Security : *“Lock up when you go”*

Pre-Conference Session, IBUC 2018

Statistics Netherlands

Agenda

- Blaise 5 server roles
- Communication between roles, HTTPS
- Userid for communicating with databases
- Database encryption and .bdix security
- Permissions, authentication, users, roles

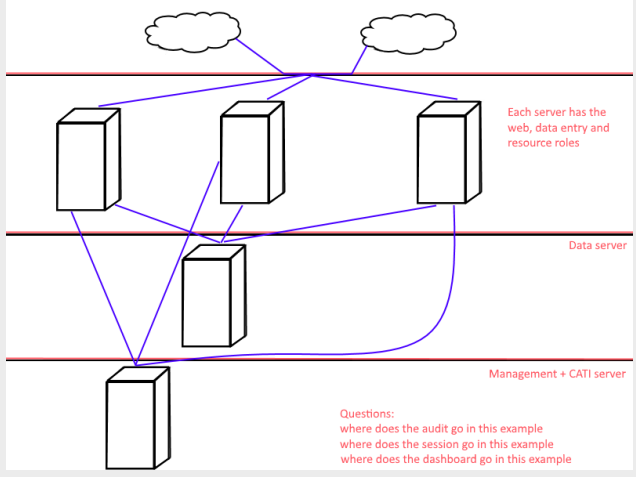
Blaise 5 server roles

- Servers can have one or more of the following roles:
- management
- audit trail
- CATI
- data
- data-entry
- resource
- session
- web
- dashboard

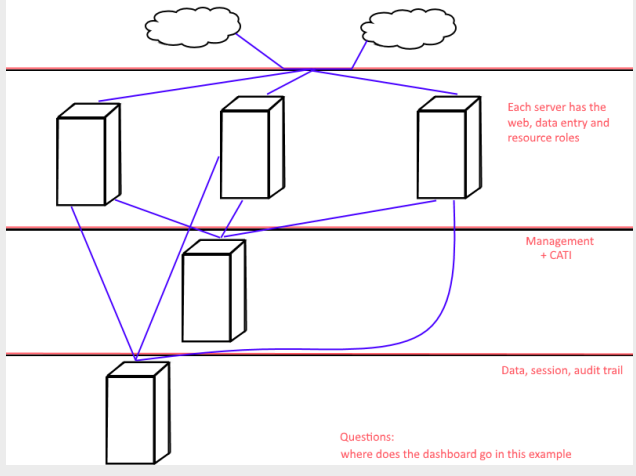
Server protection - external

- Isolate sensitive roles
- Use firewalls
- Use multiple zones
- If using the new Upload control to a BLOB type, remember to virusscan the item before doing anything with it

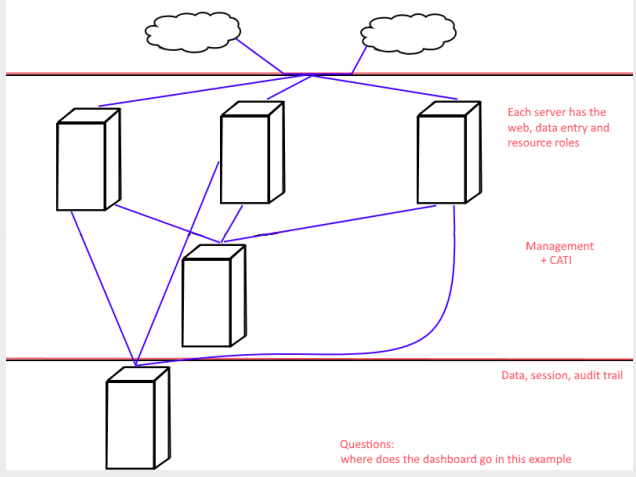
Sample server layout - 1



Sample server layout - 2



Sample server layout - 3



Communication - 1

- The roles communicate with each other using certain ports
- By default these are
  - 8031 – management communication
  - 8033 - data entry communication
- These are customizable during installation or by later editing of the configuration files but it's easier to have this planned out beforehand and to do it at installation

Communication – 2

- Communication between roles needs a protocol
- Blaise 5 uses the HTTP protocol definition to send messages between the various roles
- This does NOT mean that you need IIS installed (only the webserver and dashboard roles need IIS)
- You can secure the internal connections by going to HTTPS

Communication - 3

- You can change various settings via the Server Manager
- Start the Server Manager via "Run as administrator"
- Select the Home tab
- Click on Local server
- Choose Configuration Settings
- You can change the bindings here but remember that you need the appropriate certificates
  - it is better to have planned this from the start

Communication - 4

Configuration Settings

OK | Cancel

Management Communication Port: 8031

Service Status

Management Binding: HTTP

Windows Firewall : Add Exceptions

Data Entry Communication Port: 8033

Data Entry Binding: HTTPS (needs certificate)

Connection (Server) Certificate:
- Store Location:
- Store Name :
- Thumb Print :

Authentication (Client) Certificate:
- Store Location:
- Store Name :
- Thumb Print :

IsDataServicePubliclyHosted: Host public

Communication - 5

Server Roles

Restart Services

Server Type : Master — Port '8031', Binding 'http'

Server Roles :

Name	Port	Binding
WEB	80	http
DATA	8033	http
DATAENTRY	8033	http
RESOURCE	8033	http
SESSION	8033	http
AUDITTRAIL	8033	http
CATI	8033	http

Plan carefully and read the help!

- Consider your requirements carefully
  - are you doing web
  - are you doing smartphone/tablets with communication of data
  - have you got the correct connection certificate(s) for HTTPS
  - are you allowed to upload into your production environment
  - how do you virus-scan any BLOB types that are uploaded
- There is a lot more information in the help

Service Account for databases

- If using a server based backend storage solution such as MS SQL Server, Oracle etc.
- Set up a Service Account to restrict access to the tables in the SQL database
- Assign the Service Account the appropriate rights
- Run the Blaise 5 services under the Service Account
  - usually means having the database password for the Service Account available when switching the startup parameters for the services

Database encryption

- The iOS and Android apps always encrypt the data on the device
- You can encrypt a .bdbx at creation time as it's an SQLite dB
  - you cannot switch from unencrypted to encrypted once the tables have been made
- Supply a password for the .bdbx in the .bdix
  - the .bdix is saved encrypted
  - you can password protect the .bdix itself
- For other database systems, consult the appropriate manual

- Plan ahead and read the help!

Permissions, authentication, users, roles

- Fine-grained security access is organized in different layers
  - OS level to define who can access files, resources etc.
  - IIS level to allow various actions
  - External login controls
  - Blaise level to define user access to functions and data

OS & IIS level restrictions

- Beyond the scope of this presentation but include such things as:
  - firewalls to control access and traffic
  - access to directories and files
  - whether uploads are allowed
  - whether executing scripts or programs is allowed
  - etc.

External login controls - 1

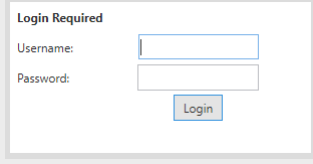
- Authentication occurs outside the Blaise instrument
- Pass userid and password or a locally encrypted combination thereof to an external program and receive *success* or *failure*
- Alternatively, can use a hardware device to supply a one-time authentication *token*
- Usually only needed once for stateful systems (Windows DEP)
- For a web solution, login status needs checking more frequently (think: bookmarks)
  - use an IIS module to check login status at server contact

External login controls - 2

- If you are legally obliged to use an external authentication system, consider:
  - how often you have to authenticate
  - how you maintain the security of the system when going out to the external service
  - how you maintain the security and integrity of what you get back
  - what traffic needs to be enabled through the firewall and to/from where

Blaise 5's Login Required setting

- On the Settings tab, there is a Login Required checkbox
- Checking this does what it says... a login is required



- What does it check the Username and Password against?
  - Blaise user definition
  - Active Directory

Users, passwords, roles, skills - 1

- In the Server Manager it's possible to define users, their password and what parts of the system they have access to.
- Here are some previously defined users:

Name	Role	Description
CMUser	CMUser	
Fred	InterviewerRole	A senior interviewer
Barney		A younger interviewer
Finn	InterviewerRole	Finn is a user in the BCS setups. If using the special offline CAPI block then you need to have the ToWhom
Wilma		A quick description via IUser2

Users, passwords, roles, skills - 2

- The lower half of the display shows detailed information about the selected user.

Name: Fred

Description: A senior interviewer

Parks:
- hyperv_1085
- LocalDevelopment
- StandAlone
- WestatTest

Skills:

Action	User permission	Role permission	Effective permission
Deployment			
Apps			
App usage		✓	✓
Enabled features in apps			
Survey Data Access		✓	✓
User Management			
CATI Management			

Users, passwords, roles, skills - 3

- Creating a new user requires:
  - name
  - password (including confirmation of password)
  - description
  - which server parks the user is allowed to operate in
  - a role (if any)
  - a list of skills (if any)
  - definition of which permissions the user has, e.g.
    - install surveys
    - add user
    - etc.

Users, passwords, roles, skills - 4

- Users' information can be edited
- Note that the username cannot be changed
- The password may be changed via a separate dialog

- Users can be deleted

Users, passwords, roles, skills - 5

- Roles define a pre-determined set of permissions to enable quick allocation of permissions to a user
- Examples:
  - dailyadmin: install surveys, create/edit/delete users
  - serverparkadmin: define serverparks, install surveys

- There are multiple settings under the following groups:
  - Deployment
  - Apps
  - Survey Data Access
  - User Management
  - CATI Management

Users, passwords, roles, skills - 5

- Skills detail particular skills for a user, for example:
  - languages spoken
  - interpersonal skills
- When assigning a skill to a user, it is possible to define a level (numeric)
- The instrument's project has a StartCondition and this can be checked against the userid who logs in, e.g.
  - User.HasRequiredSkill('Dutch', 2)
  - User.HasRequiredSkill('Patience', 10)

Active Directory

- It is possible to synchronize with Active Directory
  - this is a one-way synch – items are copied to the local Blaise user collection
  - changes made in the Blaise user collection will NOT be copied back to AD
  - there is a standalone tool to enable scheduled synchronization (SyncAD)
  - for an AD group, a Blaise Role can be specified
  - each user has a switch to turn synchronization on/off
    - if on, user credentials are checked against AD
    - if off, user credentials are checked against Blaise

Security Token Service

- The communications between the Blaise roles are controlled via security tokens
- The Security Token Service checks things (e.g. authentication) and if everything is in order, issues a security token
- The security token is created in JSON Web Token format
- The machine key supplied at installation is used to sign the token
  - all machines in a serverpark must have the same key
- The tokens are encrypted to prevent tampering
- The receiving application checks if the token came from a trusted STS and then acts accordingly

And finally...

- Plan your "physical" security in advance
  - HTTPS certificates, virus scan, DMZs, firewall rules etc.
- Check the rules at your company regarding where you can place data
  - DMZ, other backend area, Production, somewhere else
- Check requirements for database encryption and access
  - don't forget to password protect the .bdix if needed
- Consider what to do about Active Directory, if available
- Remember
  - Security is in your own hands!