DevOps Wiki

Warning: Documentation generated from markdown files Generated at Tue Dec 10 10:08:57

Contents

External Context

The external facing part of the network is the part that is visible to the public.

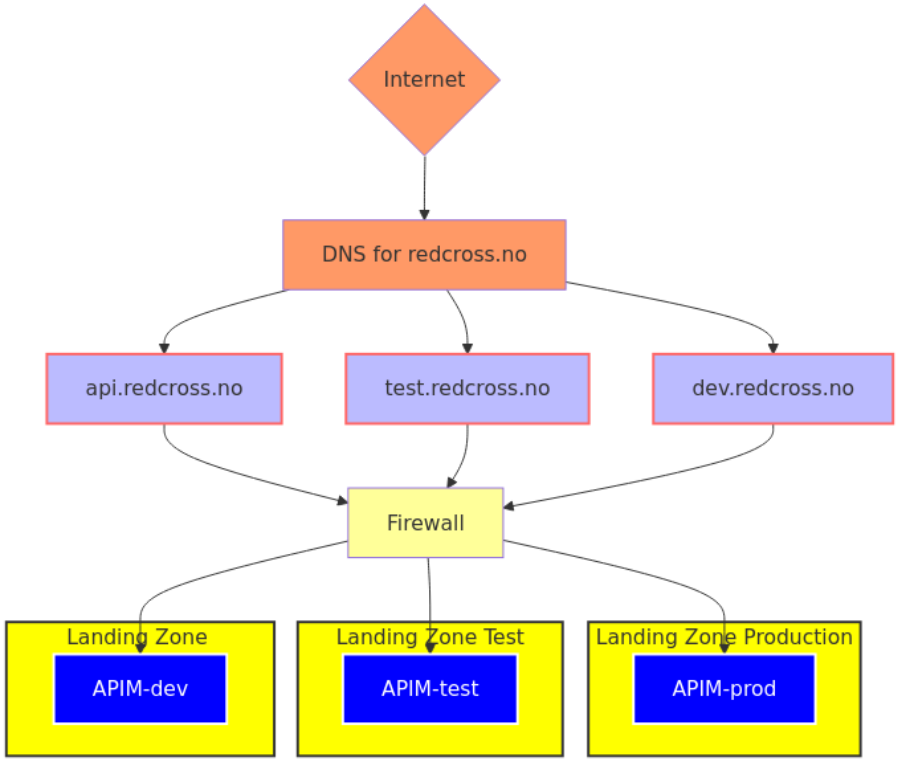

Figure 1: diagram

Subdomains and their routing

Our domain is redcross.no The new infrastructure will have 3 subdomains that are exposed to the outside. These are:

Subdomain	Description	Dest landing zone	Dest "host"
api.redcross.no	Production API	Landing Zone Production	APIM-prod
test.redcross.no	Test API	Landing Zone Test	APIM-test
dev.redcross.no	Development API	Landing Zone Development	APIM-dev

All of these subdomains are pointing to the same firewall.

The firewall routes traffic based on the subdomain to the correct landing zone.

DNS

redcross.no is the domain. It is hosted on the DNS server in the “Betala per anvending” subscription.

When we set up the new subscription we point the DNS records defined in External facing to the new DNS server.

Firewall

The firewall is the first line of defense for the network. It is the only part of the network that is exposed to the internet. The firewall routes traffic based on the subdomain to the correct landing zone.

Firewall functionality

We are using Azure Application Gateway as a firewall. The Application Gateway is the only resource with a public IP address. The Application Gateway terminates SSL and routes traffic based on subdomain.

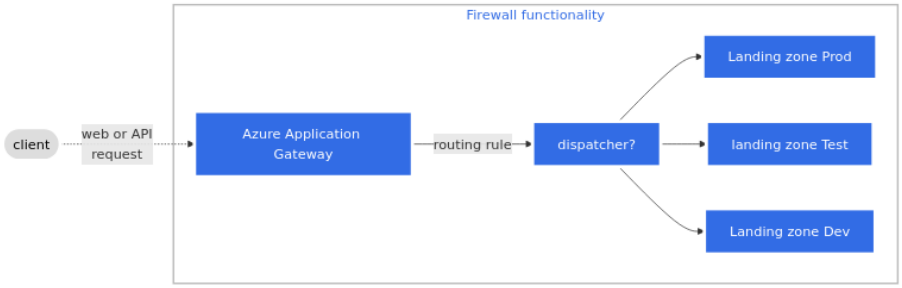

Figure 2: diagram

For mre details see:

What	Description
Firewall Rules	describes the firewall rules
Firewall SSL termination	describes the SSL termination on the firewall
Firewall doc	describes firewall doc
Firewall logging	describes how to set up logging for the firewall

Firewall documentation

We are using Azure Application Gateway as a firewall. Documentation for the product is available at Azure Application Gateway documentation.

Our special configuration is described below.

TODO: Describe the configuration of the firewall.

Firewall Rules

Below are the firewall rules for integrations in Red Cross Norway.

hostname	Source	Destination	Port	Protocol	landing Zone	Description
api.redcross.no	*	APIM-prod	443	HTTPS	Production	API for the Red Cross
api.redcross.no	*	APIM-prod	80	HTTP	Production	API for the Red Cross
test.redcross.no	*	APIM-test	443	HTTPS	Test	test API for the Red Cross
test.redcross.no	*	APIM-test	80	HTTP	Test	test API for the Red Cross
dev.redcross.no	RC Intranet	APIM-dev	443	HTTPS	Development	dev API for the Red Cross
dev.redcross.no	RC Intranet	APIM-dev	80	HTTP	Development	dev API for the Red Cross

NOTE: The `RC Intranet` is the internal network for the Red Cross Norway. It is not accessable from the internet.

Firewall SSL termination

Our SSL certificate is a wildcard certificate for redcross.no. The certificate is installed on the Azure Application Gateway.

Currently the certificate is installed on the Firewall on the "Betala per anvending" subscription. When we set up the new subscription we will install the certificate on the Azure Application Gateway. Then we will point the DNS records defined in External facing to the new Application Gateway.

TODO: Jah - is the certificate installed on the FW in the new subscription or the old?

Firewall Logging

This document describes how to set up logging for the firewall. We are collecting all logs in Sentinel.

TODO: Add information about logging and who is responsible for monitoring the logs.

Landing Zones

Integrations are using three landing zones. The landing zones are separate environments for production, test, and development. The landing zones are isolated from each other. Each landing zone has its own set of resources.

Integration Landing Zones

The landing zones are:

Landing Zone	Long name	Description
landing-prod	prod - azure integrations -az - red cross	production landing zone
landing-test	test - azure integrations -az - red cross	test landing zone
landing-dev	dev - azure integrations -az - red cross	development landing zone

IMPORTANT: Isolation The landing zones are isolated from each other. It means that an application running in one landing zone cannot access a resource in another landing zone. The landing zones are isolated to prevent unauthorized access to resources.

IMPORTANT: No inbound access There is no way to access any resources in the landing zones from the internet or the redcross internal network. All access to the landing zones is through the firewall.

Because of the isolation, the build server is the only way to deploy applications to the landing zones. The build server has access to all landing zones and can deploy applications to any of them. See more about the build server in the build server documentation.

Landing Zones diagram

The diagram below shows the landing zones and the resources in each landing zone.

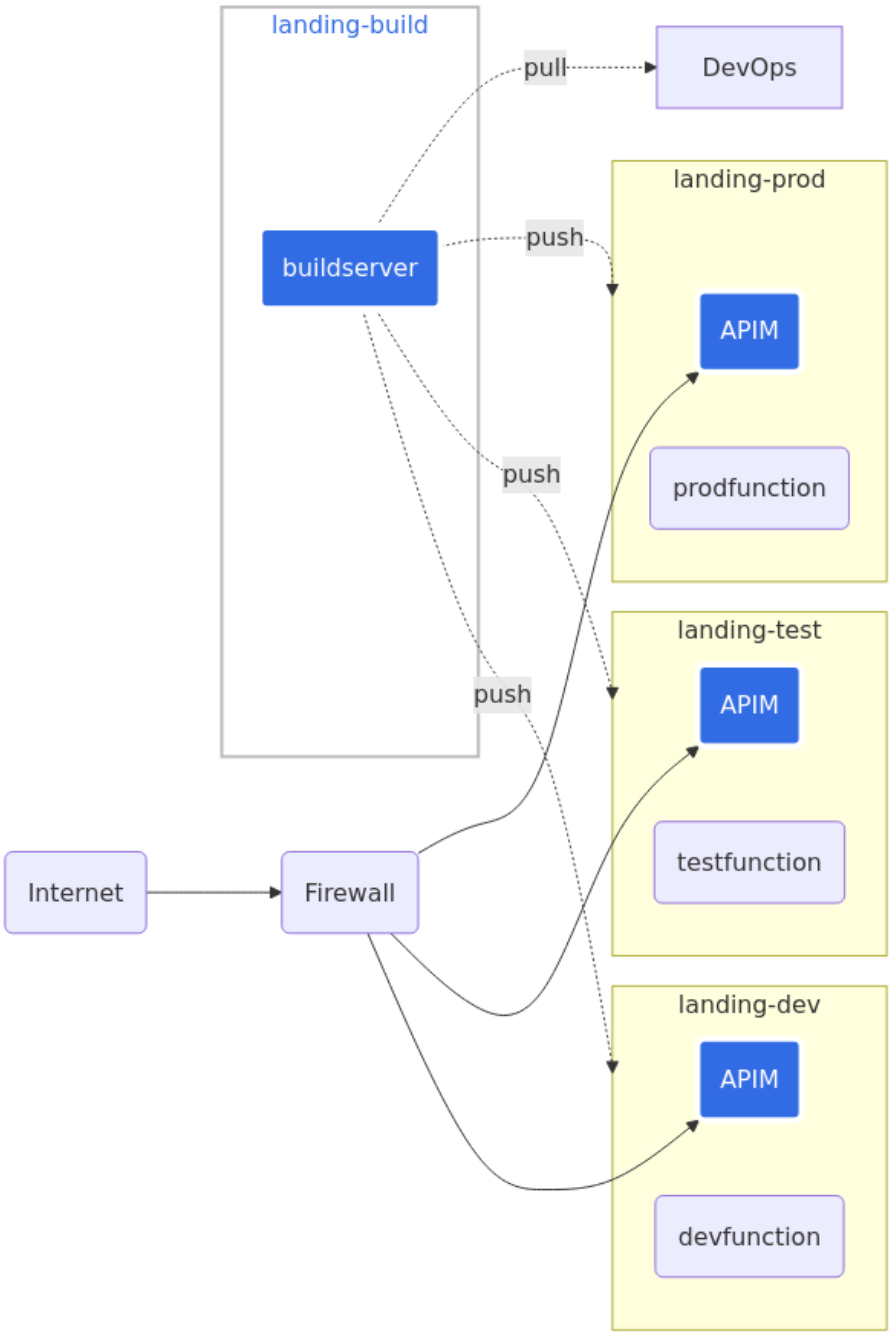

Figure 3: diagram

Landing Zone documentation overview

Landing zones are like subnets. They are isolated from each other. As a general rule there are no comminication between landing zones.

There can be exceptions to this rule, but they should be well documented.

Landing Zone Production

The production landing zone is where the production systems are located. The landing zone is accessable from the internet.

Landing Zone Test

This zone is accessable from the internet. It is used for testing systems before they are moved to production. It has the same security rules as the production zone.

Landing Zone Development

This zone is used for development. It is not accessable from the internet.

TODO: The dev landing zone can only be accessed from the internal network. How is this done?

Landing Zone Build

This zone is used for the build server. It is not accessable from the internet.

Landing Zone Production details

The production landing zone is where the production systems are located. The landing zone is accessable from the internet.

Any details about the production landing zone should be documented here.

Communication rules

All communication between systems must follow these rules.

Internal communication (between systems internally)

Communication between internal systems must use Azure API Management (APIM). This is to ensure that we have a single point of entry for all communication. This makes it easier to monitor and secure the communication.

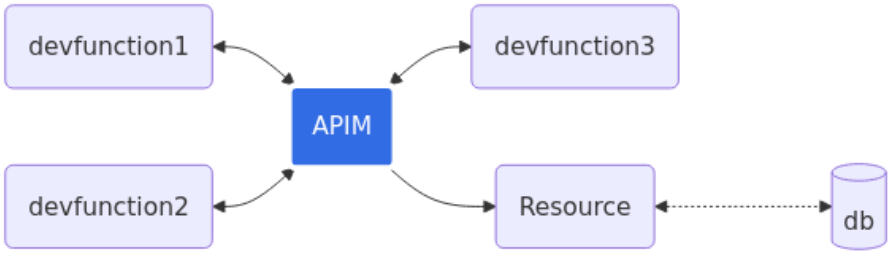

Figure 4: diagram

In the example above, the `devfunction` is an Azure Function that is calling a `resource`. The resource is a web service that is accessing a database. The Azure Function is calling the resource through APIM.

Functions can only call resources through APIM.

External communication (from internal systems to external systems)

Communication from internal systems to external systems must use Azure API Management (APIM). We are doing this so that we can respond to changes on external APIs. If an external API changes, we can update the APIM to reflect the changes. This way, we don't have to update all the internal systems that are calling the external API.

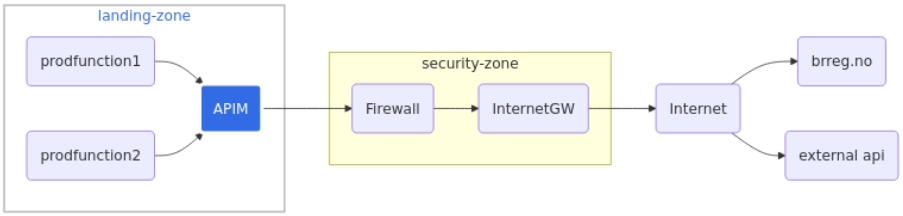

Figure 5: diagram

Requests from external systems to internal systems

Requests from external systems to internal systems will first go trugh the firewall and then to APIm in the landing zone. See External facing for more information.

APIM will route the request to the correct internal system.

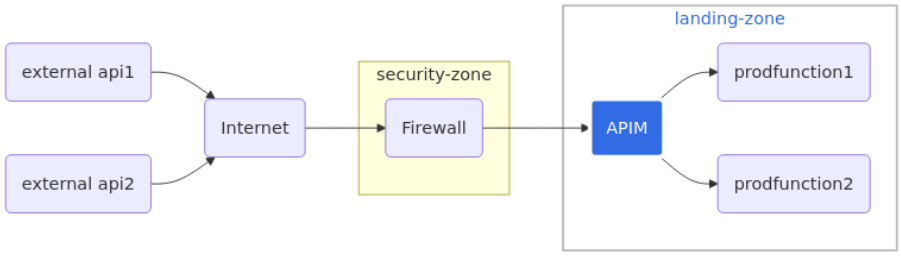

Figure 6: diagram

Definition of external systems

All systems on the old Azure "Betala per andvending" are external systems.

External systems are systems that are not part of the new Azure environment. These systems are accessed through the internet.

TODO: we need to make everyone aware of the consequences of this.

Communication rules exceptions

This document describes what is needed to make an exception to the communication rules defined in 6-0communication-rules.md.

TODO: If there should ever be exceptions to the comminication rules. We ned to document how we make exceptions to the rules.

Development

This document describes the development setup for Red Cross Norway. It is intended for developers who create and maintan integrations.

- Build server
- DevOps
- Azure Functions
- Naming conventions
- Infrastructure as code
- Development Security

Build server

Deploy from DevOps does not work because DevOps has no access into the Landing zones. There is therefore a build server.

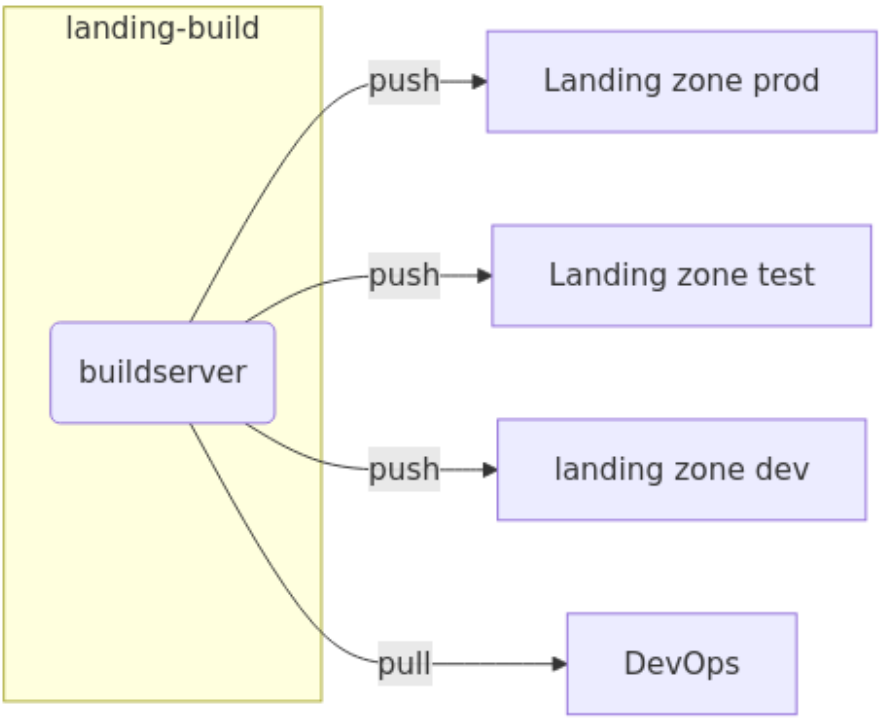

Figure 7: diagram

The build server is a virtual machine that has access to the landing zones. The build server is monitoring the source code repository for changes. When a change is detected, the build server pulls the source code and builds the application. The build server then deploys the application to the correct landing zone.

How to set up the build server for a repository

TODO: Describe how to set up the build server for a repository.

DevOps

Azure DevOps services are used during development and deployment of integrations.

Development Process

1. Get IntegrationID according to Naming conventions from the central register of integrations.
2. Identify the repo to be use. It might be an existing repo according to the central register of integrations. If a new repo is needed create the repo and follow naming conventions. TODO: Naming?
3. Secret information e.g. usernames, passwords, subscription keys, certificates should never be commited into a repo. Use Azure Key Vault for storing secrets.
4. Use Managed Identity when possible for securing communication between Azure services. Use role-based access control (RBAC) to grant permissions.
5. Always use feature branches and merge to master after a pull request.
6. Always build and deploy integrations with Pipelines. A Pipeline should deploy to all target environments with approvals and checks setup.

TODO: Decide how pipelibe should be setup?

TODO: decide naming conventions for repos.

Repo

All source code should be commited and pushed into a repo. A repo group one or more integrations related to a domain or process. In addition, integrations related to a business applications relation can be grouped e.g. all integrations between system A and system B.

The main folder structure is described in the next section Delivery Pipeline.

Delivery Pipeline

All deliveries of integration artifacts should be orchestrated with Azure Pipelines.

The Delivery pipeline is divided into three parts. The main part which is triggered when new code is pushed to the repository. The stages of the delivery pipeline are implemented here. It is defined in a file called azure-pipelines.yaml. The commit pipeline implements all jobs that should be run to prepare the artifacts for deployment, like compile, validate and test. It is defined in a file called commit.yaml The release pipeline implements all jobs that deploy artifacts to a specified environment. It is defined in a file called release.yaml.

. +– .pipeline | +– commit.yaml | +– release.yaml +– apis +– azure-pipelines.yaml +– components +– resources

Integrio has gathered their best practices into reusable pipeline templates. This standardization minimizes variations and potential errors that can arise from manual configurations or individual interpretations of documentation.

The library and how to use it can be found here: Pipeline Templates

Bicep Modules

Integrio har gathered their best practices into reusable Bicep modules that ensure that every piece of infrastructure is built to the same standards. This standardization minimizes variations and potential errors that can arise from manual configurations or individual interpretations of documentation.

The library and how to use it can be found here: Bicep Modules

Service Connections

The Azure Pipelines that deploys integrations need Service Connections to be able to create and/or updates Azure resources. The existing Service Connections that should be used are listed in the table below.

Name	Target Environment	Description
nrx-integrations-dev-sp	Landing Zone Development	Used to deploy integrations in the DEV environment.
nrx-integrations-test-sp	Landing Zone Test	Used to deploy integrations in the TEST environment.
nrx-integrations-prod-sp	Landing Zone Production	Used to deploy integrations in the PROD environment.
nrx-integrations-payg-sp	Betala per användning	Used to deploy integrations in the old Azure environment (Dev, Staging, Prod).
igr-integration-acr-sp	Integrio Infra	Used to reference Bicep modules published in Integrio ACR.
igr-integration-devops-sp	Integrio DevOps	Used to reference Pipeline templates in Integrio DevOps.

Service Connections Overview

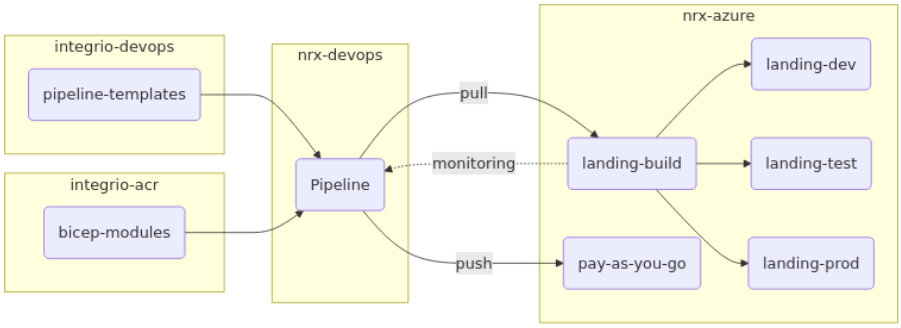

Figure 8: diagram

Azure Functions

Azure Functions is a serverless compute service that enables you to run event-triggered code without having to explicitly provision or manage infrastructure. Using Azure Functions, you can run a script or piece of code in response to a variety of events. Azure Functions can be used to process data, integrate systems, trigger alerts, and more.

CAF naming conventions

Azure Functions should follow the CAF naming conventions.

Programming languages

TODO: we need to decide on which programming languages to support in Azure Functions.

Storage for Azure Functions

TODO: if we decide that each function needs its own storage account, we need to follow CAF naming conventions for storage accounts. We also need to figure out pricing related to storage accounts.

Infrastructure as Code

IaC, Infrastructure as Code, gives the ability to always be able to deploy the same code that has been committed in the repository. Two languages that enables this (together with other tooling) are Bicep and YAML.

Bicep

A recommended way to deploy Azure resources and infrastructure is to use Azure Bicep as IaC (Infrastructure as Code). Bicep gives the advantage of modularity and reusability, and will be compiled and translated into ARM templates (Azure Resource Manager) when deployed. ARM code is relatively verbose and difficult to write, Bicep has a much simpler syntax.

There is a lot of documentation on how to use Bicep, for example: - Microsoft Bicep documentation: https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/ - Microsoft Fundamentals of Bicep: https://learn.microsoft.com/en-us/training/paths/fundamentals-bicep/

In order to develop Bicep code on a developer machine, it is recommended to install and use VS Code and the VS Code Bicep extension.

As mentioned, Bicep has the advantage of being able to organize into modules. Bicep is also idempotent, and the same bicep file can be deployed multiple times if needed, and you will get the same resources and in the same state every time. It is perfectly possible to write Bicep code all from scratch, and even create your own modules. However, to alleviate some of this work (and at the same time get tried-and-tested bicep code), there is also the possibility to use existing modules. These modules exist in a separate repository and can be referenced from your Bicep code. For more information, see Integrio Bicep Modules

YAML

YAML is used when writing the pipeline that constructs the Devops CI/CD chain. There are also pre-created YAML-templates that exists in another separate repository, which can be referenced from your YAML files. For more information, see Integrio Pipeline Templates

---

Terraform

TBD.

Development security

TODO: describe how we handle security in development (service principals, keyvault, etc.)

This document describes:

- service principals
- keywault

Service principals

Keyvault

CAF Naming conventions

We are using CAF naming conventions. The purpose of having defined naming standards is to make it possible to identify what a resource does and where it belongs just by looking at the name.

CAF naming convention for the Azure Functions

We have a central register of all integrations. The IntegrationID is a unique identifier for each integration. The IntegrationID is used in the name of the function app.

The format of the integration ID is "int" followed by a three-digit number. The number is unique for each integration.

TODO: we must make final decition on naming. Can the integration number can be added as a tag?

Functions need to be named in a CAF compliant way:

Name: func-api-testfunction-int0001-euw

Keyword	Example	Chars	Description
	`func`	3	Indicates the resource is a Function App.
	`api`	3	Denotes the integration landing zone.
	`testfunction`	12	Specifies the name of the function app.
	`int001`	6	The unique IntegrationID from our tracking system.
	`eus`	3	The region abbreviation for East US.
	`01`	2	A two-character hexadecimal to make the name unique. An instance or sequence number for versioning or multiple instances.

CAF naming convention for Azure Storage accounts

Azure Storage account names must be between 3 and 24 characters in length and can contain only lowercase letters and numbers. And it ***must be unique across all of Azure***.

TODO: Storage accounts are hard to name as they must be unique across all of Azure. What is the best practice for naming?

Because of the lenght of maximum 24 characters we have limited the length of the integration ID to 6 characters.

Name: stapitestfnint001eus01

Keyword	Example	Chars	Description
	`st`	46	2 char that denotes it's a storage account.
	`api`	64	Max 4 char that indicate landing zone. Indicates it's part of the API landing zone.
	`testfn`	22	6 char for the name
	`int001`	24	6 char Integration ID
	`eus`	61	3 char that Specifies the Azure region (East US) for the storage account.
	`01`	60	A two char hex to make the name unique.

The above rule will use the maximum length of 24 characters.

Functions have separate storage accounts so that different teams do not interfere with each other. This is a best practice for isolation and security.

TODO: What is the costs associated with storage accounts? Should we have separate storage accounts for each function app?

Costs

This is an overview of the costs for the infrastructure for Red Cross Norway.

Product	Description	Version	Monthly Cost
Azure Application Gateway	Firewall		*?1
Azure Web Application Firewall (WAF)	Firewall - exploits protection	included	
Azure DDoS Protection	Firewall - DDoS protection	Basic is included	
Azure API Management	APIM prod	API Management, Standard v2	kr7,523
Azure API Management	APIM test	API Management, Standard v2	kr7,523
Azure API Management	APIM dev	API Management, Standard v2	kr7,523 *?2
Landing Zone Prod	Landing zone for production		
Landing Zone Test	Landing zone for testing		
Landing Zone Dev	Landing zone for development		
Landing Zone Build	Landing zone for build server		
Build server	Linux VM that builds and deploys		

Questions:

1) "Azure Application Gateway: Overview: Azure Application Gateway is a platform-managed, scalable, and highly available application delivery controller (ADC) as a service. It provides layer 7 load balancing, centralized SSL offload, and integrated web application firewall (WAF) capabilities." Azure DDoS Protection Basic is included, Standard is an extra service. It seems that all the stuff we need is in the same product. We already have a firewall in the new CleanAzure subscription. It is named afw-prod-hub-network-euw so we do not need another one!

2) Can we use the API Management "Basic" or developer tier instead of "Standard v2" for the dev landing zone? See costs for API Management here

Infrastructure / integrations documentation for Red Cross Norway

This document describes the infrastructure and how to develop integrations for Red Cross Norway. It is intended for developers and administrators who work with integrations.

All documentation here is automatically compiled into one PDF that can be found here. In the PDF file you will find a list of TODO:s that are not yet implemented in the documentation.

- Readme first
- Generated TODO list
- Costs
- External facing
- DNS
- Firewall
  - Firewall documentation
  - Firewall Rules
  - Firewall SSL termination
  - Firewall logging
- Landing Zones for integrations
  - Landing Zone documentation
- Rules for communication (in and out of our systems and between internal systems)
- Communication rules exceptions
- Development setup
  - Build server
  - DevOps
  - Azure Functions
  - Infrastructure as code
- CAF naming conventions
- how we write the documentation

Generated list of TODO:s

Warning: List of pending tasks extracted from documentation Generated at Tue Dec 10 10:08:57 UTC 2024

Section	TODO Item
Firewall documentation	TODO: Describe the configuration of the firewall.
Firewall SSL termination	TODO: Jah - is the certificate installed on the FW in the new subscription or the old?
Firewall Logging	TODO: Add information about logging and who is responsible for monitoring the logs.
Landing Zone Development	TODO: The dev landing zone can only be accessed from the internal network. How is this done?
Definition of external systems	TODO: we need to make everyone aware of the consequences of this.
Communication rules exceptions	TODO: If there should ever be exceptions to the comminication rules. We ned to document how we make exceptions to the rules.
How to set up the build server for a repository	TODO: Describe how to set up the build server for a repository.
Development Process	TODO: Decide how pipelibe should be setup?
(No heading)	TODO: decide naming conventions for repos.
Programming languages	TODO: we need to decide on which programming languages to support in Azure Functions.
Storage for Azure Functions	TODO: if we decide that each function needs its own storage account, we need to follow CAF naming conventions for storage accounts. We also need to figure out pricing related to storage accounts.
Development security	TODO: describe how we handle security in development (service principals, keyvault, etc.)
CAF naming convention for the Azure Functions	TODO: we must make final decition on naming. Can the integration number can be added as a tag?

Section	TODO Item
CAF naming convention for Azure Storage accounts	TODO: Storage accounts are hard to name as they must be unique across all of Azure. What is the best practice for naming?
(No heading)	TODO: What is the costs associated with storage accounts? Should we have separate storage accounts for each function app?