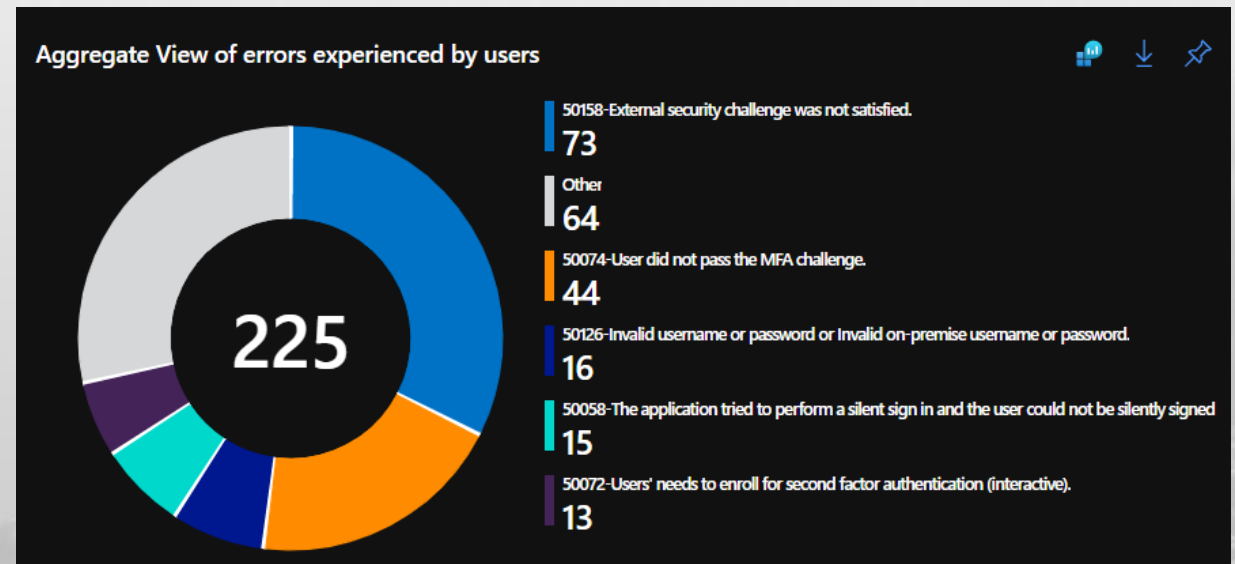
Translates to..

- Monitor provisioning during the event
- Monitor attendee sign in activity and patterns

Distinct Count of Users and Aggregate View of Errors

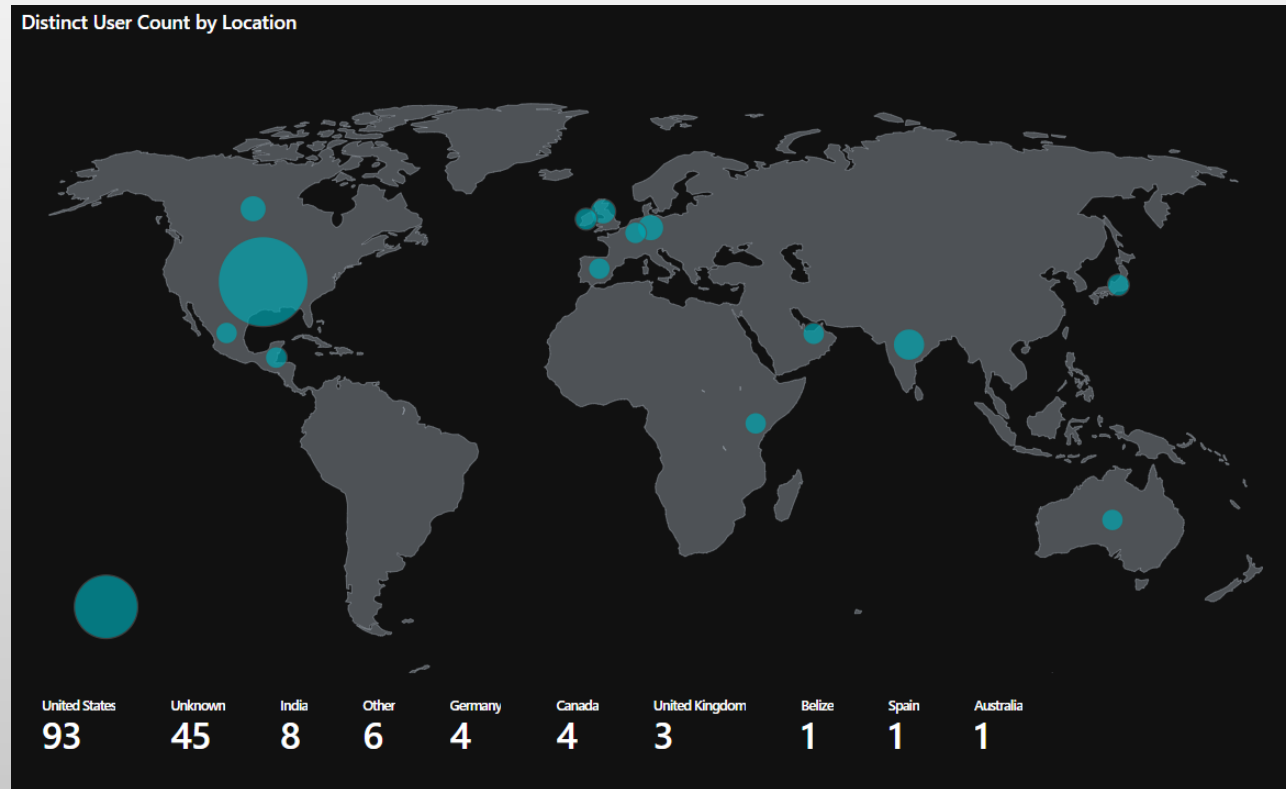


```
SignInLogs  
| summarize distinctUsers=dcount(UserId)  
  by bin(TimeGenerated, 1h)
```



```
SignInLogs  
| where (ResultType != 0) and (ResultType != 50140)  
| extend Description = strcat(ResultType,"-", ResultDescription)  
| summarize DistinctUsers=dcount(UserId) by Description
```

Distinct User Count by Location




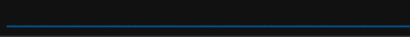

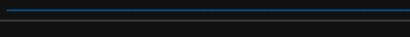


```
SigninLogs
| extend CountryRegion = iff(LocationDetails.countryOrRegion == '', 'Unknown', toString
(LocationDetails.countryOrRegion))
| summarize distinctUsers = dcount(UserId) by CountryRegion
```

Total Sign-Ins by County/Region and City

Total Sign-ins by Country and City

Search

Name	↑↓	Sign-in Count	↑↓	Trend	Failure Count	↑↓	Interrupt Count	↑↓
> US		3.783K			441		0	
> IN		154			68		0	
> Unknown country		144			133		0	
> AU		42			19		0	
> CA		40			22		0	
> GB		25			16		0	
> DE		24			5		0	
> KE		17			9		0	
> MX		6			4		0	
> LU		4			4		0	

Total Sign-ins by Country/Region and City

```

let data = SigninLogs
    //registrationapp
    | extend CountryRegion = iff(LocationDetails.countryOrRegion == '', 'Unknown', toString(LocationDetails.countryOrRegion))
    | extend City = iff(LocationDetails.city == '', 'Unknown city', toString(LocationDetails.city))
    | extend errorCode = Status.errorCode
    | extend SigninStatus = case(errorCode == 0, "Success", errorCode == 50133, "Pending user action", errorCode == 500021, "Pending user action", errorCode == 81012, "Pending user action", "Failure")
    | where SigninStatus == '*' or '*' == '*' or '*' == 'All Sign-ins';
let countryData = data
    | summarize TotalCount = count(), SuccessCount = countif(SigninStatus == "Success"), FailureCount = countif(SigninStatus == "Failure"), InterruptCount = countif(SigninStatus == "Pending user action") by CountryRegion
    | join kind=inner
    (
        data
        | make-series Trend = count() default = 0 on TimeGenerated in range(ago(14d), now(), 6h) by CountryRegion
        | project-away TimeGenerated
    )
    on CountryRegion
    | project CountryRegion, TotalCount, SuccessCount, FailureCount, InterruptCount, Trend
    | order by TotalCount desc, CountryRegion asc;
data
| summarize TotalCount = count(), SuccessCount = countif(SigninStatus == "Success"), FailureCount = countif(SigninStatus == "Failure"), InterruptCount = countif(SigninStatus == "Pending user action") by CountryRegion, Ci
ty
| join kind=inner
(
    data
    | make-series Trend = count() default = 0 on TimeGenerated in range(ago(14d), now(), 6h) by CountryRegion, City
    | project-away TimeGenerated
)
on CountryRegion, City
| order by TotalCount desc, CountryRegion asc
| project CountryRegion, City, TotalCount, SuccessCount, FailureCount, InterruptCount, Trend
| join kind=inner
(
    countryData
)
on CountryRegion
| project Id = City, Name = City, Type = 'City', ['Sign-
in Count'] = TotalCount, Trend, ['Failure Count'] = FailureCount, ['Interrupt Count'] = InterruptCount, ['Success Rate'] = 1.0 * SuccessCount / TotalCount, ParentId = CountryRegion
| union (
    countryData
    | project Id = CountryRegion, Name = CountryRegion, Type = 'Country', ['Sign-
in Count'] = TotalCount, Trend, ['Failure Count'] = FailureCount, ['Interrupt Count'] = InterruptCount, ['Success Rate'] = 1.0 * SuccessCount / TotalCount, ParentId = 'root')
| order by ['Sign-in Count'] desc, Name asc

```

Break it down...

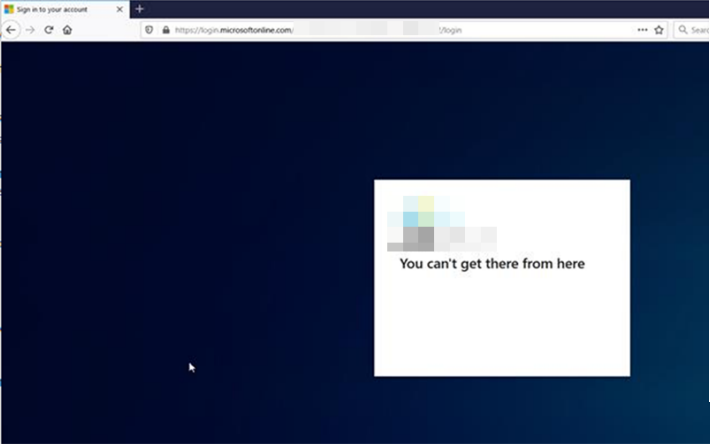
```
let data = SigninLogs
    //registrationapp
    | extend CountryRegion = iff(LocationDetails.countryOrRegion == '', 'Unknown', toString(LocationDetails.countryOrRegion))
    | extend City = iff(LocationDetails.city == '', 'Unknown city', toString(LocationDetails.city))
    | extend errorCode = Status.errorCode
    | extend SigninStatus = case(errorCode == 0, "Success", errorCode == 50133, "Pending user action", errorCode == 500021, "Pending user action", errorCode == 81012, "Pending user action", "Failure")
    | where SigninStatus == '*' or '*' == '*' or '*' == 'All Sign-ins';
let countryData = data
    | summarize TotalCount = count(), SuccessCount = countif(SigninStatus == "Success"), FailureCount = countif(SigninStatus == "Failure"), InterruptCount = countif(SigninStatus == "Pending user action") by CountryRegion
    | join kind=inner
    (
        data
        | make-series Trend = count() default = 0 on TimeGenerated in range(ago(14d), now(), 6h) by CountryRegion
        | project-away TimeGenerated
    )
    on CountryRegion
| project CountryRegion, TotalCount, SuccessCount, FailureCount, InterruptCount, Trend
| order by TotalCount desc, CountryRegion asc;
```

```
data
| summarize TotalCount = count(), SuccessCount = countif(SigninStatus == "Success"), FailureCount = countif(SigninStatus == "Failure"), InterruptCount = countif(SigninStatus == "Pending user action") by CountryRegion, City
| join kind=inner
  (
    data
    | make-series Trend = count() default = 0 on TimeGenerated in range(ago(14d), now(), 6h) by CountryRegion, City
    | project-away TimeGenerated
  )
  on CountryRegion, City
| order by TotalCount desc, CountryRegion asc
| project CountryRegion, City, TotalCount, SuccessCount, FailureCount, InterruptCount, Trend
| join kind=inner
  (
    countryData
  )
  on CountryRegion
| project Id = City, Name = City, Type = 'City', ['Sign-in Count'] = TotalCount, Trend, ['Failure Count'] = FailureCount, ['Interrupt Count'] = InterruptCount, ['Success Rate'] = 1.0 * SuccessCount / TotalCount, ParentId = CountryRegion
| union (
  countryData
  | project Id = CountryRegion, Name = CountryRegion, Type = 'Country', ['Sign-in Count'] = TotalCount, Trend, ['Failure Count'] = FailureCount, ['Interrupt Count'] = InterruptCount, ['Success Rate'] = 1.0 * SuccessCount / TotalCount, ParentId = 'root')
| order by ['Sign-in Count'] desc, Name asc
```

Scenario: Figuring things out on the fly

Hi Ramiro,

Here's the best screenshot we have but we haven't gotten an attendee to tell us detailed steps they got to this point. I'll tag on to this message to get more details from any attendee.



Tenant Restrictions!

Basic info Location Device info Authentication Details Conditional Access

Date (UTC) Request ID Correlation ID Authentication requirement Status Sign-in error code Failure reason

cf6 Request ID Correlation ID Single-Factor Authentication Failure Reason 500021 Access is denied

https://login.microsoftonline.com/error

Error Code: Code..

Submit

Error Code	500021
Message	Access to '{tenant}' tenant is denied.
Remediation	Please contact your IT department.

Scenario: Tenant Restrictions

Business Questions

(they did not know they had a question 😊)

Translates to..

- Find out at scale how big of an issue this is



Data to the rescue

Tenant Restriction Report

Tenant restrictions is a feature in Azure AD that allows enterprises to restrict what tenants are users allowed to authenticate to from their corporate network. This is relevant to this event because we are asking customers to authenticate to this tenant, which is blocked from their network as described above. This customers in Financial Services, Manufacturing and Healthcare.

Total users who have attempted sign-in

23.4k

Number of users who attempt sign in from IPs with Tenant Restrictions

336

Number of users from that list who have never succeeded logging in

246

IP Addressess with Tenant Restrictions

IPAddress	↑↓	FailedUserCount↑↓	FailedRequestCount↑↓
10.10.10.10		1	2
10.10.10.11		1	1

Detailed List of Users Affected

UserPrincipalName	↑↓	FailedRequestCount↑↓	DistinctIPCount↑↓
john.doe@contoso.com		2	1
jane.smith@contoso.com		1	1

Total users who have attempted sign-in

22k

Number of users who attempt sign in from IPs with Tenant Restrictions

315

Number of users from that list who have never succeeded logging in

235

```
let trv1users = SigninLogs
| where ResultType == 500021
| summarize by UserId;
let usersWhoSucceed=SigninLogs
| where (UserId in (trv1users))
| where ResultType == 0
| summarize by UserId;
let totaluserSummary = SigninLogs | summarize Stage = "Total users who have attempted sign-
in", DistinctUsers=dcount(UserId);
let trv1userSummary = trv1users | summarize Stage = "Number of users who attempt sign in from IPs wit
h Tenant Restrictions", DistinctUsers=dcount(UserId);
let usersWhoNeverSucceeded = SigninLogs
| where (ResultType == 500021) and (UserId !in (usersWhoSucceed))
| summarize Stage = "Number of users from that list who have never succeeded logging in", DistinctUser
s=dcount(UserId);
union totaluserSummary, trv1userSummary, usersWhoNeverSucceeded
| sort by DistinctUsers desc
```

IP Addressess with Tenant Restrictions

IPAddress	↑↓	FailedUserCount↑↓	FailedRequestCount↑↓
[REDACTED]		1	2
[REDACTED]		1	1

```
let trv1users = SigninLogs
| where ResultType == 500021
| summarize by UserId;
let usersWhoSucceed=SigninLogs
| where (UserId has_any (trv1users))
| where ResultType==0
| summarize by UserId;
SigninLogs
| where (ResultType == 500021) and (UserId !in (usersWhoSucceed))
| summarize FailedUserCount=dcount(UserId),FailedRequestCount=count() by IPAddress
| order by FailedUserCount desc;
```

Detailed List of Users Affected

UserPrincipalName	↑↓	FailedRequestCount↑↓	DistinctIPCount↑↓
[REDACTED]		2	1
[REDACTED]		1	1

```
let trv1users = SigninLogs
| where ResultType == 500021
| summarize by UserId;
let usersWhoSucceed=SigninLogs
| where (UserId has_any (trv1users))
| where ResultType==0
| summarize by UserId;
SigninLogs
| where (ResultType == 500021) and (UserId !in (usersWhoSucceed))
| summarize FailedRequestCount=count(), DistinctIPCount=dcount(IPAddress) by UserPrincipalName;
```

Meta-Learnings

- Simplicity is Key: Trend over time, failure categories, non-aggregated info for investigation
- Technical Insight != Business Insight
- Think through what you want to do before starting to query
- Follow your instincts – if something seems off, it probably is!
- Take advantage of the Public Workbooks – it is a great place to start
- Make this data proactive by setting up Alerts
- Consider your data retention!

KQL Resources

- Workbooks from this talk - <https://aka.ms/KQLHero>
- [Advanced KQL Pluralsight course](#)
- [Become a KQL Ninja \(security-tzu.com\)](https://security-tzu.com)
- [Sign-in log schema](#)
- [Audit log schema in Azure Monitor](#)
- [Log Analytics Tutorial](#)
- [Create and share dashboards of Azure Log Analytics data - Azure Monitor | Microsoft Docs](#)

Share your Workbook ideas!!

- [Azure AD Workbooks · Microsoft Discussions \(github.com\)](#)

Please provide your feedback!

Your opinion is very important to us

- Please share your feedback on this session by completing a session survey

Thank you in advance for your time.

