IHE SERVICES | Building trust in eHealth interoperability

Configuration sharing

Cédric Eoche-Duval

Agenda

- Sharing of Configurations
  - The concept of “Configuration” in Gazelle
  - Editing and approving your configurations
  - Retrieving configurations for partners
  - OIDs

CONFIGURATION CONCEPT

Online Connectathon : Test network over internet

- Online Connectathon is exchanging test data between peers all over the world
  - Usage of internet infrastructure
  - Public IP addresses for the systems under test
    - Each system must have static IP address
    - An IP address can be reused for several systems in the same company
  - Fully Qualified Domain Name (FQDN) registration
    - Each IP address should have a domain name registration
    - Will rely on public DNS (with hosts file backup)
  - Firewall setup according to Gazelle Configurations

Gazelle concepts of “hosts“ and “configuration”

- Hosts are node on the network (endpoints or devices)
  - IP address
  - FQDN in case of online event
- Configurations are interfaces of IHE actors implemented by the system
  - Bound to an actor and a system
  - Type (HTTP WS, HL7v3 on SOAP, HL7v2, DICOM…) and as responder or initiator
  - Node on which this interface is hosted
  - Port in case of responder
  - Additional information depending on the Configuration type (Resource URL, AETitle, Application/Facility names etc)

Default configurations

- In advance of the Connectathon
  - The project manager asks the tool to generate the default configurations for each system
    - No IP address is assigned (only fake hostname)
    - All configuration are said “not approved”
  - The SUT operator
    - Review the hosts generated, define its IP address(es) and complete the hostname with the fully qualified domaine name associated to its IP.
    - Reviews the generated configuration entries and update them to match the actual configuration of his system
    - Marks the configurations “approved” when they are ready to be used by others

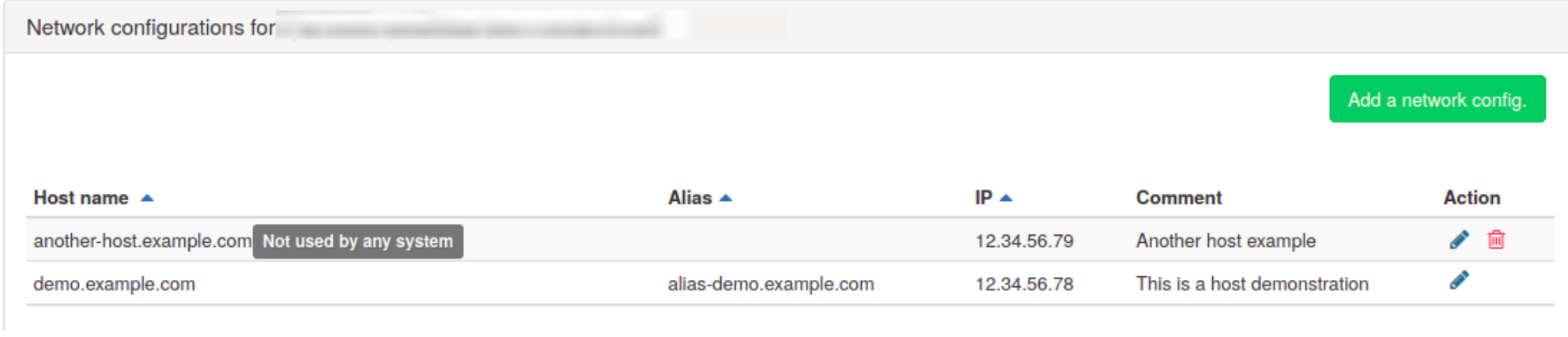
All the information in one place

- Gazelle Test Management allows
  - Listing of all the endpoints of each system under test
    - Configurations > All configurations
    - By default, list is filtered to show only entries for your company
  - Download of the hosts file
    - “Download hosts file” button at the bottom of the Network Configuration Overview page
    - List all registered nodes in the test session
    - Input for firewall filtering whitelist
    - Backup plan to prevent DNS propagation delays
  - Retrieval of the systems’ endpoints as CSV file
    - Link “URL for downloading configurations as CSV” on top of the “all configurations” table.

EDITING CONFIGURATIONS

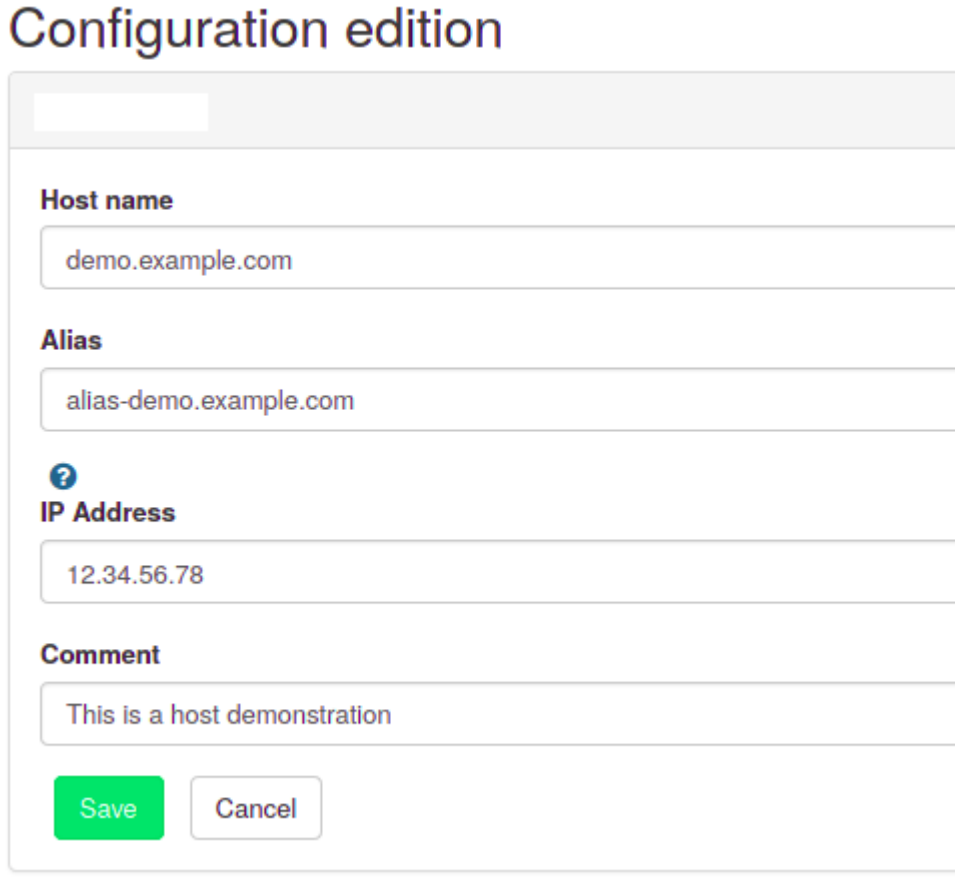
Review the generated hosts for your system

- Once the Connectathon project manager announces it, review the hosts generated for your system and adapt them
  - From Configurations > MY COMPANY: Systems Configuration
- For each entry, you can
  - Edit
  - Delete unassigned hosts



Review the generated hosts for your system

- Host name must be the fully qualified domain name
- Alias is optional
- IP Address must be the static public IP through which your system's machine will be accessible or through which your system will reach out other systems.

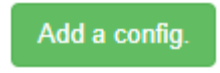


Review the generated configurations for your system

- Then, review the configurations generated for your system and adapt them
  - From Configurations > MY COMPANY: Systems Configuration
- For each entry, you can
  - Edit
  - Approve *(Only approved configurations will be visible to test peers)*
  - Delete
- There might be duplicates: TLS and non-TLS
  - Although your system is an ATNA/Secure Node or Secure application, not all test cases require to use TLS
  - Gazelle Proxy is not yet able to decode TLS encrypted exchanges

Tips

- You can ask for additional hostnames (nodes) 

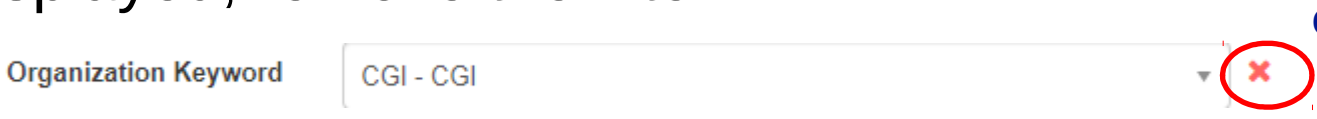
- You can add additional configurations (interface) 

- You can approve a batch of entries
  - Use ✔ button from the table header
- You can use the same hostname for different systems in your organization
  - It might be useful if several systems are hosted on the same node
- When a non-TLS endpoint is marked approved, a port appears in red between bracket
  - This is the port to be used on the proxy (see other presentation)

SHARING CONFIGURATIONS

Retrieve your partners' configurations

- From menu **Configurations** > **All configurations**
  - By default, only configurations for your company are displayed, remove the filter



- From the test instance page
  - When a test is started, in the **Test Participants** section

- As a CSV file
  - Parametric URL is given in the **All configurations** page

  - User manual

Which details are shared ? (1)

- DICOM

Sys	Table	Actor	Host name	IP	Port	is Secured ?	AE Title	SOP class	Approved
PACS_AGFA_1 / AGFA	J3	CHANGE_REQUESTER - Change Requester	agfa68	172.16.0.206	104(13024)		AGFA_PACS	STORAGE	yes

Hostname, IP address and port when you DO NOT use the proxy

Port to use in conjunction with the IP address of the Proxy for the messages to be captured

- HL7v2

Sys	Table	Actor	Host name	IP	Port	is Secured ?	Receiving application / facility	Namespace	Approved
OF_RDI_LTW / RDI	A2	AM - Automation Manager	rdi5	172.16.1.18	20468(12412)		OF_RDI_LTW / RDI	RDO2	yes

Assigning authority to be used by this system

- HL7V3

Sys	Table	Actor	Host name	IP	Port	is Secured ?	WSType	URL	Namespace	Approved
OTHER_InterSystems_HS17 / InterSystems	K4	DOC_REGISTRY - Document Registry	intersy	172.16.0.108	80(12391)		ITI-44:Patient Identity Feed HL7 V3	http://intersystems12/csp/connect/HS.IHE.XDSb.Registry.Services.cls	INO2	yes

Which details are shared ? (2)

- Webservices

Sys	Table	Actor	Host name	IP	Port	is Secured ?	WSType	URL	Approved
OTHER_InterSystems_HS17 / InterSystems	K4	DOC_REGISTRY - Document Registry	intersystem	172.16.0.108	443	☑	ITI-18:Stored Query:sq.b	https://intersystems12/csp/connect/HS.IHE.XDSb.Registry.Services.cls	yes

This port is protected by TLS

- Syslog

Sys	Table	Actor	Host name	IP	Port	is Secured ?	Transport	Protocol	Approved
PACS_synedra_2017 / synedra	K7	ARR - Audit Record Repository	synedra22	172.16.0.69	11641(12643)	☐	TCP		yes

TCP or UDP

OIDs

OIDs

- Some integration-profiles requires OIDs to identify the system or the module participating in a transaction.
- At each testing event, the technical management team use Gazelle to generate and assign new OIDs to all systems and all actors that need OID(s) according to their registration.
- Once the OID generation have been announce by the technical team, you will have to setup your system using the given OIDs.

OIDs

- Find the OIDs assigned to your system
  - From **Configurations** > **OIDs for current session**
  - Filter on your system 

  - A label gives the purpose of use of each OID
- Find the OIDs assigned to your partners
  - On this same page
    - Remove the filter on your system
    - Filter on a given company or system
  - From the “Test Participants” section on a test instance page
  - Using the parametric URL to download the CSV file (see previous slide)

IHE SERVICES Building trust in eHealth interoperability

Configuration sharing

Cédric Eoche-Duval