



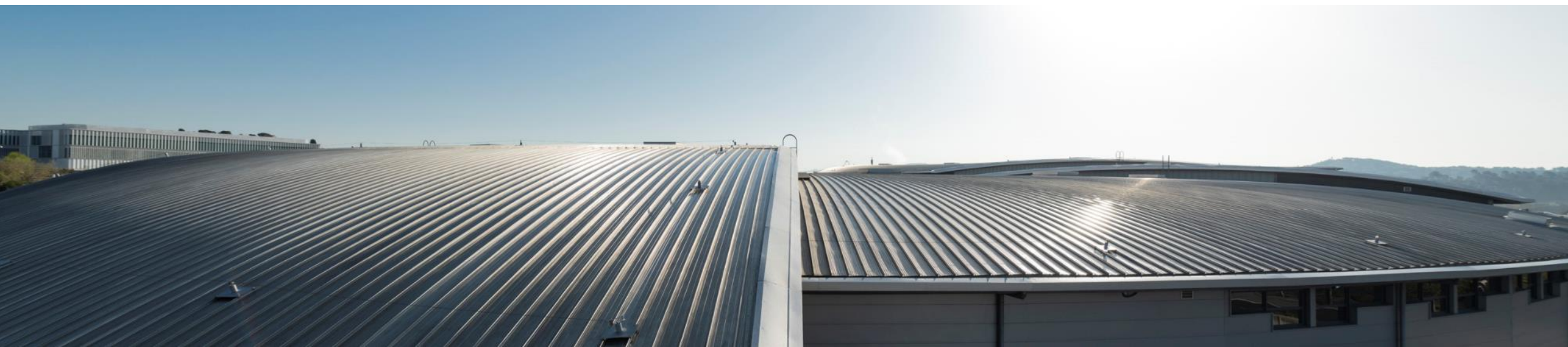
VISA infrastructure and users' Docker image

IT Systems

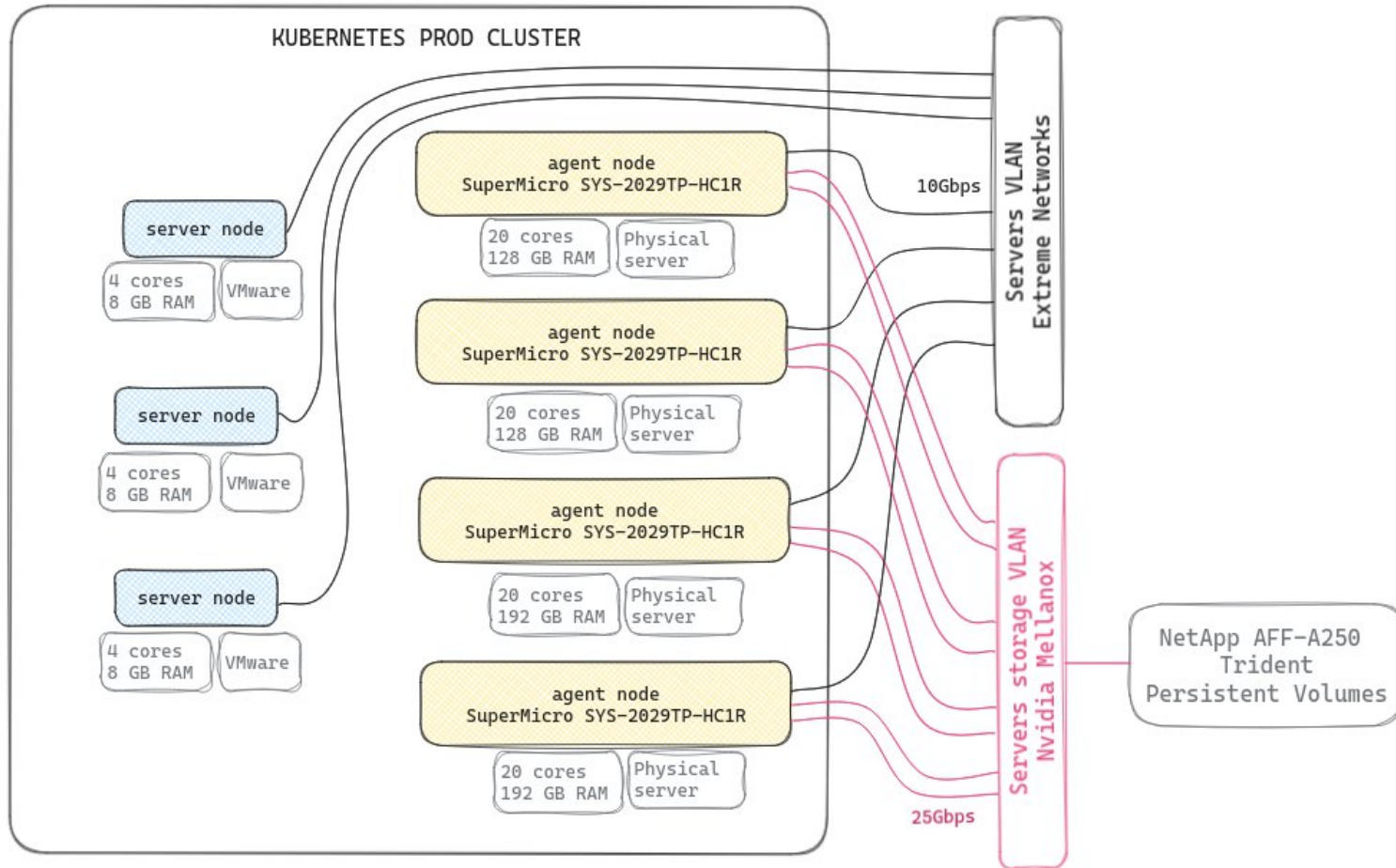
Adara Acarrión Gallegos

Matías Adrián Fisz Ansaldi

02-06-25



Infrastructure



- Kubernetes cluster on premises, v1.28
- RKE2 distribution
- 3 server/master nodes + 4 agent/worker nodes
- No GPUs for the moment
- Network:
 - 10 Gbps network
 - Cilium CNI
- Storage:
 - 25 Gbps network
 - NetApp All Flash (NVMe), trident CSI, persistent volumes
- Management: Rancher v2.8.5

Infrastructure

- **Server Supermicro 2029TP-HC1R**
 - Processor: Xeon 4210R (2.40 GHz) (20 cores)
 - RAM: 192GB
 - GBIC: mngmt:10Gbps and Storage:25Gbps



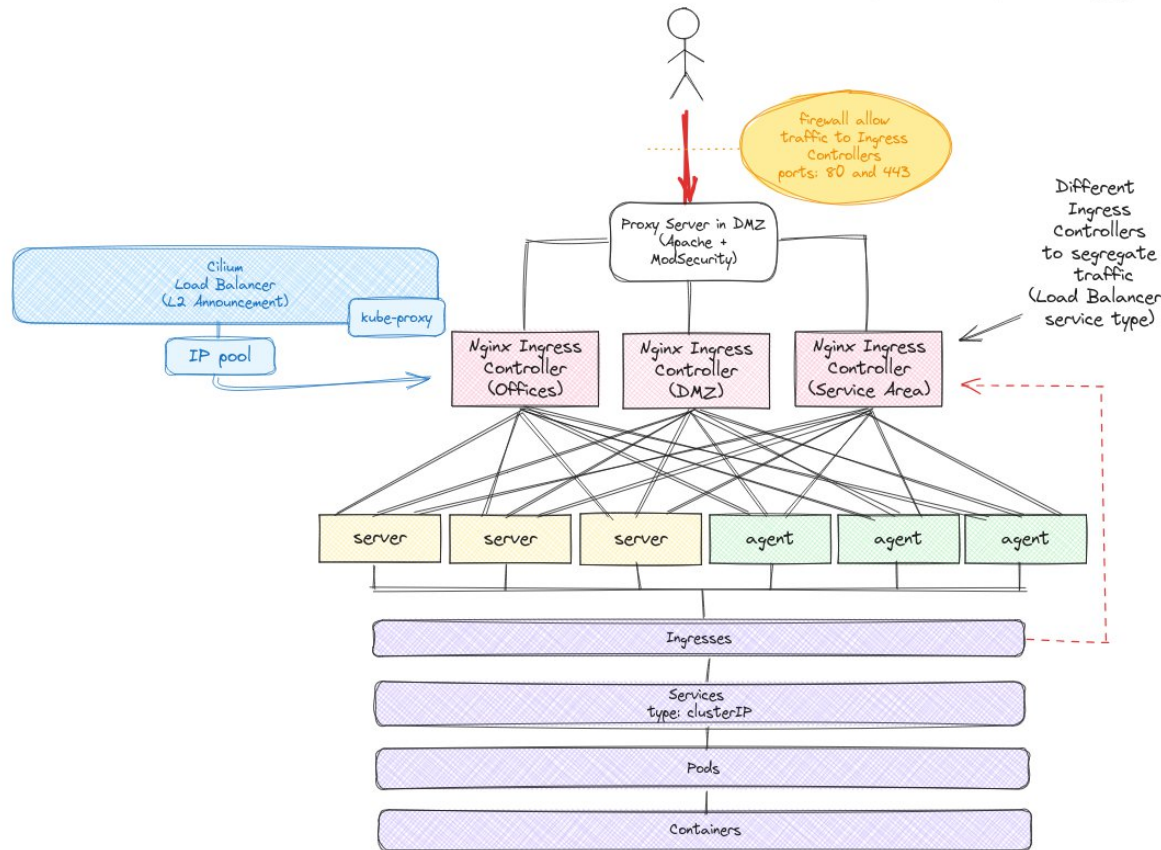
- **Storage Netapp AFF250**
 - 8TB Drives NVMe SSD



- **Networking Mellanox SN2100**
 - Ports: 16 × 100GbE QSFP28



Security

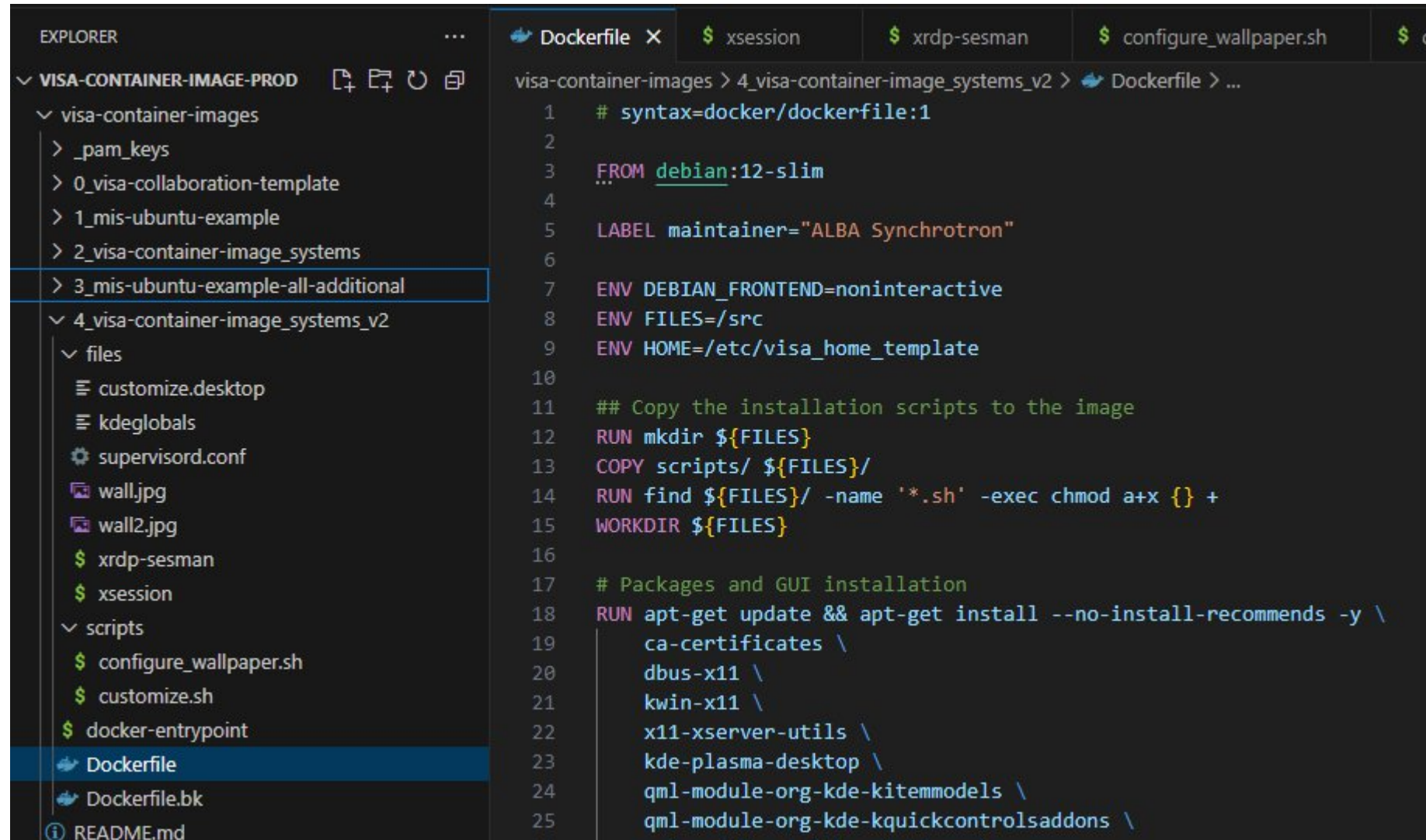


- Proxy Server (Apache) and Web Application Firewall (ModSecurity) in DMZ filtering and allowing traffic only to an specific Ingress Controller
- Dedicated **namespace** for user pods (different than the one where VISA components pods are deployed)
- **Network Policies** to avoid communication between user pods and to other namespaces
- Principle of Least Privilege:
 - Read only access to storage
 - Container user with only the needed LDAP groups
 - Container user without much permissions in the system
 - User pods deployed with a dedicated Service Account with very restricted privileges

User image stored in a **dedicated** project in Harbor, the corporate **Container Registry**

Users' Docker base image

- Based on Debian 12 official Docker image
- Image size: 3 GB
- Graphical Interface: KDE Plasma
- Accessible via RDP (XRDP)
- In separated containers:
 - VISA-PAM
 - Guacamole
 - VISA-cups
 - VISA node-fs



The image shows a code editor with two panels. The left panel, titled 'EXPLORER', displays a file tree for a project named 'VISA-CONTAINER-IMAGE-PROD'. The tree structure is as follows:

- visa-container-images
 - _pam_keys
 - 0_visa-collaboration-template
 - 1_mis-ubuntu-example
 - 2_visa-container-image_systems
 - 3_mis-ubuntu-example-all-additional
 - 4_visa-container-image_systems_v2
 - files
 - customize.desktop
 - kdeglobals
 - supervisord.conf
 - wall.jpg
 - wall2.jpg
 - xrdp-sesman
 - xsession
 - scripts
 - configure_wallpaper.sh
 - customize.sh
 - docker-entrypoint
 - Dockerfile
 - Dockerfile.bk
 - README.md

The right panel shows the content of the 'Dockerfile' selected in the file tree. The code is as follows:

```
1 # syntax=docker/dockerfile:1
2
3 FROM debian:12-slim
4
5 LABEL maintainer="ALBA Synchrotron"
6
7 ENV DEBIAN_FRONTEND=noninteractive
8 ENV FILES=/src
9 ENV HOME=/etc/visa_home_template
10
11 ## Copy the installation scripts to the image
12 RUN mkdir ${FILES}
13 COPY scripts/ ${FILES}/
14 RUN find ${FILES}/ -name '*.sh' -exec chmod a+x {} +
15 WORKDIR ${FILES}
16
17 # Packages and GUI installation
18 RUN apt-get update && apt-get install --no-install-recommends -y \
19     ca-certificates \
20     dbus-x11 \
21     kwin-x11 \
22     x11-xserver-utils \
23     kde-plasma-desktop \
24     qml-module-org-kde-kitemmodels \
25     qml-module-org-kde-kquickcontrolsaddons \
```

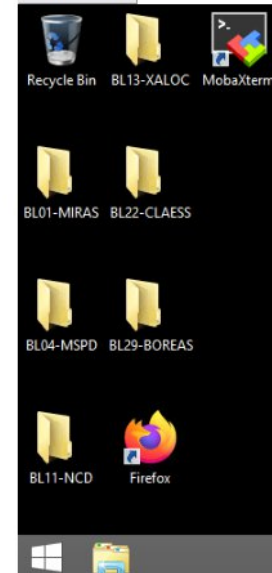
Cells.Gateway

Enter credentials

User name: Password: Password2: IdApplication: 

Resource List

Beamlines Data Analysis Id: [Delivery Controllers.Beamlines Data Analysis:
 • DPH Visa Linux Id: [Delivery Controllers.DPH Visa Linux SP286] Disabled: [false]
 • DPH Visa Linux2 Id: [Delivery Controllers.DPH Visa Linux2 SP289] Disabled: [false]
 • W10 Virtual Desktop Id: [Delivery Controllers.W10 VDI SS30-56] Disabled: [false]

1024 768 

actionSprite_531B7A6FF85CA.
 folder_template_D3D951500A
 viewSprite_B2F322BDC8824F
 favicon_9B19689CB70C681E.ic
 List
 Citrix_HalfHeaderLogo.png
 data:image/svg+xml;...
 folder-root_2D7914C4A01DE
 data:image/svg+xml;...
 data:image/svg+xml;...
 data:image/svg+xml;...
 data:image/svg+xml;...
 GetUserName

```

69: {clienttypes: ["ica30", "rdp"],...}
70: {clienttypes: ["ica30", "rdp"], desktopassignmenttype: "shared",...}
71: {clienttypes: ["ica30", "rdp"],...}
72: {clienttypes: ["ica30", "rdp"],...}
73: {clienttypes: ["ica30", "rdp"], desktopassignmenttype: "shared",...}
74: {clienttypes: ["ica30", "rdp"], desktopassignmenttype: "shared",...}
75: {clienttypes: ["ica30", "rdp"],...}
76: {clienttypes: ["ica30", "rdp"],...}
77: {clienttypes: ["ica30", "rdp"], desktopassignmenttype: "shared",...}
  clienttypes: ["ica30", "rdp"]
  desktopassignmenttype: "shared"
  iconurl: "Resources/Icon/L0NpdHJpeC9TdG9yZS9yZXNvdXJjZXNvdjIvTTRkT01VZE5Sa1YwVDBkMGE
  id: "DeliveryControllers.W10 VDI SS30-56"
  isdesktop: true
  launchstatusurl: "Resources/GetLaunchStatu
  launchurl: "Resources/LaunchIca/RGVsaXZlcn1Db250cm9sbGVycy5XMTAgVkrJICRTMzAtNTY-.ica
  name: "W10 Virtual Desktop"

```

- Citrix PoC with VISA – 2021/2022
- A Proof of Concept (PoC) was initiated with VISA using Citrix during 2021–2022
- The project is currently on hold but can be resumed if required
- Key setup completed:
 - New StoreFront installation
 - IIS configuration + HTML5
 - Creation of VM pools for Virtual Desktops (VDI)



www.cells.es

Cerdanyola del Vallès (Barcelona) Spain

Tel: (+34) 93 592 43 00