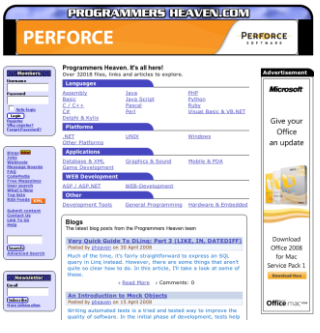
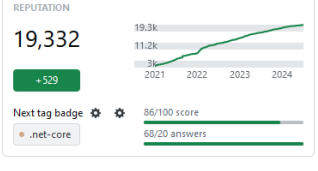
Introducing the Azure Cloud Debugging Tool

About Your Instructor

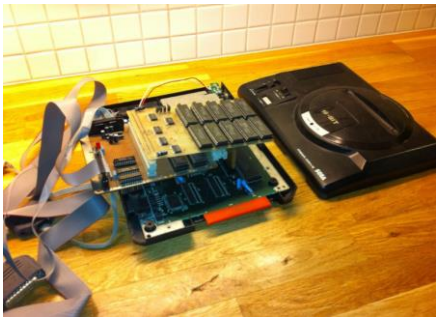
- Tore Nestenius
- Programming for over 40 years
- **1996, www.programmersheaven.com**
  A popular website for programmers with over 750,000 monthly visitors.

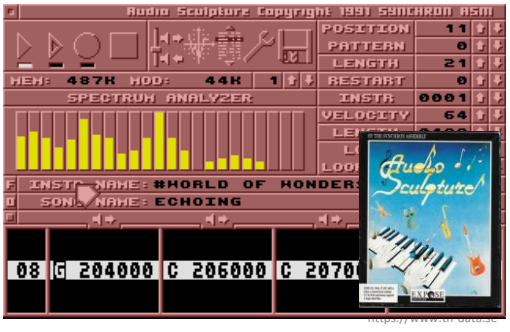


- **2020, Stack Overflow**
  Started to help others!



Past Projects – 1987-1993

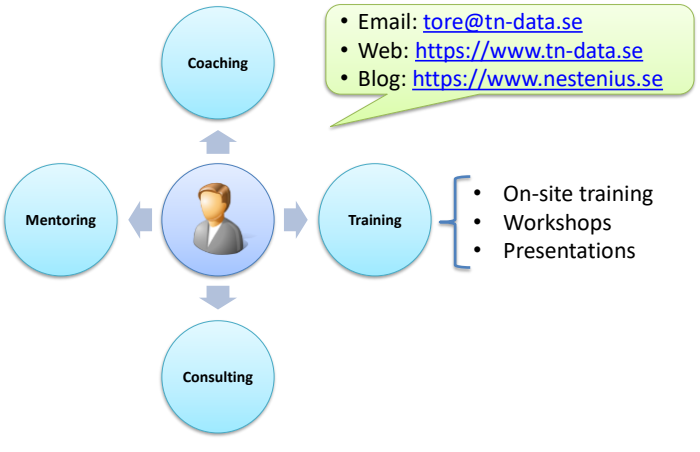




3

My current occupation

Today, I am self-employed at T.N. Datakonsult AB



What topics do I focus on?

https://www.tn-data.se

4

My Courses

Fundamentals
- Containers and **Kubernetes**
- Introduction to **Git** and **GitHub**

Architecture
- Modern Application **Architecture**
- Service Communication - **REST** vs. **GraphQL** vs. **gRPC**

OpenID Connect and OAuth
- Introduction to **OIDC** and **OAuth**
- Securing ASP.NET Using OIDC and **IdentityServer**
- **IdentityServer** in Production

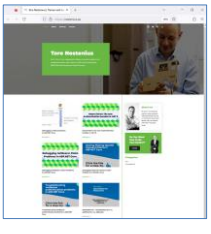
Web
- **Web Security** Fundamentals

.NET
- Applied **D**omain-**D**riven **D**esign in .NET
- **CQRS** and **Event Sourcing** in .NET
- Building ASP.**NET Core** APIs
- **Asynchronous** Programming in C#
- C# Expert
- C# Fundamentals
- TDD.NET

For course details, see https://www.tn-data.se

My blog

I blog at https://nestenius.se/



- User Delegation SAS Tokens In Azure Explained
- Running Docker in an Azure Windows Virtual Machine – Not so fast!
- Deploy containers Azure App Services using user-assigned identity
- Debugging cookie problems in ASP.NET Core
- BearerToken: The new Authentication handler in .NET 8
- Debugging JwtBearer Claim Problems in ASP.NET Core
- Debugging OpenID Connect Claim Problems in ASP.NET Core
- Troubleshooting JwtBearer authentication problems in ASP.NET Core
- IdentityServer – IdentityResource vs. ApiResource vs. ApiScope
- ASP.NET Core JwtBearer library: what's new?
- How I built my own Sega Mega Drive hardware dev kit from scratch
- .NET 5 Source Generators – MediatR – CQRS – OMG!
- Storing the ASP.NET Core Data Protection Key Ring in Azure Key Vault
- Exploring the non-nullable type warnings in C# 8
- …

Important Notes!

- **Interrupt me!**
- **Discuss!**
- **Ask questions**!

Agenda!

- **Introducing the Cloud Debugger**
- **DefaultAzureCredentials deep dive**

First some background!

AZ-204 Azure Developer Associate

You've earned your Microsoft Certified: Azure Developer Associate certification

Microsoft certification ID: 7319380

Congratulations! You've earned your Microsoft Certified: Azure Developer Associate certification.

Studying for AZ-204 the hard way!

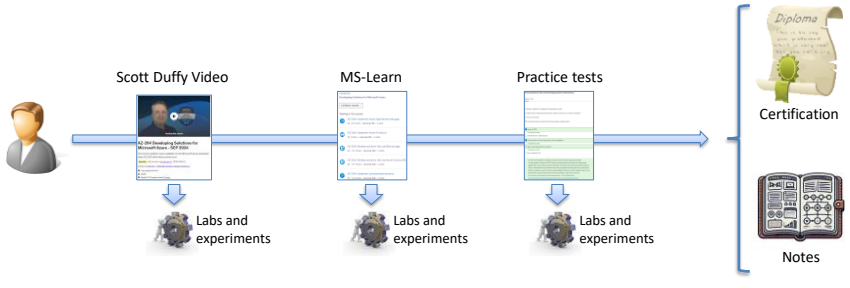
How are we going to learn all of this?

Azure SDKs API Gateway Content Delivery Network (CDN) Consistency Models (Strong, Eventual) OAuth Authorization Server Deployment Slots (App Service) Quotas and Throttling Azure App Service Application Insights Retry Pattern GitHub Actions IPsec A/B Testing Data Encryption (In-Transit, At-Rest) Infrastructure as a Service (IaaS) Application Gateway Message Brokers Log Analytics Role-Based Access Control (RBAC) Azure Activity Log Network Watcher Azure SQL Database Metrics and Alerts Azure Repos Azure DevOps Pipelines Service Principals Azure Kubernetes Service (AKS) Azure Portal SOAP Caching (Redis Cache) Application Insights Managed Identity Automatic Failover Groups Azure PowerShell Dependency Injection Azure Data Lake Storage Azure Event Grid JWT (JSON Web Token) CQRS (Command Query Responsibility Segregation) Diagnostic Settings Database Sharding Secrets Management Deployment Stages Continuous Deployment (CD) Continuous Integration (CI) Middleware Build Agents Visual Studio Code Serverless Computing Software as a Service (SaaS) Identity and Access Management (IAM) Azure File Storage Dead-letter Queue (DLQ) NoSQL Databases Circuit Breaker Pattern Shared Access Signature (SAS) Queue and Message TTL (Time-to-Live) Azure DevOps Sharding Autoscale Azure Boards Pub/Sub Pattern Distributed Tracing Azure Functions Azure Monitor OpenAPI/Swagger Data Replication (LRS, ZRS, GRS, RA-GRS) Azure Resource Manager (ARM) Azure Functions Core Tools Canary Release Azure Regions and Availability Zones REST API Azure Table Storage Partition Key Azure Blob Storage Azure Storage Explorer Azure Artifacts External Identity Providers Distributed Tracing Rollback Strategy Microservices Architecture Stateless and Stateful Services Azure Database for PostgreSQL Azure Database for MySQL API Versioning WebSockets Resource Throttling Azure Service Health Azure Cosmos DB Azure Relay Platform as a Service (PaaS) HTTP/HTTPS Rate Limiting Azure Key Vault TCP/IP Azure Notification Hubs OData SQL Elastic Pools Azure API Management Azure Queue Storage Durable Functions Geo-replication Multi-Factor Authentication (MFA) Azure SignalR Service Azure Container Instances (ACI) Resource Groups Azure Logic Apps Retry Policies Azure SQL Managed Instance Policies (XML-based policy configuration) Blue-Green Deployment Backend Service Azure Event Hubs Topic and Subscription API Gateway Pattern OAuth 2.0 Azure Monitor Logs Hot, Cool, and Archive Storage Tiers Infrastructure as Code (IaC) Azure Service Bus Serverless Orchestration Managed Identity Authentication App Service Plan Azure Function Triggers and Bindings Connection Strings Continuous Monitoring Access Tokens Service Endpoint Policy-Based Authorization ARM Template Deployment Mode Blob Storage Lifecycle Management Durable Task Framework Function Chaining Event Sourcing Authorization Code Flow Load Testing Static Web Apps….

What are our options?

Studying for AZ-204

We could do it the usual way:

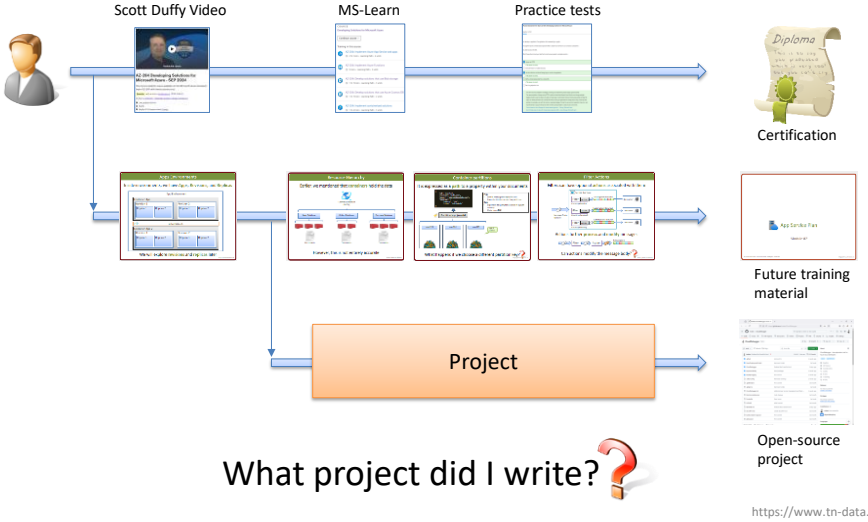


How did I do it?

You don't know something until you can explain it to others!

Studying for AZ-204 the hard way!

My study process



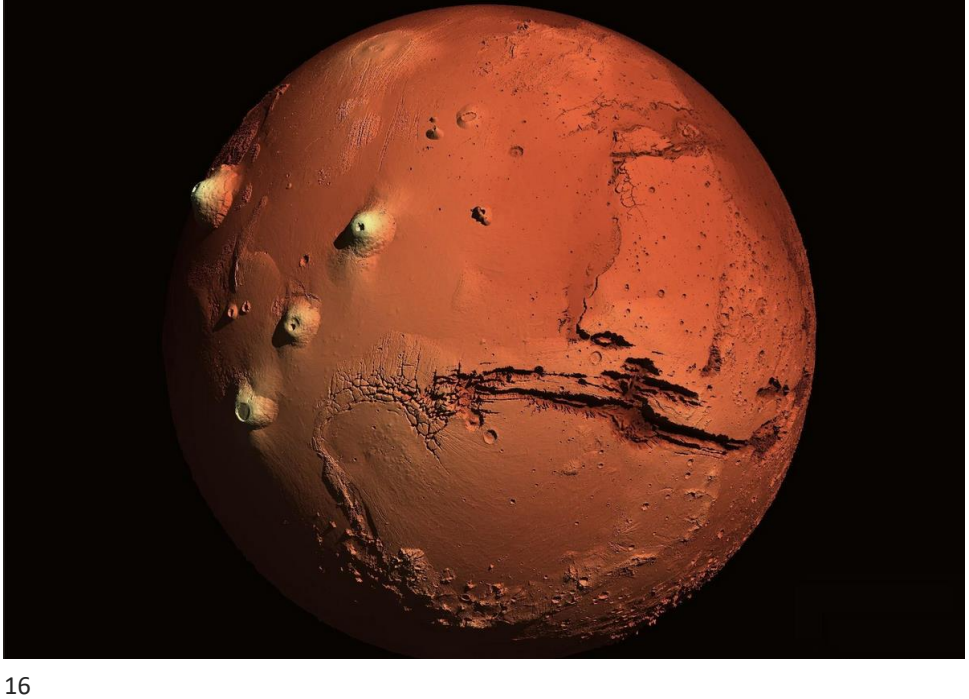
What project did I write?

https://www.tn-data.se

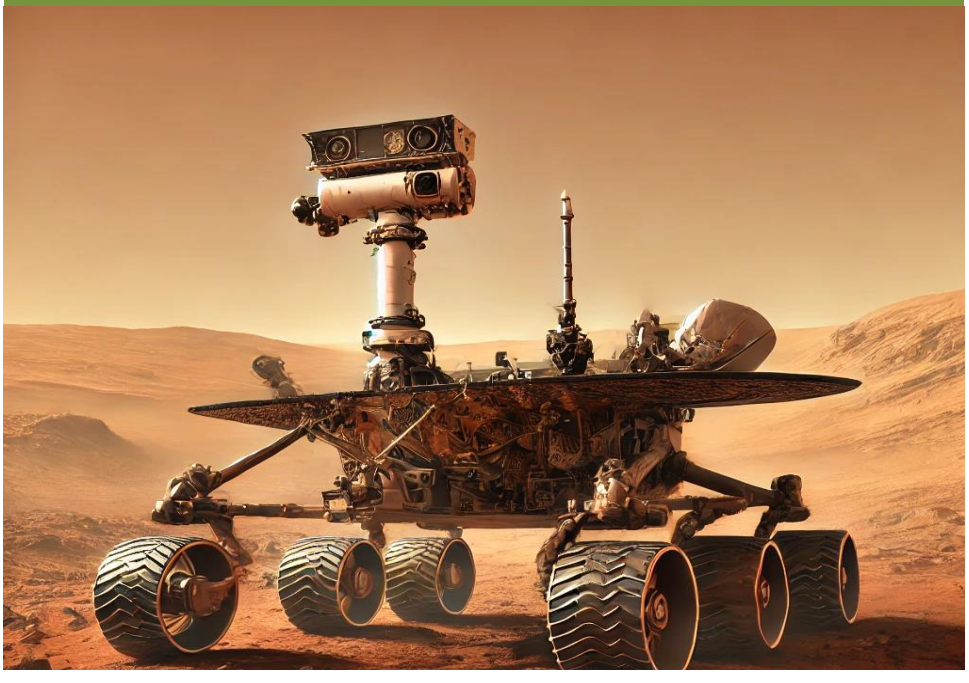
Introducing the project

https://www.tn-data.se

Exploring Mars



Mars Rover



17

How should we explore Azure?

18

Introducing the Cloud Debugger

What can it do?

https://www.tn-data.se

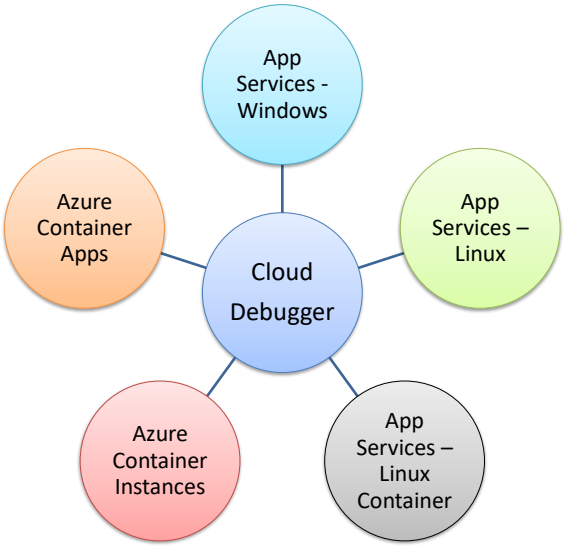
What can it do?

- Logging
- REST API
- Calling APIs
- File system
- Local cache
- Credentials caching
- DefaultAzureCredentials
- Runtime details
- Environment variables
- Configuration
- Network
- Logging
- Error handling
- Caching
- User Delegation SAS Token
- Web Hooks
- Data Protection API
- Connection Strings
- …

- App Services
- Azure Functions
- Azure Container Instances
- Container Apps
- Cosmos DB
- Azure SQL Server
- Redis
- Entra ID
- API Gateway
- Blob Storage
- Azure CDN
- Event Hub
- Event Grid
- Log analytics Workspace
- …

https://www.tn-data.se

Deployment Targets

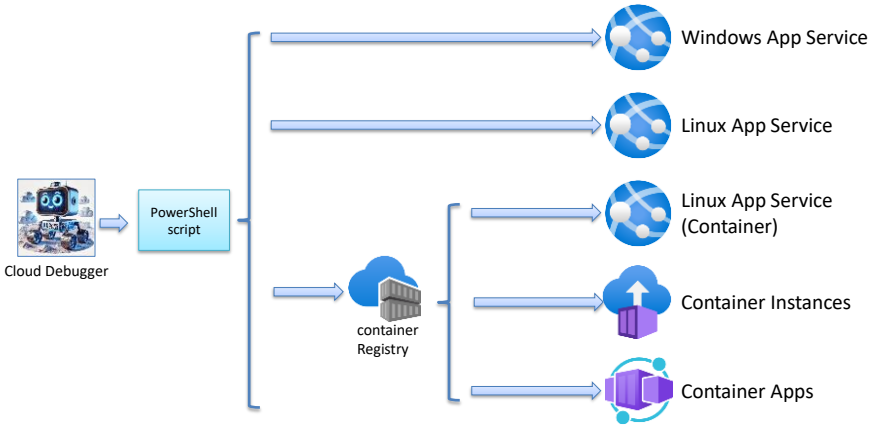


How is this deployed?

https://www.tn-data.se

Deployment

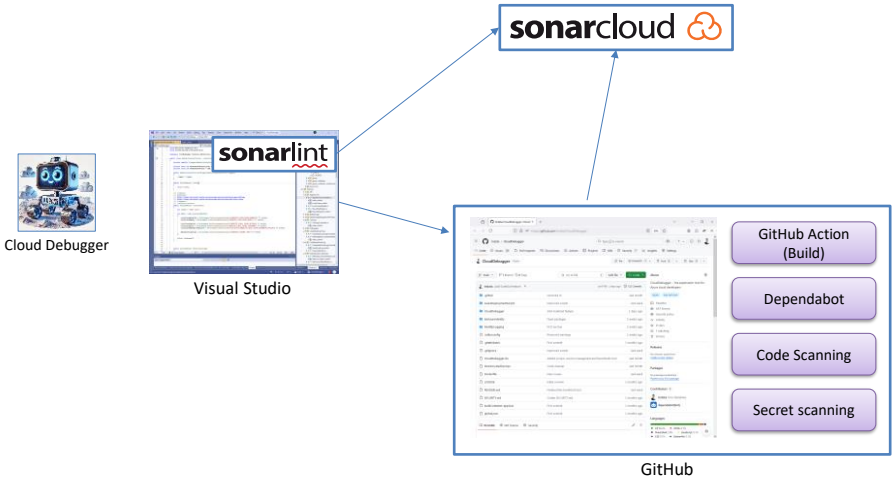
The deployment setup



https://www.tn-data.se

Deployment

Secure development practices



https://www.tn-data.se

The Tools

https://www.tn-data.se

Redis Tool

Azure Cache for Redis

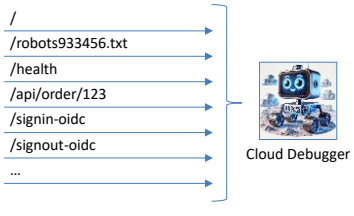
We can **read** and **write** keys to **Redis** instances

Supports both **access keys** and **managed identity**

Request Logger

Request Logger

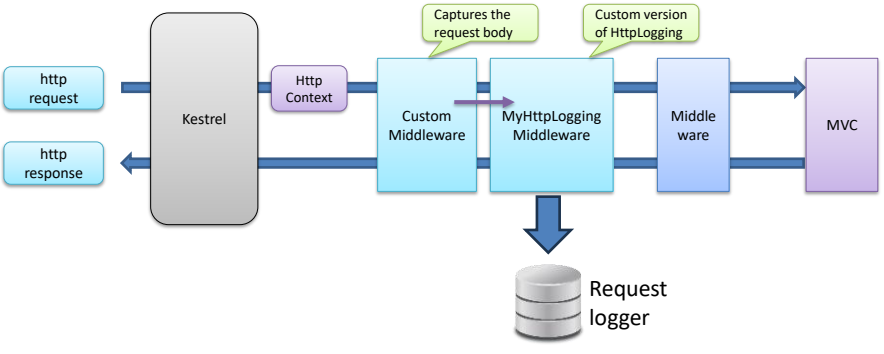
Our tool will receive a lot of request during its lifetime



This tool will capture and log all the **requests** and **responses**

Request Logger

Internally two **middleware** modules are use



Important, this tool will capture sensitive information!

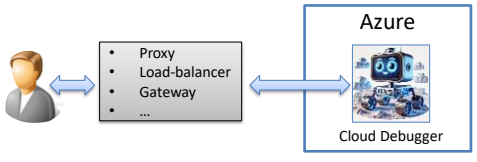
https://www.tn-data.se

Current Request Viewer

https://www.tn-data.se

Current Request Viewer

This tool displays the received **request headers**



HTTP(s) protocol details

Received protocol	HTTP/2
Received scheme	https

TLS/SSL details

Protocol	Tls12
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Cipher strength	256
Cipher algorithm	Aes256
KeyExchange algorithm	44550 (DiffieHellman)
KeyExchange strength	384
Local SSL certificate	CN=localhost
Local SSL Serial number	00D9395EE2457863D3

Request headers

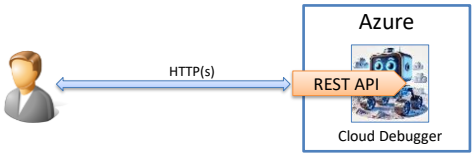
Accept	text/html,application/xhtml+xml,application/xml;
Accept-Encoding	gzip, deflate, br, zstd

Azure often rewrites and adds headers to the request

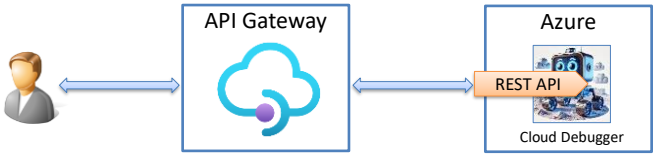
REST API Tool

REST API Tool

This tool exposes a simple REST API



This can be useful for testing with an **API Gateway**

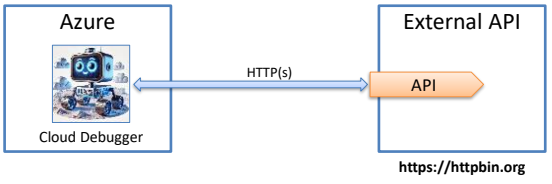


Allows us to verify that we can send traffic to an API

Calling External APIs

Calling External APIs

Makes HTTP requests to an external API outside of Azure

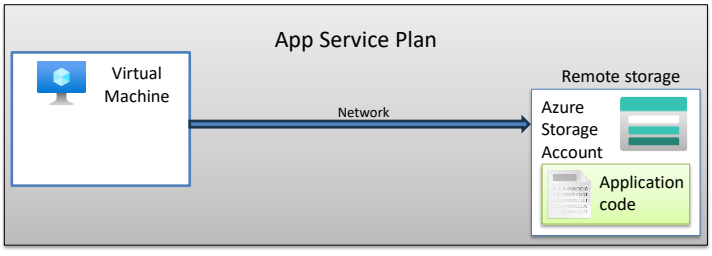


httpbin is a simple HTTP Request & Response Service

App Services Tools – Local Cache

App Services Tools – Local Cache

By default, the application code is stored in a remote storage



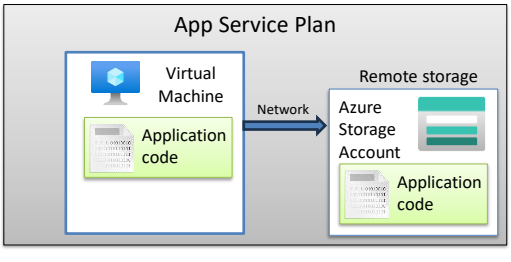
Some of the problems with this are:

- Increased Latency
- Higher Load on Remote Storage
- Reduced Performance
- Scalability Challenges
- …

How can we improve this?

App Services Tools – Local Cache

We can enable an optional **local cache** feature



- Reduced latency
- Improved performance
- Scalability
- Resilience to
  - Network Issues
  - Storage issues

When enabled, Azure will make a local copy of the App

A feature for Windows non-container-based apps

How do we enable this feature?

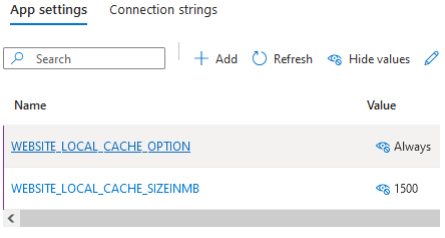
App Services Tools – Local Cache

To enable it, we need to set this configuration setting:

Setting name	Value
WEBSITE_LOCAL_CACHE_OPTION	Always
WEBSITE_LOCAL_CACHE_SIZEINMB	1000

Optional, 1000 is the default (1GB)

It can for example, be set in the portal:



What does this tool do?

https://www.tn-data.se

App Services Tools – Local Cache

This tool will display the current local cache settings:

App Service Local Cache details

If enabled

LocalCache Option	**Always** (Default, Always, Diabled)
LocalCache Size	**[Not set]** MB (1-2000 MB)
LocalCache Read-Write options	**[Not set]** Available options are: - ReadOnly: Cache is read-only. - WriteButDiscardChanges: Allow writes to local cache but discard changes made locally.
LocalCache Enabled	**True**
LocalCache Ready	**TRUE** (Read-only flag indicating if the app using local cache).
Website Volume Type	**LocalCache** (Shows the storage volume type currently in use. Should either be PrimaryStorageVolume or LocalCache if set).

https://www.tn-data.se

App Services Tools – Show File System

https://www.tn-data.se

App Services Tools – Show File System

This tool will display the core App Service directories

App Service details

Operating System	Microsoft Windows 10.0.20348
Home Directory	C:\home
Temp Directory	C:\local\Temp
Application Directory	C:\home\site\wwwroot\

Home Directory	Application directory	Temp directory
\.ssh \ASP.NET \ShutdownSentinel \data \logfiles \site	\wwwroot Azure.Core.Amqp.dll Azure.Core.dll Azure.Identity.dll Azure.Messaging.EventGrid.dll Azure.Messaging.EventHubs.dll Azure.Storage.Blobs.ChangeFeed.dll Azure.Storage.Blobs.dll Azure.Storage.Common.dll CloudDebugger.deps.json CloudDebugger.dll CloudDebugger.exe CloudDebugger.pdb CloudDebugger.runtimeconfig.json Flurl.Http.dll Flurl.dll Humanizer.dll Microsoft.AI.DependencyCollector.dll Microsoft.AI.EventCounterCollector.dll Microsoft.AI.PerfCounterCollector.dll	\siteExtLogs

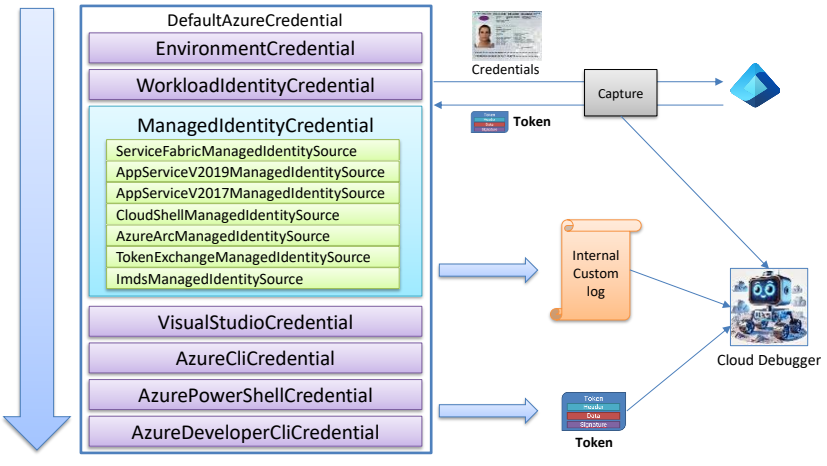
https://www.tn-data.se

Credentials - DefaultAzureCredentials

https://www.tn-data.se

Credentials - DefaultAzureCredentials

This tool will try to get an **access token** from Entra ID



This tool will give you insights in how this credential work

https://www.tn-data.se

Credentials – Token caching

Credentials – Token caching

This tool explores the caching of access tokens

```
ŵắs çsêđ   ŋêx Dêğắụĺţ̈AćụsêCsêđêŋţ̈íắĺ
ğǫ̣s  îŋţ̈ î   .  î   .. î
    ţ̈ǫ̣lêŋ   çsêđ ĜêţAççêşşŢǫ̣lêŋ
```

```
ğǫ̣s  îŋţ̈ î   .  î   .. î
    ŵắs çsêđ   ŋêx Dêğắụĺţ̈AćụsêCsêđêŋţ̈íắĺ
    ţ̈ǫ̣lêŋ   çsêđ ĜêţAççêşşŢǫ̣lêŋ
```

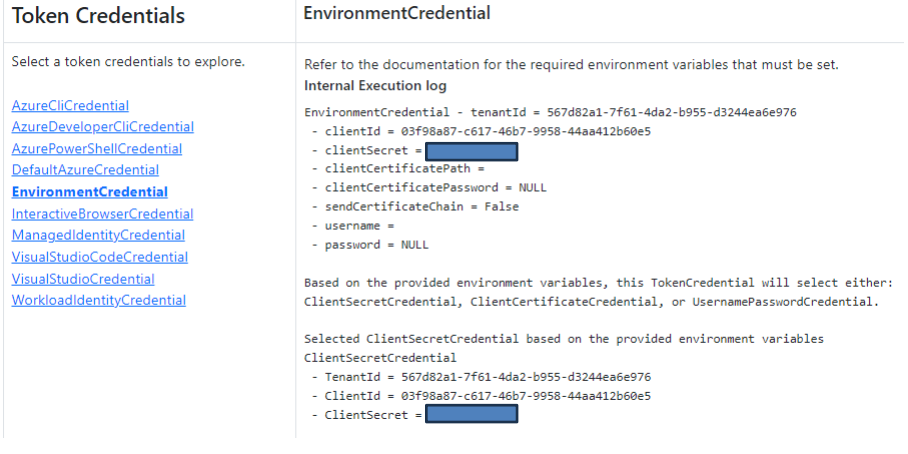
Different credentials handle caching differently!

Credentials – TokenCredentials Explorer

https://www.tn-data.se

Credentials – TokenCredentials Explorer

This tool allows you to execute different **TokenCredentials**



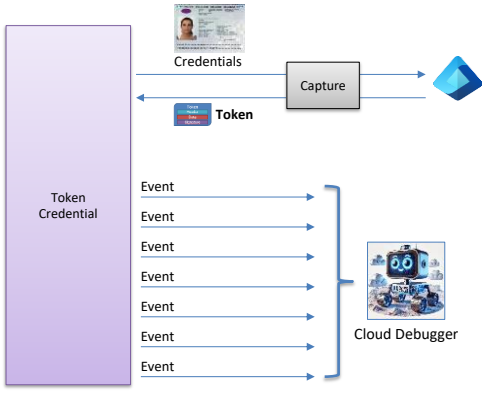
Perfect to try out in different environments

https://www.tn-data.se

Credentials – Event Log viewer

Credentials – Event Log Viewer

Captures the internal events from the **TokenCredentials**

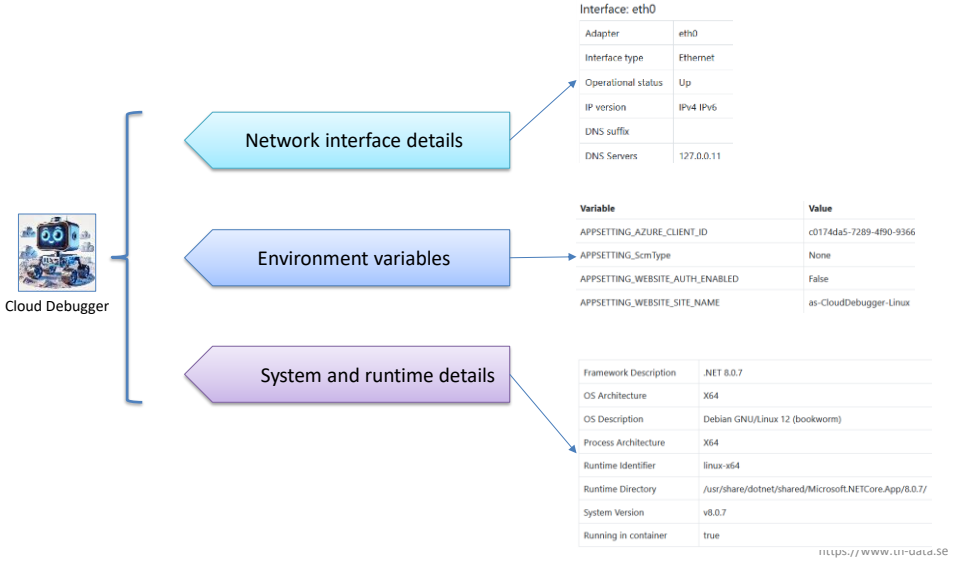


Including the internal communication with Entra ID

Diagnostics and system information

Diagnostics and system information

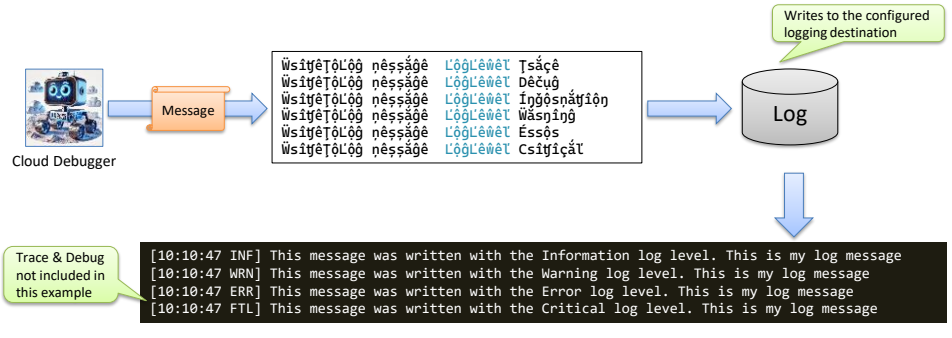
These tools will display details like:



Logging – Write message to the logs

Logging – Write message to the logs

This tool writes a log message with the six different log levels

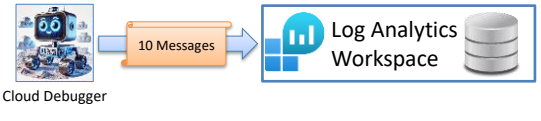


Perfect for troubleshooting logging issues

Logging – Log Analytics Workspaces

Logging – Log Analytics Workspaces

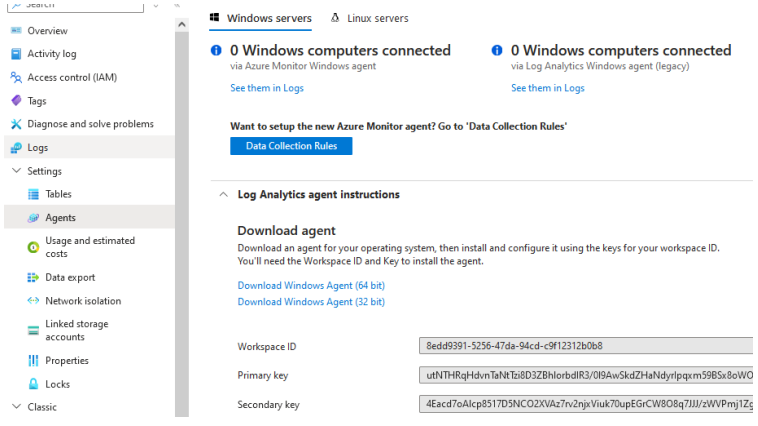
This tool will send 10 log entries to a **Log Analytics Workspace**



Where do I get the Log Analytics **ID** and **key**?

Logging – Log Analytics Workspaces

The key can be found under **Settings -> Agents**



What does the events look like in the workspace?

https://www.tn-data.se

Logging – Log Analytics Workspaces

This is the result:

Results | Chart

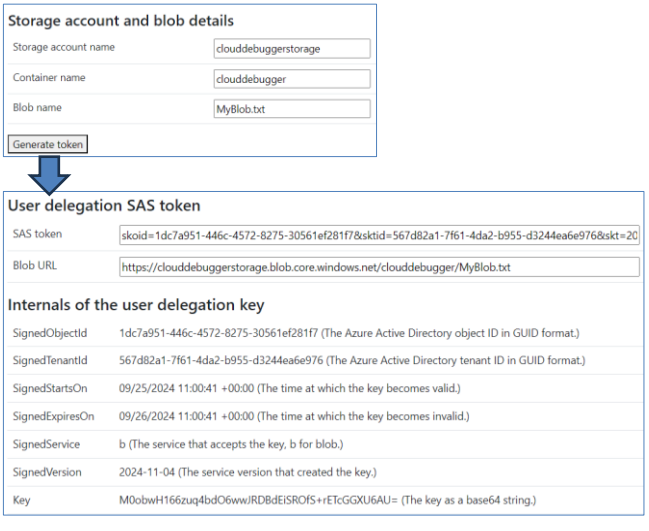
TimeGenerated [UTC]	Message	Severity_s	Timestamp_t [UTC]	Type
25/09/2024, 09:31:08.508	This is my custom message #0	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
TenantId	8edd9391-5256-47da-94cd-c9f12312b0b8			
SourceSystem	RestAPI			
TimeGenerated [UTC]	2024-09-25T09:31:08.5083338Z			
Message	This is my custom message #0			
Severity_s	Error			
Timestamp_t [UTC]	2024-09-25T09:31:07.8021112Z			
Type	MyApplicationLog_CL			
25/09/2024, 09:31:08.508	This is my custom message #1	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #2	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #3	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #4	Warning	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #5	Information	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #6	Information	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #7	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #8	Error	25/09/2024, 09:31:07.802	MyApplicationLog_CL
25/09/2024, 09:31:08.508	This is my custom message #9	Information	25/09/2024, 09:31:07.802	MyApplicationLog_CL

https://www.tn-data.se

Blob Storage - Create a User Delegation SAS Token

Blob Storage - Create a User Delegation SAS Token

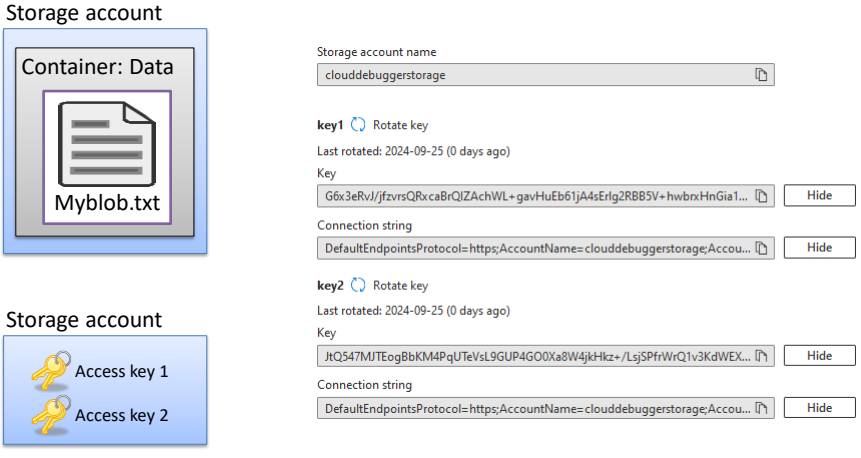
This tool creates a **SAS token** to a given blob in blob storage



What is the problem with standard SAS tokens 

Blob Storage - Create a User Delegation SAS Token

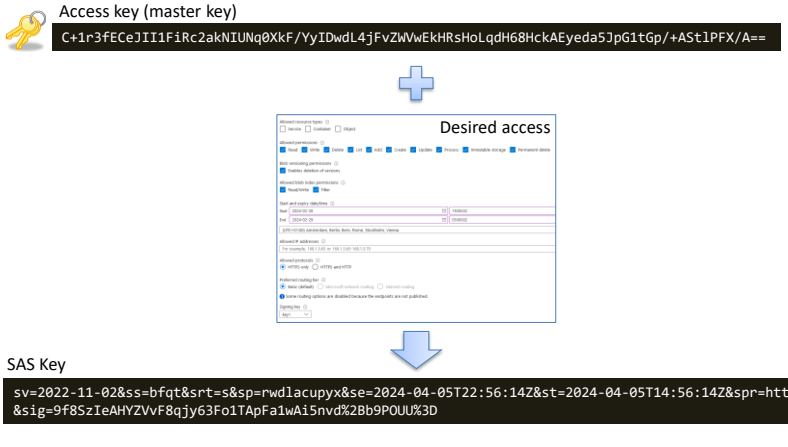
A storage account includes two access keys:



How do you generate a SAS token from these keys?

Blob Storage - Create a User Delegation SAS Token

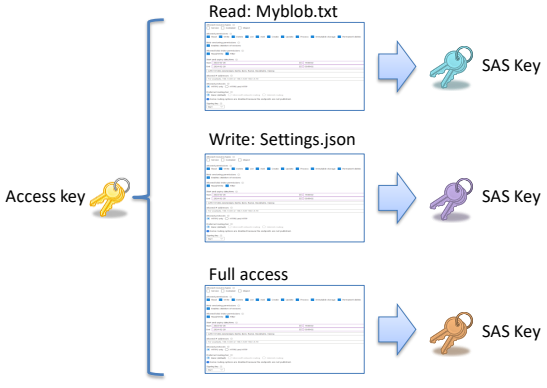
You can create a signed SAS token based on these keys



What does this allow us to do?

Blob Storage - Create a User Delegation SAS Token

From this access key, we can issue multiple SAS keys



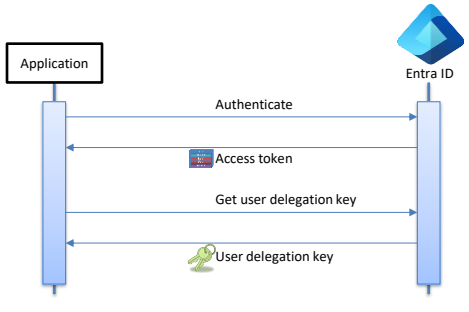
How can delegated access tokens improve this?

https://www.tn-data.se

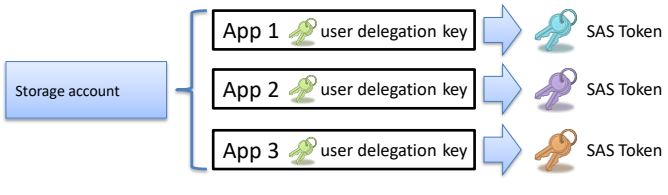
63

Blob Storage - Create a User Delegation SAS Token

Your application asks for a custom key from Entra ID



From the received **delegation key**, we can issue SAS tokens



https://www.tn-data.se

64

Blob Storage - Create a User Delegation SAS Token

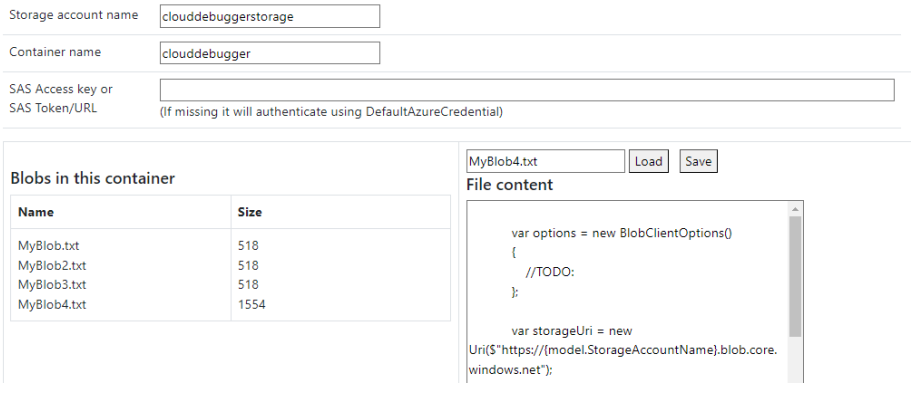
What are the Benefits of Using delegation SAS tokens?

- **Key Management:**
  - SAS tokens are signed using Entra ID via managed identity, removing the need for manual key management.
- **Limited Lifetime:**
  - Tokens can be short-lived, minimizing unauthorized access risks.
- **Enhanced Auditing:**
  - User Delegation SAS tokens appear in Azure Storage access logs, improving traceability.
- **Least Privilege:**
  - Tokens are issued with limited permissions, adhering to the principle of least privilege.
- **Access Control:**
  - Tokens can't exceed the issuing application's permissions, ensuring proper privilege containment.
- **Reduced Risk:**
  - Eliminates reliance on account keys, reducing the risk of key leakage and compromising the entire storage account.

Blob Storage – Accessing Blobs

Blob Storage – Accessing Blobs

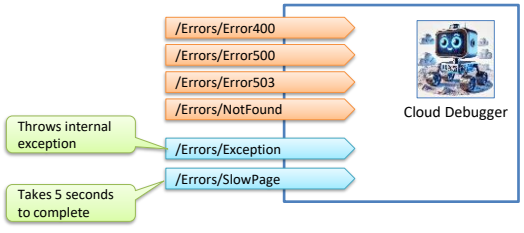
This tool allows you to **list**, **read** and **create** blobs



Blob Storage – Error Pages

Blob Storage – Error Pages

This tool generates various HTTP errors and exceptions

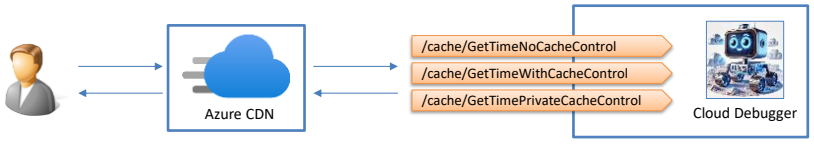


Useful for various testing purposes

Caching and Azure CDN

Caching and Azure CDN

This tool is useful for testing browser and CDN caching



URL	Response content
çắçḥê ĞêŧƫĵîṇêṆǫCắçḥêCǫṇƫsǫĺ	No caching response headers
çắçḥê ĞêŧƫĵîṇêẄîŧƫḥCắçḥêCǫṇƫsǫĺ	çắçḥê çǫṇƫsǫĺ řцčĺíç ṇắẏ ắĝê _
çắçḥê ĞêŧƫĵîṇêRsîẅắƫêCắçḥêCǫṇƫsǫĺ	çắçḥê çǫṇƫsǫĺ ṇǫ ştǫôsê ṇǫ çắçḥê ṇắẏ ắĝê . ṇụştƫ sêẅắĺíđắƫê řsǫẏẏ sêẅắĺíđắƫê řsíẅắƫê êyřîsệş řsắĝṇắ ṇǫ çắçḥê

Cache for 5 seconds

No caching

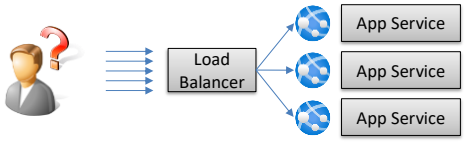
https://www.tn-data.se

Scale-out

https://www.tn-data.se

Scale-out

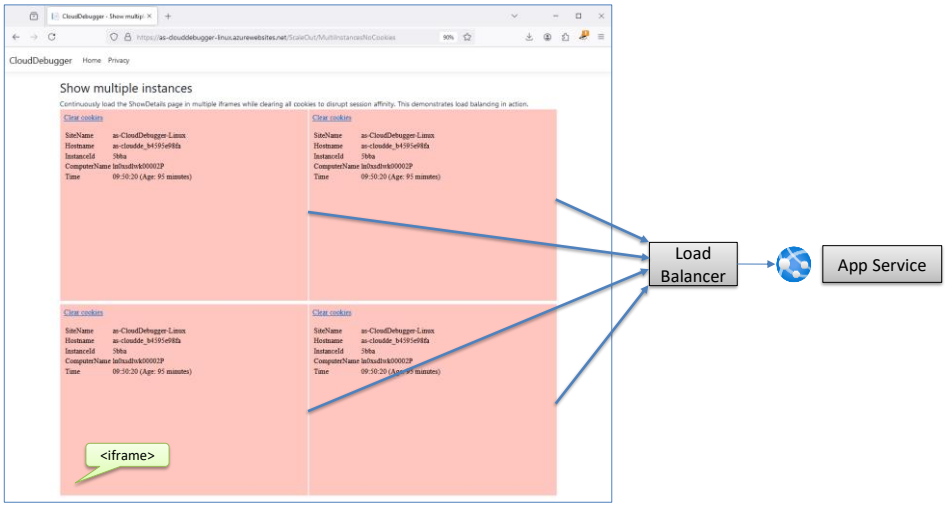
How can we tell if a service is load balanced?



https://www.tn-data.se

Scale-out

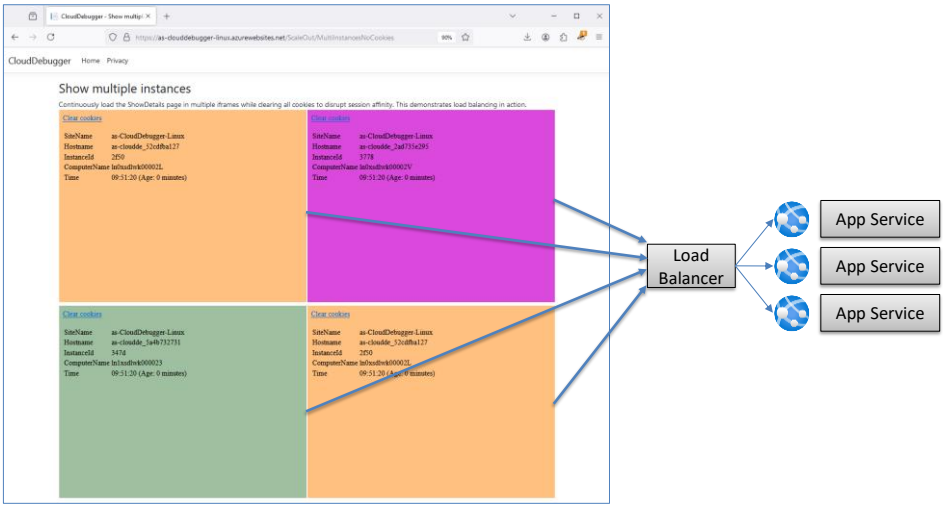
This tool will help you visualize service scale-out



https://www.tn-data.se

Scale-out

When we scale out, each instance is assigned a unique color



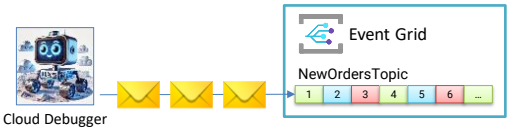
https://www.tn-data.se

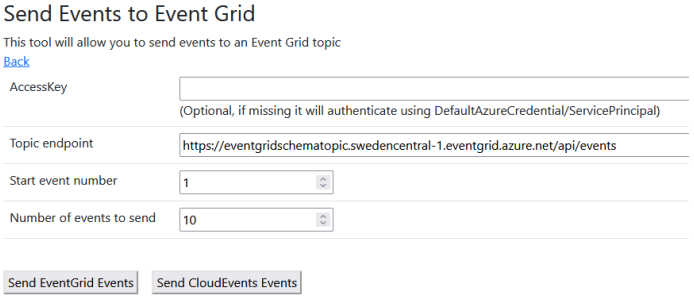
Event Grid

https://www.tn-data.se

Event Grid

This tool will send events to a given **Event Grid topic**



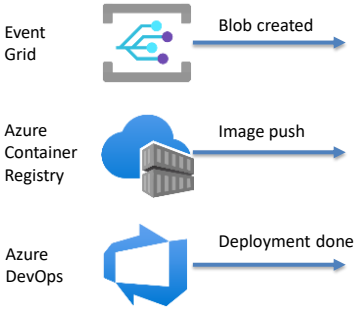


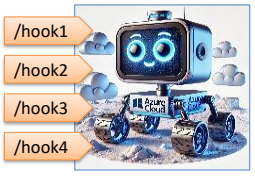
It support both **EventGrid** and **CloudEvents** schemas

Webhooks

Webhooks

This tool exposes **four endpoints** for exploring **webhooks**



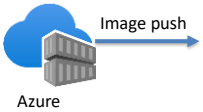


Cloud Debugger

What does a webhook request look like?

Webhooks

Here is a sample webhook request



Azure Container Registry

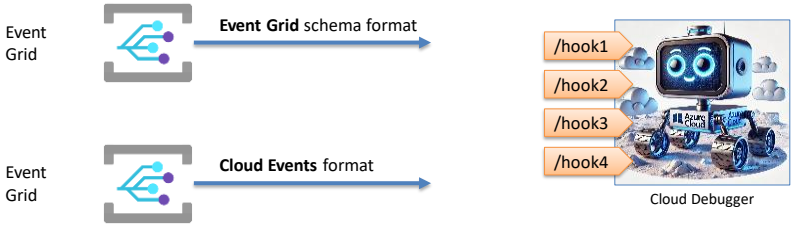
```
POST /hook1
Content-Type: application/json; charset=utf-8
User-Agent: AzureContainerRegistry/1.0
...

{
  "id": "9b17169d-bc07-4eb8-b918-31bf6e722089",
  "timestamp": "2024-10-03T12:48:15.462377991Z",
  "action": "push",
  "target": {
    "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
    "size": 1788,
    "digest": "sha256:a48fecdacb5e3bdf010874f6023937565b87da...",
    "length": 1788,
    "repository": "clouddebugger",
    "tag": "latest"
  },
  "request": {
    "id": "84557676-0f55-4da2-8e2c-af071614abc5",
    "host": "tncontaineregistry.azurecr.io",
    "method": "PUT",
    "useragent": "docker/27.2.0 go/go1.21.13 git-commit/3ab5c7d kernel/5.15.133.1-
microsoft-standard-WSL2 os/linux arch/amd64 UpstreamClient(Docker-Client/27.2.0
\\(windows\\))"
  }
}
```

What about events from **EventGrid**?

Webhooks

Event Grid supports two webhook formats

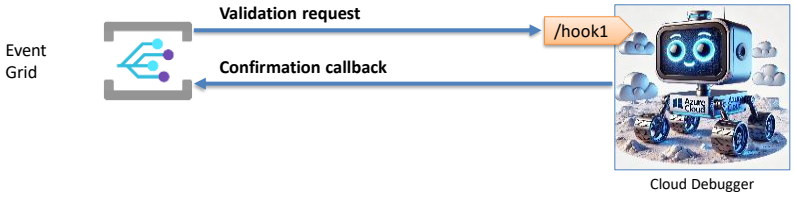


What must happen before EventGrid can send requests?

https://www.tn-data.se

Webhooks

The webhook must first respond to a validation requests



What does this look like?

https://www.tn-data.se

Webhooks

The initial validation request

```
POST /hook1
Content-Type: application/json; charset=utf-8
Host: as-clouddebugger-linux.azurewebsites.net
aeg-subscription-name: EVENTGRIDSUBSCRIPTION

[
  {
    "id": "0588c8e0-193c-4c19-99ab-40f905173d12",
    "topic": "/subscriptions/b78d216b-d714-4664-b39a-26ef8dbcfdf1/resourceGroups/rg-
CloudDebugger/providers/Microsoft.Storage/storageAccounts/clouddebuggerstorage",
    "subject": "",
    "data": {
      "validationCode": "194A76BD-17E0-41E4-BAEE-7FD21E27CE85",
      "validationUrl": "https://rp-
swedencentral.eventgrid.azure.net:553/eventsubscriptions/eventgridsubscription/validate?id=194A76BD-17E0-41E4-
BAEE-7FD21E27CE85&t=2024-10-04T09:28:29.2050157Z&apiVersion=2023-12-15-
preview&token=egZvMTdTIazJ5%2fKgBI1%2bh4xzaaGnciOXt3OYr9qJTmE%3d"
    },
    "eventType": "Microsoft.EventGrid.SubscriptionValidationEvent",
    "eventTime": "2024-10-04T09:28:29.2050821Z",
    "metadataVersion": "1",
    "dataVersion": "2"
  }
]
```

What happens next? 

Webhooks

Next, we need to send a request to the **validationUrl**

```
GET https://rp-
swedencentral.eventgrid.azure.net:553/eventsubscriptions/eventgridsubscription/validate?id=194A76BD-17E0-41E4-
BAEE-7FD21E27CE85&t=2024-10-04T09:28:29.2050157Z&apiVersion=2023-12-15-
preview&token=egZvMTdTIazJ5%2fKgBI1%2bh4xzaaGnciOXt3OYr9qJTmE%3d
```

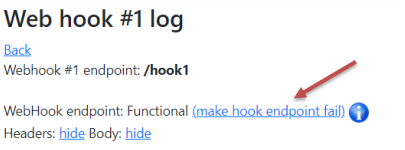
Then, EventGrid will respond with:

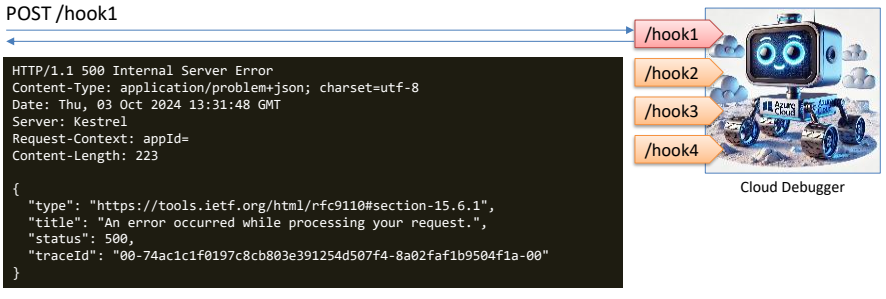
```
"Webhook successfully validated as a subscription endpoint."
```

What else can this tool do? 

Webhooks

Webhook endpoint failures can be simulated

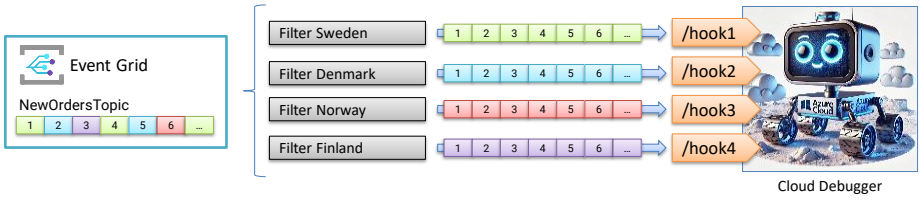




Webhooks overview tool

Webhooks overview tool

This tool will give you an overview of the four webhooks

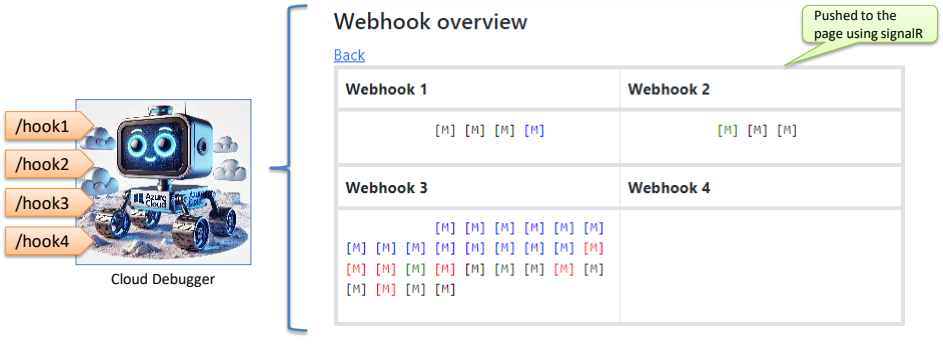


What does the result look like?

https://www.tn-data.se

Webhooks overview tool

This is a sample output:



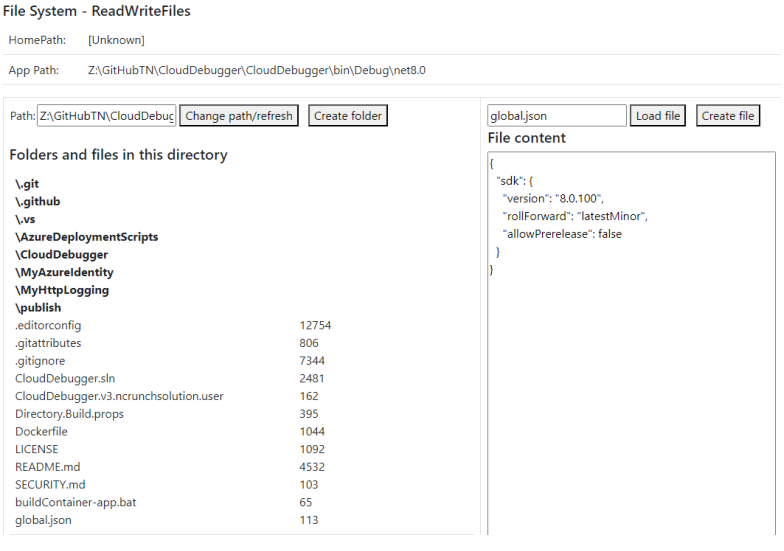
Different event messages will have different colours

https://www.tn-data.se

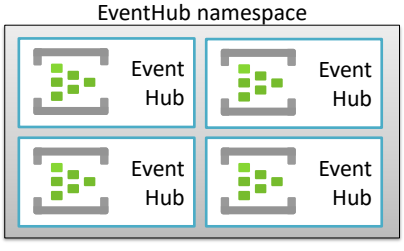
File System Explorer

File System Explorer

This tool allows you to explore the local file system



Event Hub



https://www.tn-data.se

Event Hub

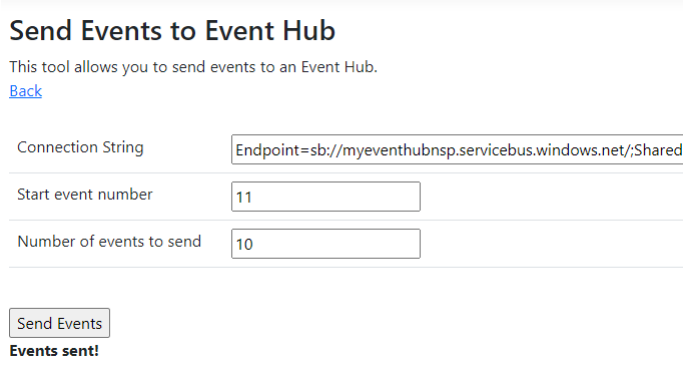
This tool allows you to send and consume **Event Hub** events

What does this tool look like?

https://www.tn-data.se

Event Hub

This is the send tool:

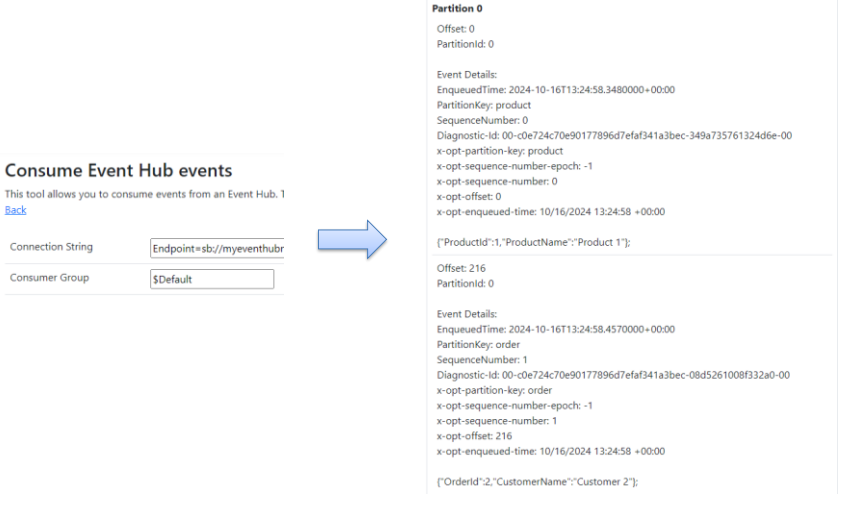


What does the receive tool look like?

https://www.tn-data.se

Event Hub

The is the consumer tool:

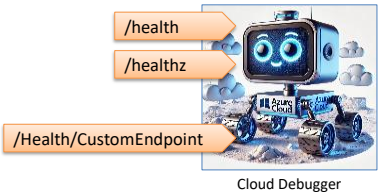


https://www.tn-data.se

Health Endpoints

Health Endpoints

This tool exposes two types of health endpoints



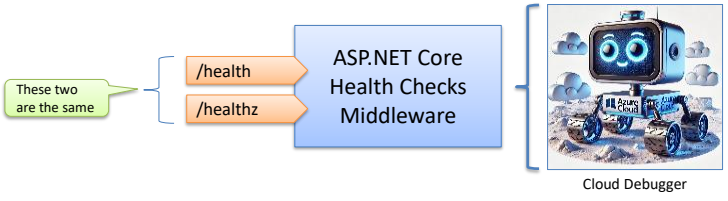
Cloud Debugger

Both are used to monitor the status of applications

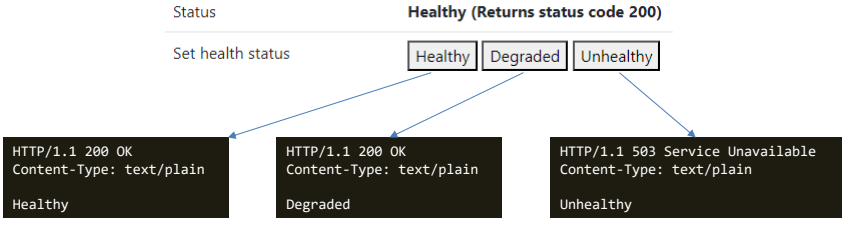
How can we control them?

Health Endpoints

These endpoints use the **Health Checks** Middleware



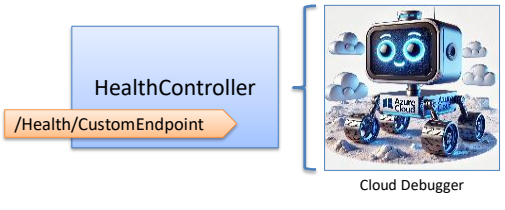
The health can be controlled using:



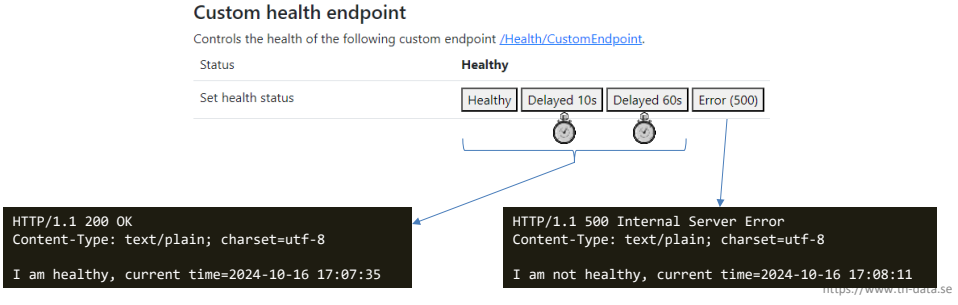
https://www.tn-data.se

Health Endpoints

The custom endpoint is a plain HTTP endpoint



The health can be controlled using:



Thanks for listening!

Contact me at tore@tn-data.se

Follow me on LinkedIn

Cloud Debugger – Open Source at https://github.com/tndata/CloudDebugger

- Try it out!
- Submit PR!

www.tn-data.se

- Email: tore@tn-data.se
- Web: https://www.tn-data.se
- Blog: https://www.nestenius.se