INTEGRATE 2022

Brought you by

BIZTALK360 | SERVERLESS360 Azure Management Platform

Toon Vanhoutte

CTO **Noest** | Founder **Your Azure Coach**

My 10 favorite Azure API Management tips and tricks!

Platinum

codit | QUIBIQ POWER OF INTEGRATION

Gold

affinus REPLY CLUSTER

DEKIRU SOLUTIONS

Technology Partner

Microsoft

Who am I ?

Toon Vanhoutte

CTO @ NOEST

Founder @ YOUR AZURE COACH

MVP Microsoft® Most Valuable Professional

#10

Go to www.menti.com

Code: 59 91 12

#1

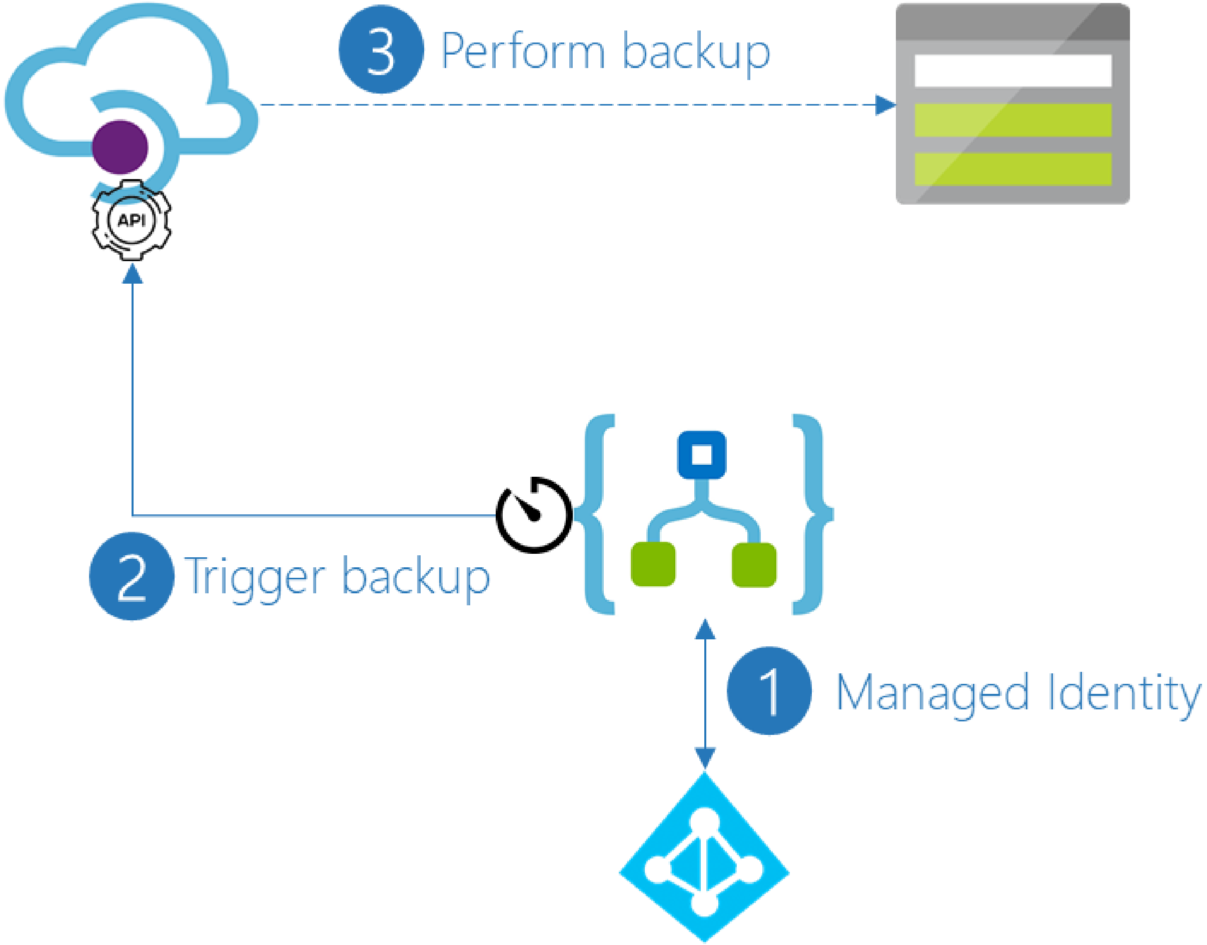
Go to www.menti.com

Code: 59 91 12

Nightly backups

- Yes, it’s possible in API Management!
- Some limitations:
  - A backup or restore operation takes about 10-15 minutes
  - You can only restore backups within the same tier
  - Backups expire after 30 days
  - Backup functionality is not available in the consumption tier
  - You get an API; you must do the plumbing yourself

Nightly backups



NOEST YOUR AZURE COACH

#2

Go to www.menti.com
Code: 59 91 12

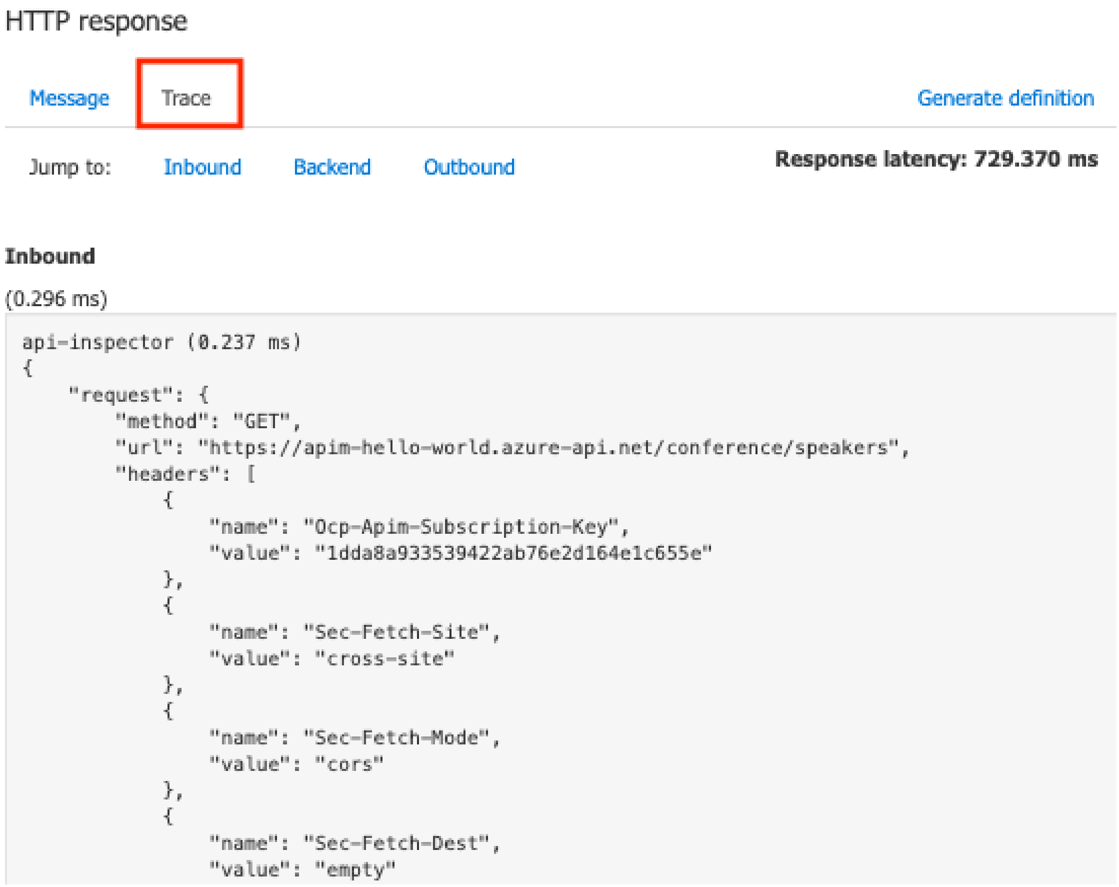
Expose your Open API Definition

- The options are:
    - Download from the Azure Portal
    - Export from the Developer Portal
    - Dynamically expose your Open API Specification
        - Think about security

#3

API Inspector traces

- What are these?



HTTP response

Response latency: 729.370 ms

Inbound

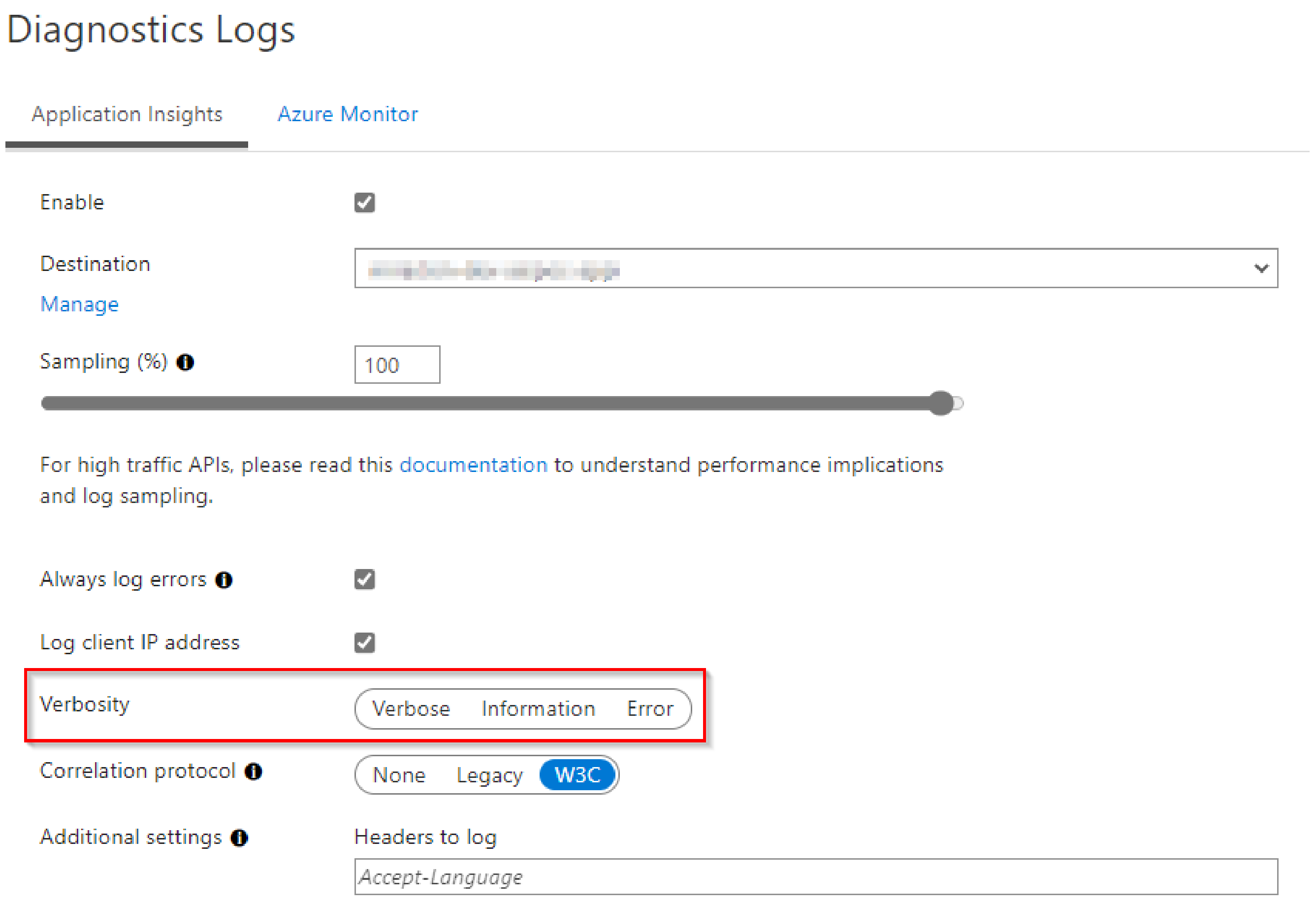
(0.296 ms)

```
api-inspector (0.237 ms)
{
    "request": {
        "method": "GET",
        "url": "https://apim-hello-world.azure-api.net/conference/speakers",
        "headers": [
            {
                "name": "Ocp-Apim-Subscription-Key",
                "value": "1dda8a933539422ab76e2d164e1c655e"
            },
            {
                "name": "Sec-Fetch-Site",
                "value": "cross-site"
            },
            {
                "name": "Sec-Fetch-Mode",
                "value": "cors"
            },
            {
                "name": "Sec-Fetch-Dest",
                "value": "empty"
```

Go to www.menti.com
Code: 59 91 12

API Inspector traces to App Insights

- Set App Insights verbosity to *debug*



Diagnostics Logs

Application Insights | Azure Monitor

Enable ☑

Destination [redacted]

Manage

Sampling (%) 100

For high traffic APIs, please read this documentation to understand performance implications and log sampling.

Always log errors ☑

Log client IP address ☑

Verbosity: Verbose Information Error

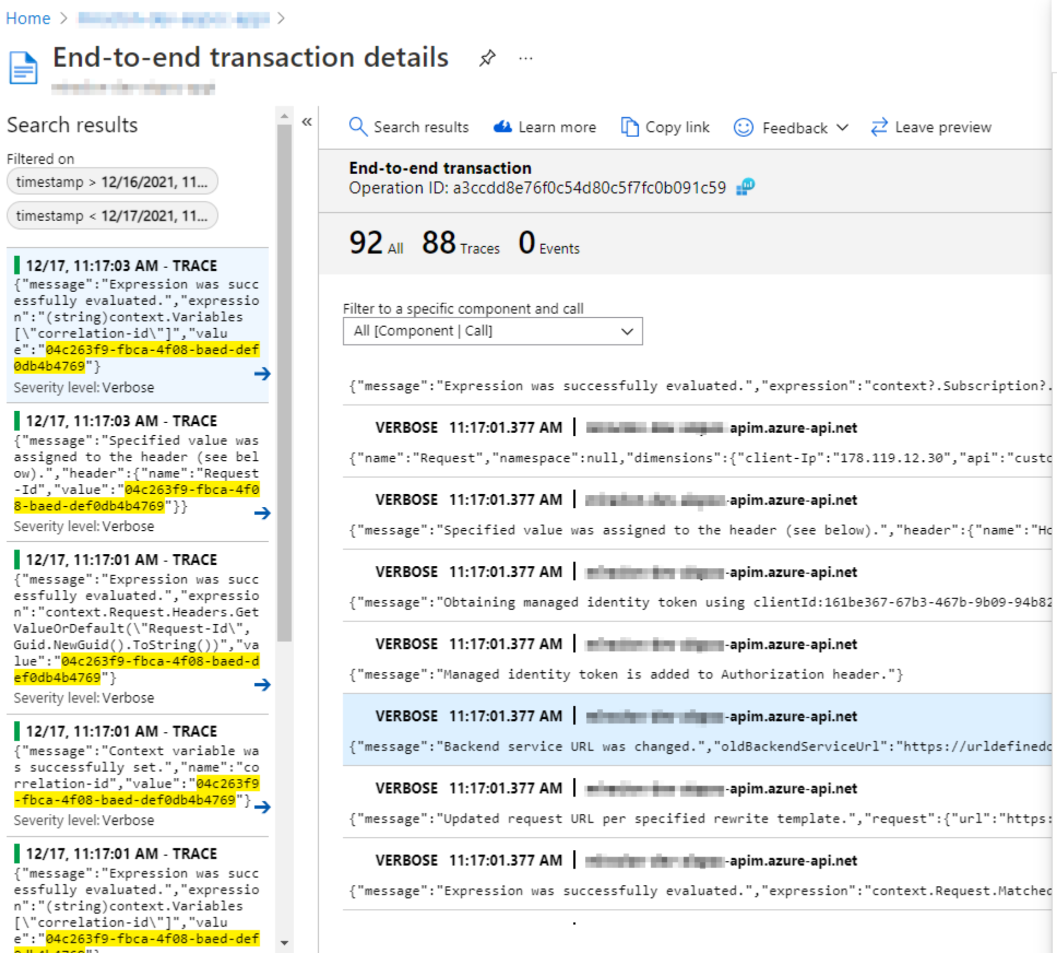
Correlation protocol: None Legacy [✓ W3C]

Additional settings: Headers to log

Accept-Language

API Inspector traces to App Insights

Enjoy the result!



Home > [redacted] >

End-to-end transaction details

[redacted]

Search results

Filtered on

timestamp > 12/16/2021, 11...

timestamp < 12/17/2021, 11...

12/17, 11:17:03 AM - TRACE

```
{"message":"Expression was successfully evaluated.","expression":"(string)context.Variables[\"correlation-id\"]","value":"04c263f9-fbca-4f08-baed-def0db4b4769"}
```

Severity level: Verbose

12/17, 11:17:03 AM - TRACE

```
{"message":"Specified value was assigned to the header (see below).","header":{"name":"Request-Id","value":"04c263f9-fbca-4f08-baed-def0db4b4769"}}
```

Severity level: Verbose

12/17, 11:17:01 AM - TRACE

```
{"message":"Expression was successfully evaluated.","expression":"context.Request.Headers.GetValueOrDefault(\"Request-Id\", Guid.NewGuid().ToString())","value":"04c263f9-fbca-4f08-baed-def0db4b4769"}
```

Severity level: Verbose

12/17, 11:17:01 AM - TRACE

```
{"message":"Context variable was successfully set.","name":"correlation-id","value":"04c263f9-fbca-4f08-baed-def0db4b4769"}
```

Severity level: Verbose

12/17, 11:17:01 AM - TRACE

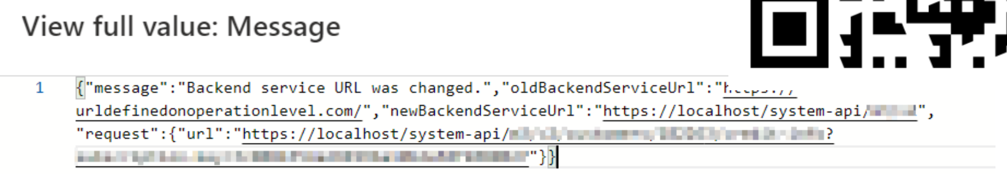
```
{"message":"Expression was successfully evaluated.","expression":"(string)context.Variables[\"correlation-id\"]","value":"04c263f9-fbca-4f08-baed-def
```

End-to-end transaction
Operation ID: a3ccdd8e76f0c54d80c5f7fc0b091c59

92 All 88 Traces 0 Events

Filter to a specific component and call: All [Component | Call]

```
{"message":"Expression was successfully evaluated.","expression":"context?.Subscription?.
VERBOSE 11:17:01.377 AM | [redacted]apim.azure-api.net
{"name":"Request","namespace":null,"dimensions":{"client-Ip":"178.119.12.30","api":"custo
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Specified value was assigned to the header (see below).","header":{"name":"He
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Obtaining managed identity token using clientId:161be367-67b3-467b-9b09-94b82
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Managed identity token is added to Authorization header."}
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Backend service URL was changed.","oldBackendServiceUrl":"https://urldefinedc
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Updated request URL per specified rewrite template.","request":{"url":"https:
VERBOSE 11:17:01.377 AM | [redacted]-apim.azure-api.net
{"message":"Expression was successfully evaluated.","expression":"context.Request.Matchec
```



View full value: Message

```
{"message":"Backend service URL was changed.","oldBackendServiceUrl":"https://
urldefinedonoperationlevel.com/","newBackendServiceUrl":"https://localhost/system-api/[redacted]",
"request":{"url":"https://localhost/system-api/[redacted]?
[redacted]"}}
```

#4

Hide stack traces

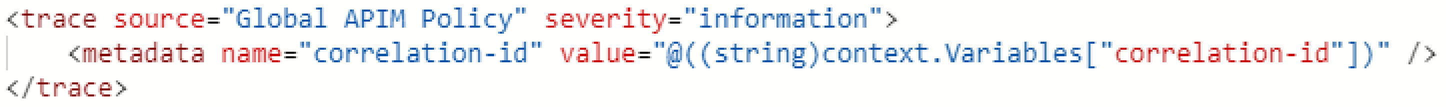
- Tradeoff

Security
Usability

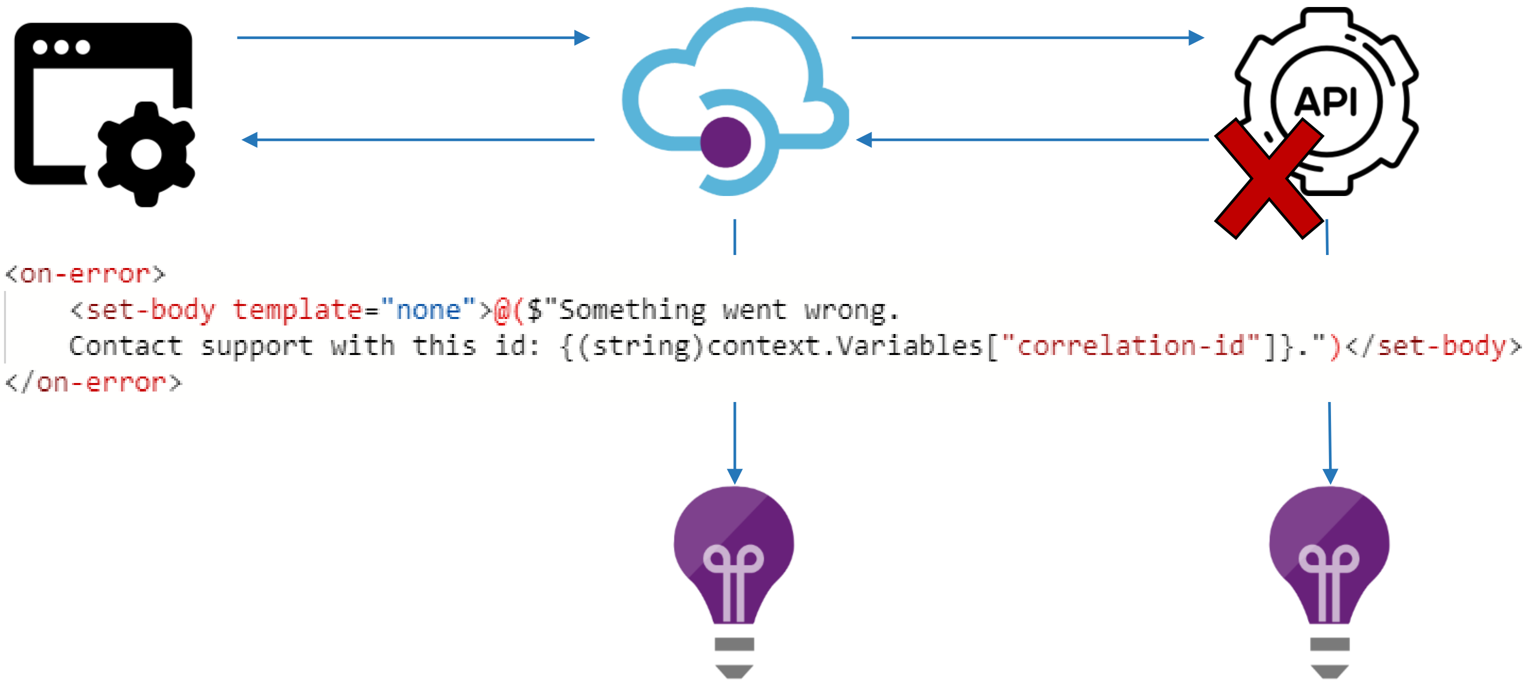
Go to www.menti.com
Code: 59 91 12

Optimally hide stack traces

- Trace correlation Id in App Insights
- Include Id in generic error message



```
<trace source="Global APIM Policy" severity="information">
    <metadata name="correlation-id" value="@((string)context.Variables["correlation-id"])" />
</trace>
```



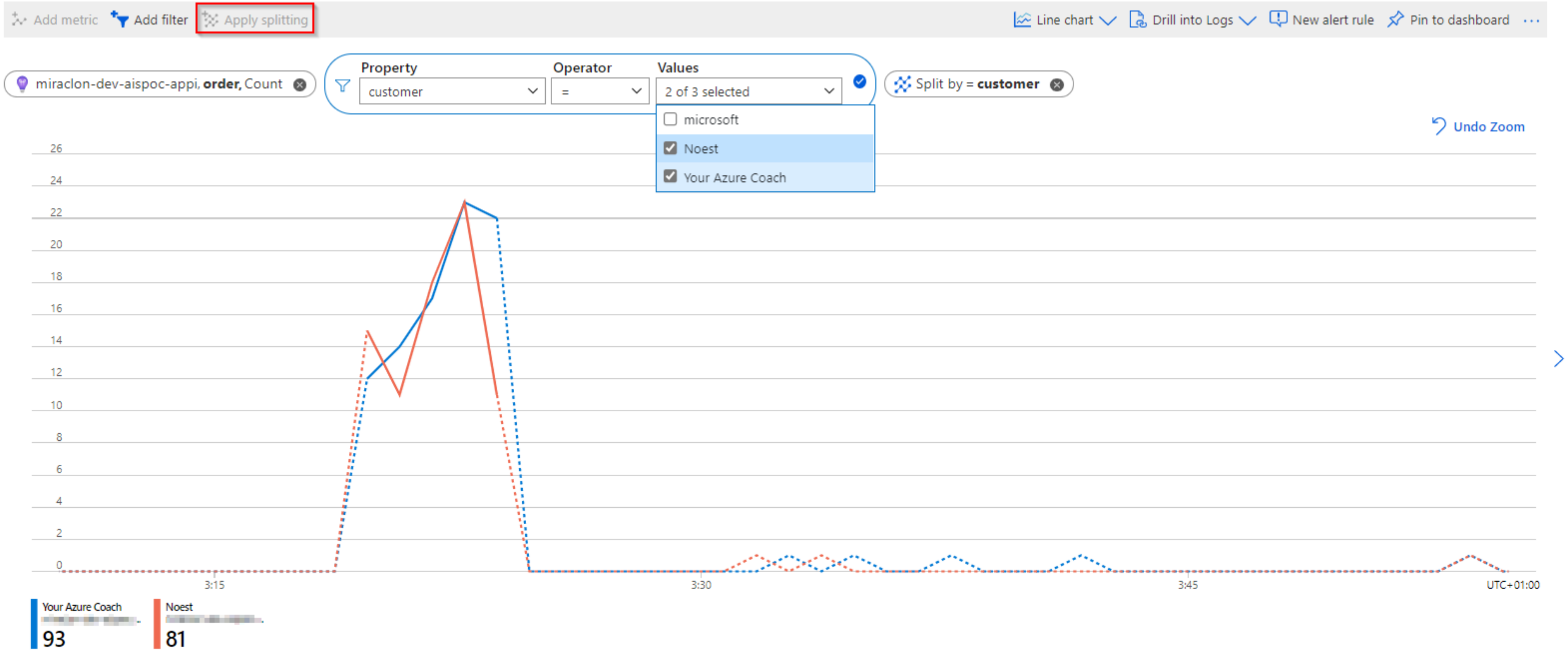
```
<on-error>
    <set-body template="none">@($"Something went wrong.
    Contact support with this id: {(string)context.Variables["correlation-id"]}.")</set-body>
</on-error>
```

#5

Go to www.menti.com
Code: 59 91 12

Emit custom metrics from APIM

- There is a policy!
  - Multi-dimensional metrics within a custom namespace
  - Can be easily integrated with Power BI



miraclon-dev-aispoc-appi, **order**, Count

Property: customer

Operator: =

Values: 2 of 3 selected

☐ microsoft

☑ Noest

☑ Your Azure Coach

Split by = **customer**

Your Azure Coach [redacted] 93

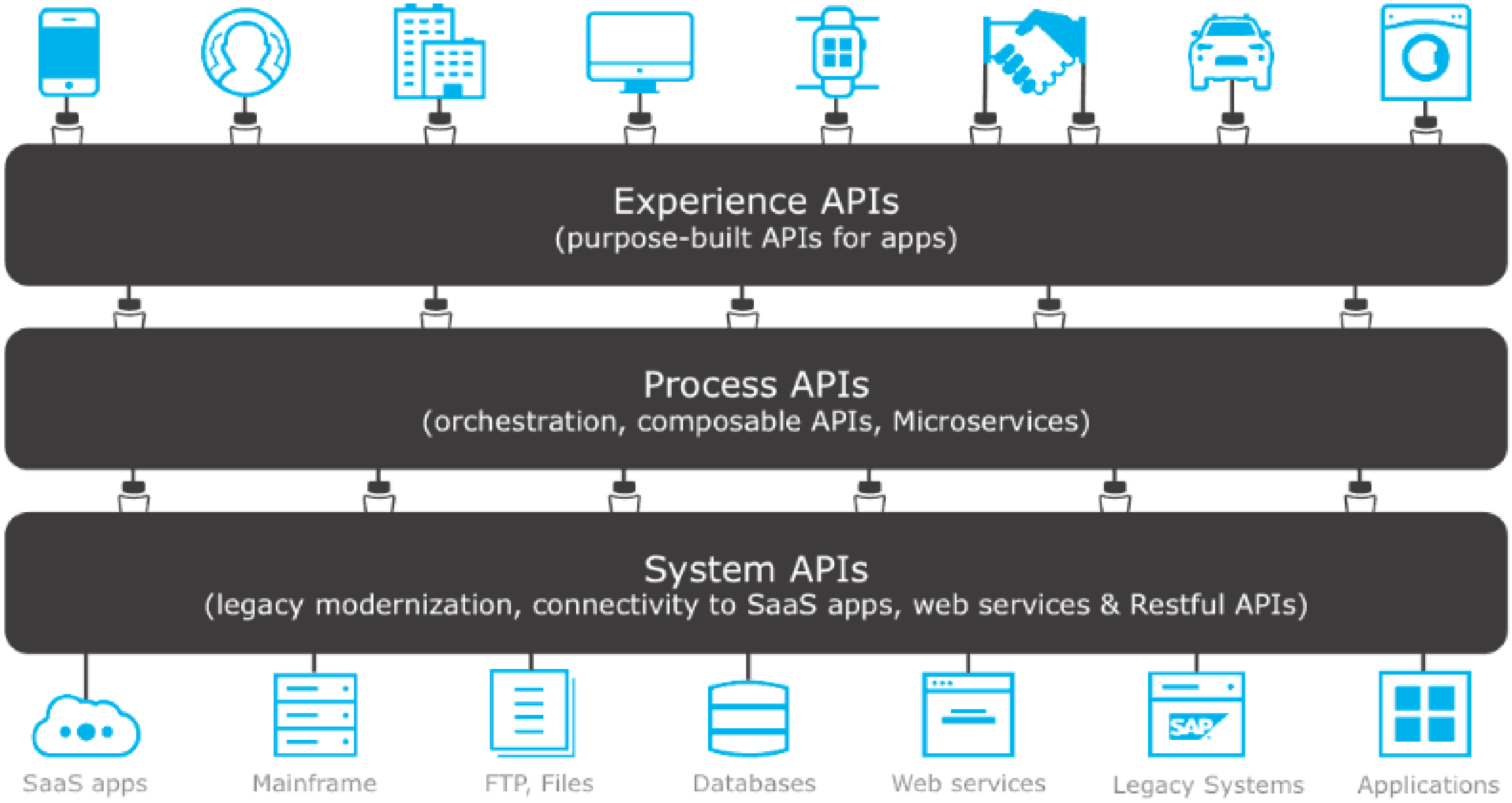
Noest [redacted] 81

NOEST

YOUR AZURE COACH

#6

Layered API Design



Experience APIs
(purpose-built APIs for apps)

Process APIs
(orchestration, composable APIs, Microservices)

System APIs
(legacy modernization, connectivity to SaaS apps, web services & Restful APIs)

SaaS apps

Mainframe

FTP, Files

Databases

Web services

Legacy Systems

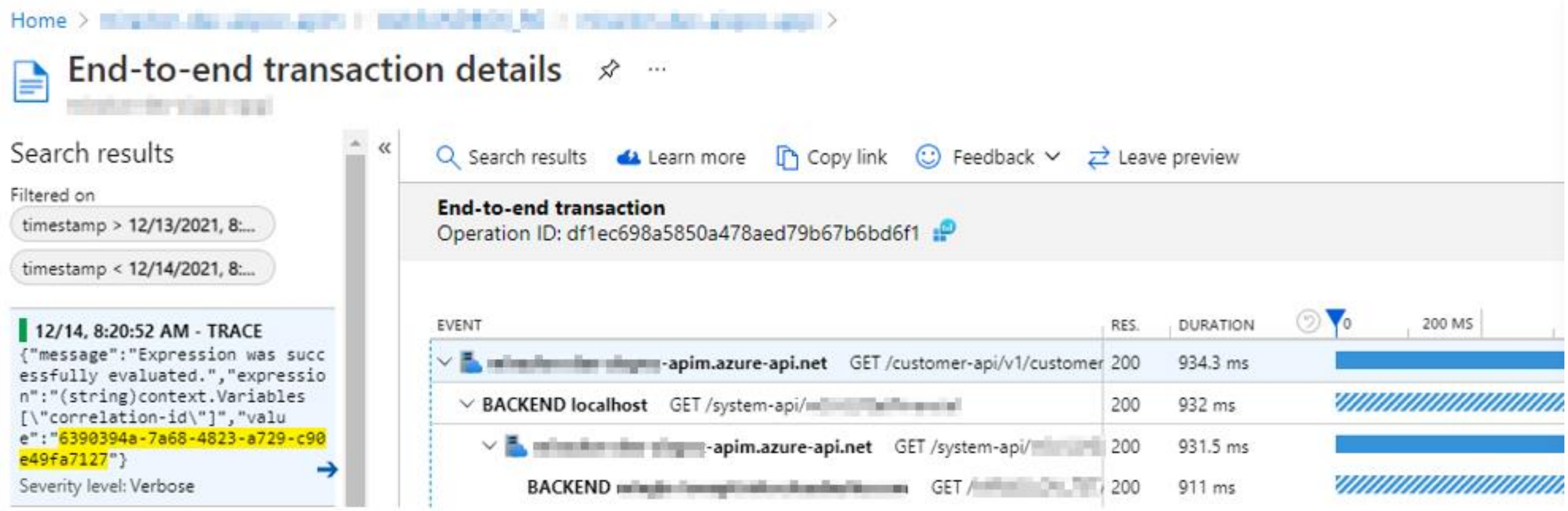
Applications

Go to www.menti.com

Code: 59 91 12

Layered API Design

- Internal routing
  - You can route via https://localhost/…



Home > [redacted] | [redacted] > [redacted] >

End-to-end transaction details

[redacted]

Search results

Filtered on

timestamp > 12/13/2021, 8:...

timestamp < 12/14/2021, 8:...

12/14, 8:20:52 AM - TRACE

```
{"message":"Expression was succ
essfully evaluated.","expressio
n":"(string)context.Variables
[\"correlation-id\"]","valu
e":"6390394a-7a68-4823-a729-c90
e49fa7127"}
```

Severity level: Verbose

End-to-end transaction

Operation ID: df1ec698a5850a478aed79b67b6bd6f1

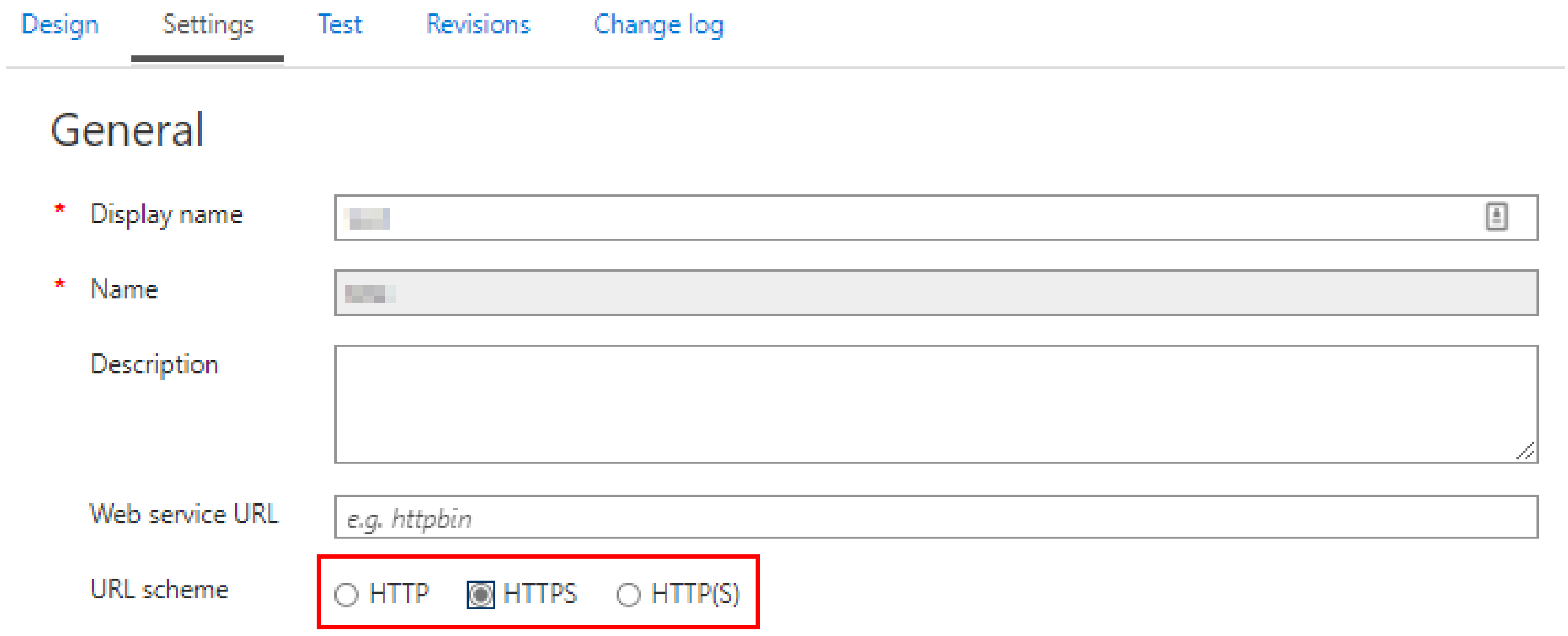
EVENT		RES.	DURATION
[redacted]-apim.azure-api.net	GET /customer-api/v1/customer	200	934.3 ms
BACKEND localhost	GET /system-api/[redacted]	200	932 ms
[redacted]-apim.azure-api.net	GET /system-api/[redacted]	200	931.5 ms
BACKEND [redacted]	GET /[redacted]	200	911 ms

NOEST YOUR AZURE COACH

#7

HTTP or HTTPS?

- Configurable on each API



General

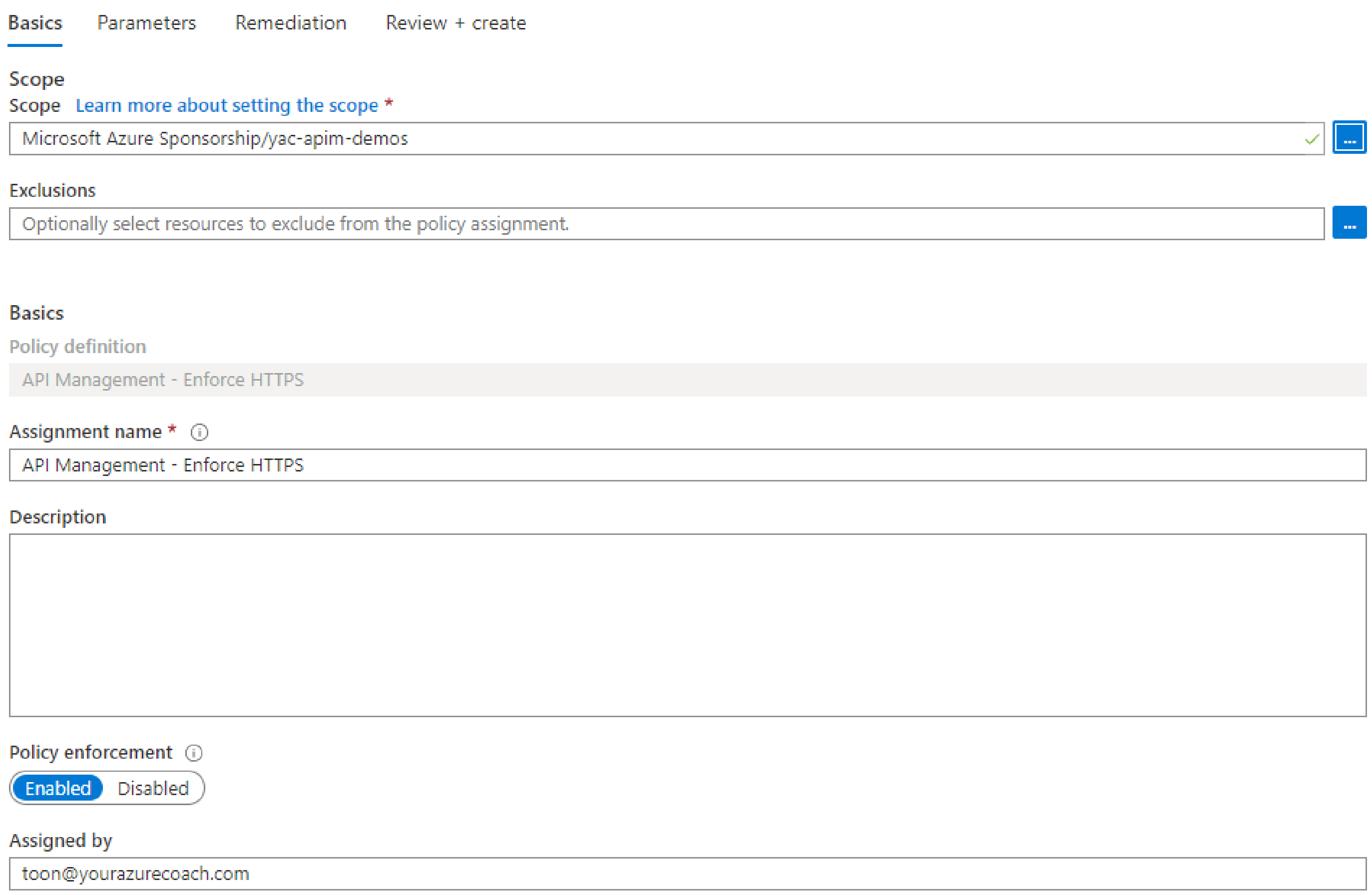
* Display name	[redacted]
* Name	[redacted]
Description	
Web service URL	*e.g. httpbin*
URL scheme	○ HTTP ● HTTPS ○ HTTP(S)

Go to www.menti.com

Code: 59 91 12

Enforce HTTPS with Azure Policy

- You can write a custom Azure policy



Scope

Scope Learn more about setting the scope *

Microsoft Azure Sponsorship/yac-apim-demos ✓

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

API Management - Enforce HTTPS

Assignment name *

API Management - Enforce HTTPS

Description

Policy enforcement

[✓ Enabled] Disabled

Assigned by

toon@yourazurecoach.com

#8

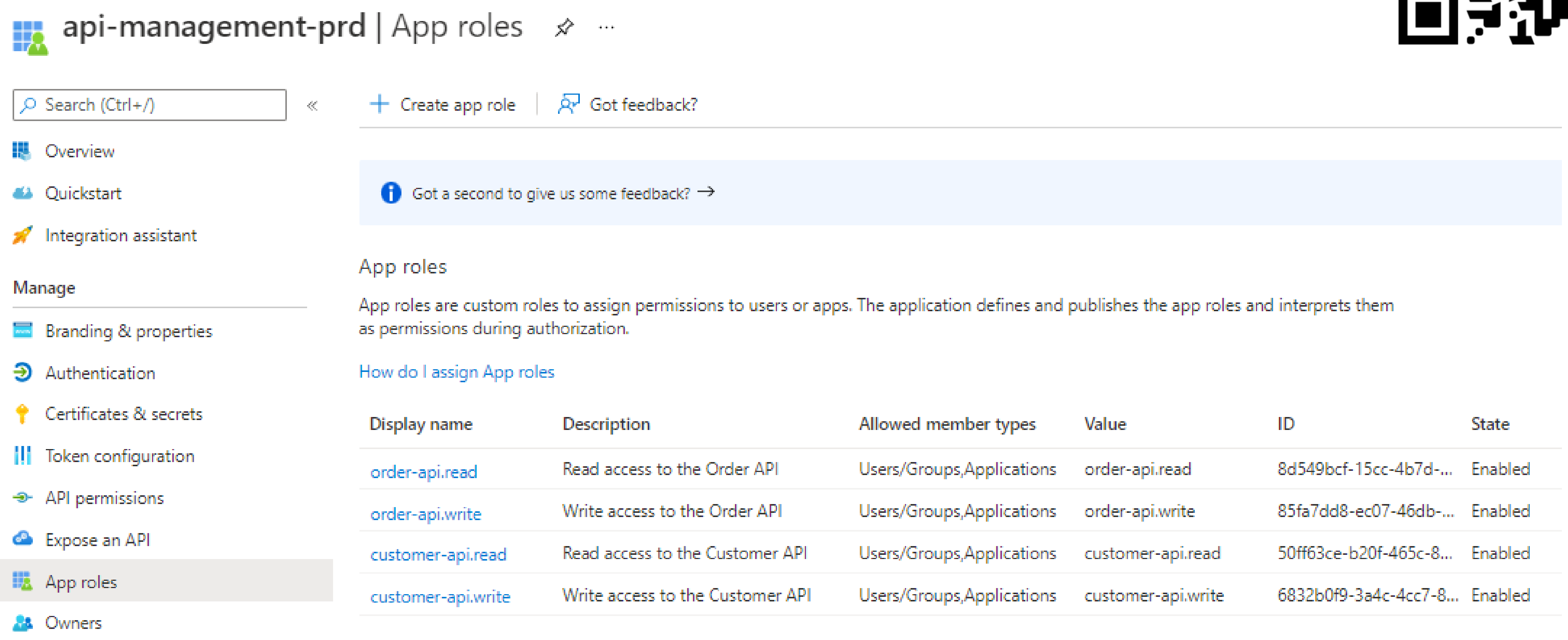
Go to www.menti.com
Code: 59 91 12

Global access control

- Common security requirements:
  - Access control is managed in IdP, not in API Management
  - The API consumers can be users or daemons
  - The API consumers use standardized OAuth2 authentication flows
  - The API consumers can authenticate with client secret or certificate
  - For each API, read and/or write access can be granted.

Global access control

Implementation with Azure AD



api-management-prd | App roles

Search (Ctrl+/)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

+ Create app role | Got feedback?

Got a second to give us some feedback? →

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

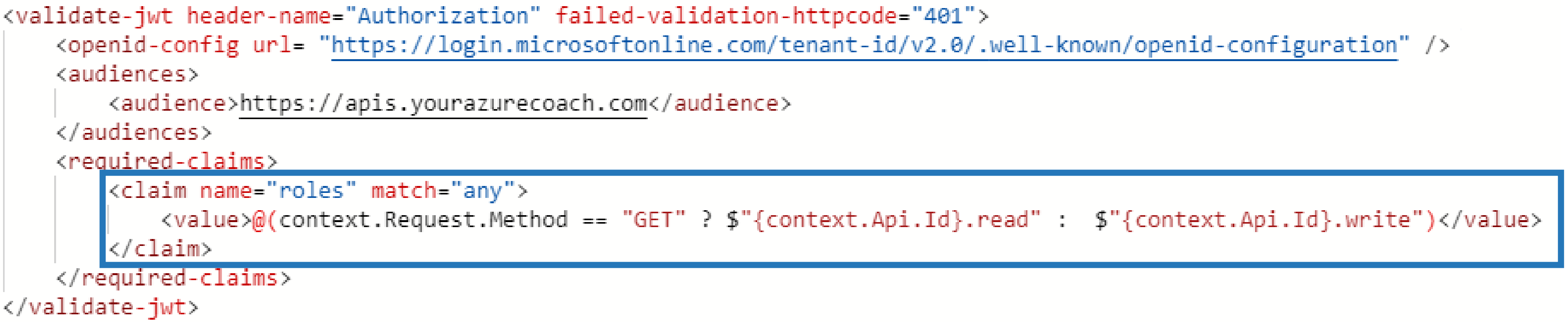
How do I assign App roles

Display name	Description	Allowed member types	Value	ID	State
order-api.read	Read access to the Order API	Users/Groups,Applications	order-api.read	8d549bcf-15cc-4b7d-...	Enabled
order-api.write	Write access to the Order API	Users/Groups,Applications	order-api.write	85fa7dd8-ec07-46db-...	Enabled
customer-api.read	Read access to the Customer API	Users/Groups,Applications	customer-api.read	50ff63ce-b20f-465c-8...	Enabled
customer-api.write	Write access to the Customer API	Users/Groups,Applications	customer-api.write	6832b0f9-3a4c-4cc7-8...	Enabled

NOEST YOUR AZURE COACH

Global access control

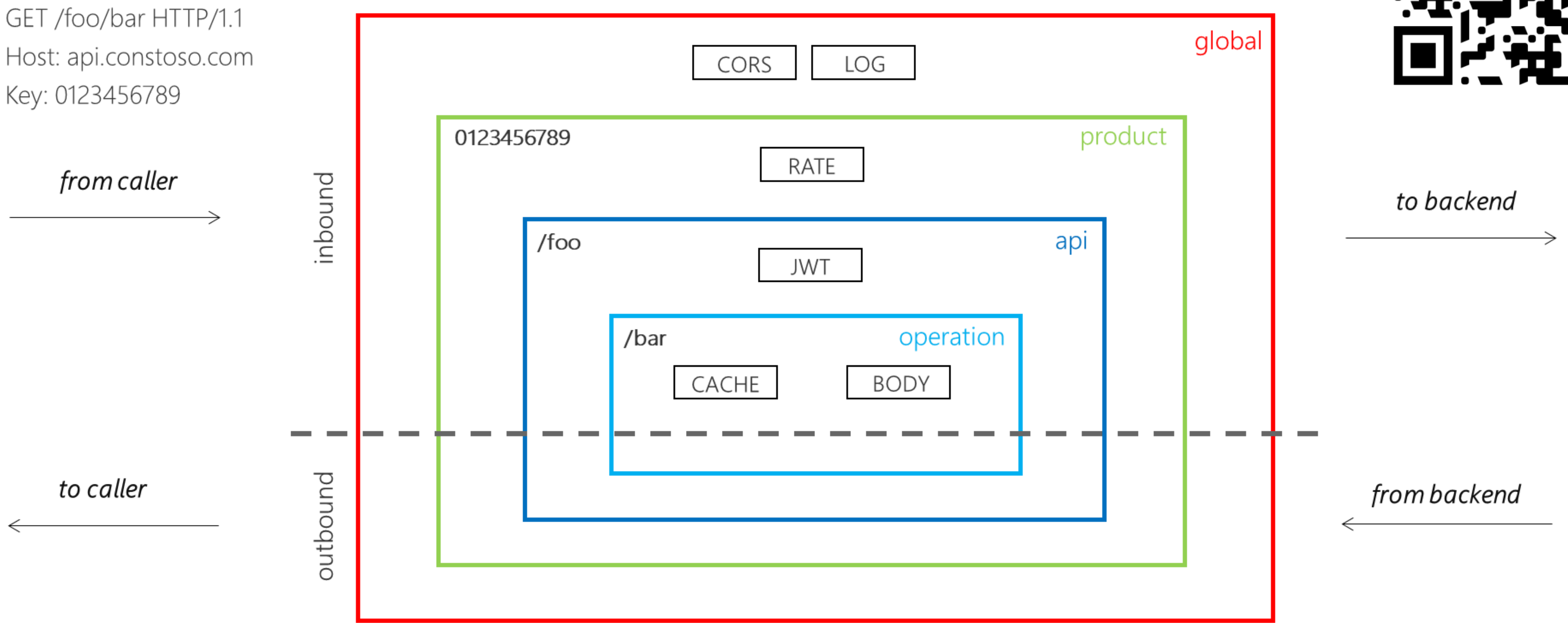
- Implementation with Azure AD



```
<validate-jwt header-name="Authorization" failed-validation-httpcode="401">
    <openid-config url= "https://login.microsoftonline.com/tenant-id/v2.0/.well-known/openid-configuration" />
    <audiences>
        <audience>https://apis.yourazurecoach.com</audience>
    </audiences>
    <required-claims>
        <claim name="roles" match="any">
            <value>@(context.Request.Method == "GET" ? $"{context.Api.Id}.read" :  $"{context.Api.Id}.write")</value>
        </claim>
    </required-claims>
</validate-jwt>
```

#9

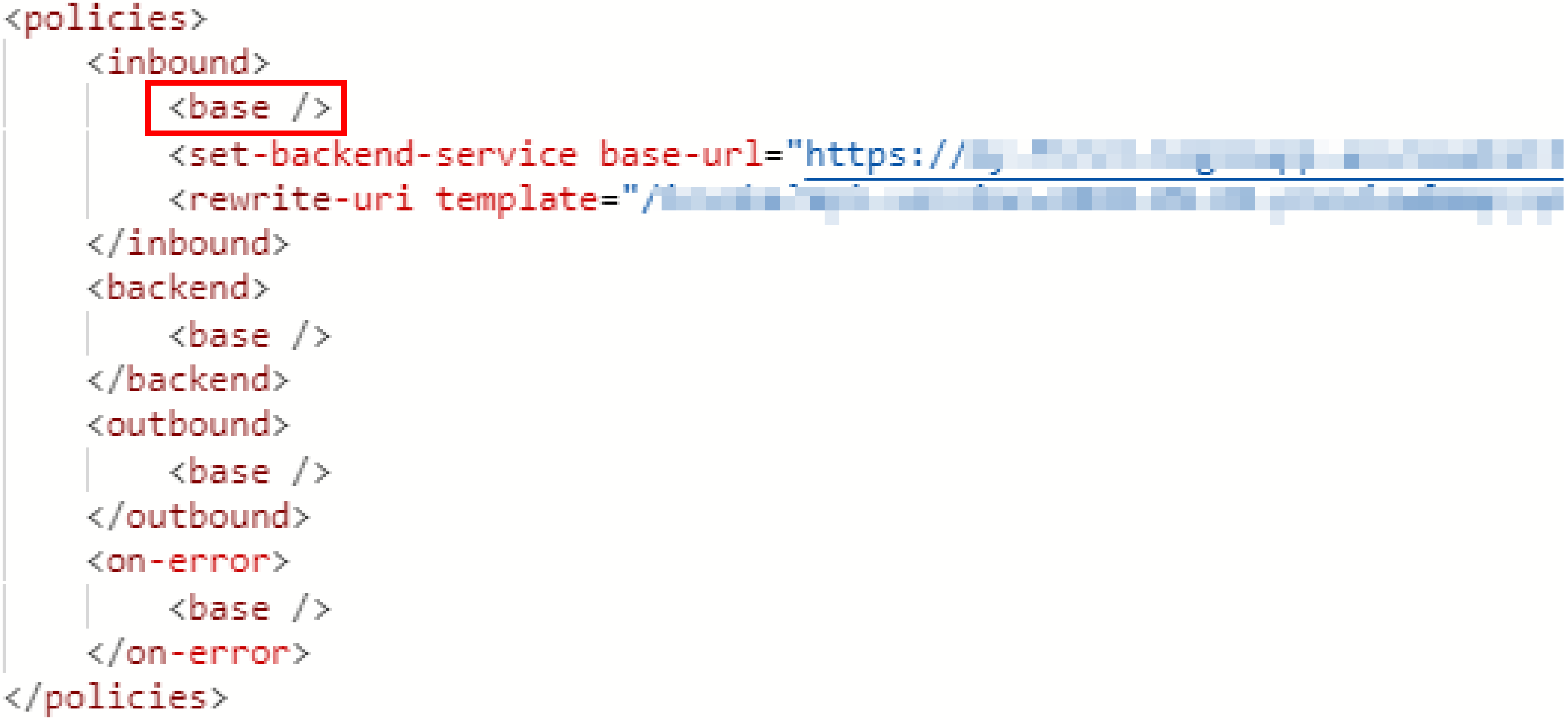
Understanding policy scopes



GET /foo/bar HTTP/1.1
Host: api.constoso.com
Key: 0123456789

The <base/> element

- No <base/> = no parent scope execution



```
<policies>
    <inbound>
        <base />
        <set-backend-service base-url="https://[redacted]
        <rewrite-uri template="/[redacted]
    </inbound>
    <backend>
        <base />
    </backend>
    <outbound>
        <base />
    </outbound>
    <on-error>
        <base />
    </on-error>
</policies>
```

Go to www.menti.com

Code: 59 91 12

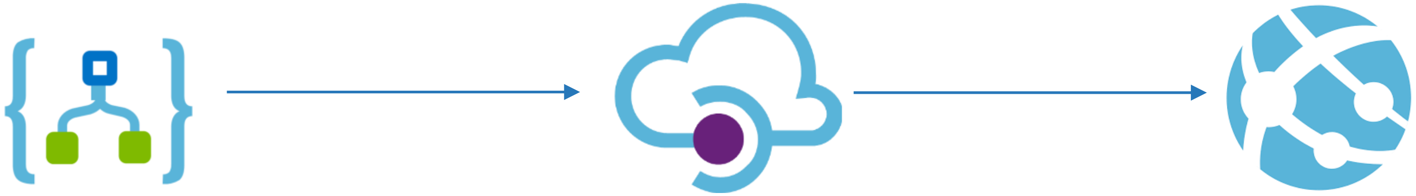
Enforce the <base/> element

- There are two options:
  - Validate policies in source control
  - Validate policies within an API Management instance

#10

Passwordless communication

- Use Managed Identity wherever possible
    - It's free
    - It's simple
    - No need to manage credentials
    - Available on frontdoor and backdoor



NOEST YOUR AZURE COACH

Go to www.menti.com
Code: 59 91 12

www.yourazurecoach.com

THANK YOU !!!

TOON VANHOUTTE

ToonVanhoutte