Elia Server Standards

Summary	This document describes the Elia IT server standards for hardware, software and operating systems
Version	V4.01
Date	24/03/2025

Document creation and distribution

Author	Wim Michiels /IT
Function	IT Server Team Responsible
File location	STEAM Sharepoint Online (Server_Standards.docx) https://eliagroup.sharepoint.com/:w:/r/sites/IOS/Steam/Public/Server_Standards.docx?d=w4158861e855d499695851ce623973cb6&csf=1&web=1&e=YVC3NW
Distribution	All (internal+external) clients of the Elia IT Server Team

Previous vHersions (changes emailed to ASE/HVDB/GFL for distribution)

Version	Date	Author	Summary of changes
V1.a	16/Sep/09	Wim Michiels	Changes about dedicated servers
V1.B	28/Oct/09	Wim Michiels	Changes about dedicated servers
V2.0	5/Sep/10	Bert Van de Merckt	Major update
V2.1	15/06/2011	Wim Michiels	Minor update (paragraph 6)
V2.2	29/Nov/11	Bert Van de Merckt	Major update (with track changes)
V2.3	10/Jan/13	Bert Van de Merckt	Major update (with track changes)
V2.4	13/10/14	Jonathan Vingerhoets	Major update
V2.5	29/05/2015	Wim Michiels, Bert Van de Merckt	Update about new environments, versions, deployment proces
V2.6	09/09/2015	Wim Michiels	Update about application updates/upgrades / deployments
V2.7	10/02/2016	Jonathan Vingerhoets	Update standard hardware
V2.8	29/02/2016	Wim Michiels	Add POC servers – update dedicated servers
V2.9	10/01/2017	Jonathan Vingerhoets	Add Hardware lifetime Full review
V2.10	08/09/2017	Wim Michiels	Update Win + SQL standards (2016) + security update + exchange 2016
V2.11	19/09/2017	Wim Michiels	Review reboot windows
V2.12	27/09/2017	Wim Michiels	Use of cloud services
V2.13	28/02/2018	Wim Michiels	General update
V2.14	11/05/2018	Wim Michiels	General update
V2.15	05/06/2019	Wim Michiels	Small update
V2.16	21/08/2019	Danny De Haan	Adding Linux as a server standard
V2.17	26/08/2019	Steam Mgt	General update

V2.18	09/07/2020	Jonathan Vingerhoets	Add Temporary Admin account
V2.19	16/10/2020	Wim Michiels	Adding RedHat OJDK as standard
V2.20	25/01/2021	Wim Michiels	Adding naming conventions for on prem and Cloud servers + services
V2.21	19/02/2021	Wim Michiels	Update oracle std (BE + DE)
V2.22	02/06/2022	Jonathan Vingerhoets	General update
V2.23	18/08/2022	Wim Michiels	Adding Mongo db as standard – small update (corrections on contact persons)
V2.24	25/08/2022	Sven Vansteenkiste	Update Mongo db
V2.25	29/12/2022	Wim Michiels	Update backup retentions
V2.26	20/03/2023	Wim Michiels	Update patch timings
V2.27	18/8/2023	Wim Michiels	4 monthly review + small updates
V2.28	12/09/2023	Steven Martens	Small updates on 6.3.4/6.3.5/6.3.6/6.3.8/6.4/6.4.6
V2.29	12/9/2023	Bert Van de Merckt	Small updates on 3, 4.1, 5, 6.1, 6.2, 15.1, 16, 17
V2.30	13/09/2023	Steven Martens	Small update 6.3.8
V2.31	18/09/2023	Jonathan Vingerhoets	Updates on 2.1, 2.2, 2.6, 2.7, 2.8, 2.10, 6.7, 8, 9.1, 9.2, 9.4, 10.1, 11
V2.32	20/09/2023	Pascal Mingeot	Updates on 6.5
V2.33	28/9/2023	Joachim Loser	Updates on 6.3.3, 6.3.12, 15.2
V2.34	21/11/2023	Wim Michiels	Update on 50 Hz service windows (13)
V3.0	16/01/2024	Wim Vercammen	Major update
V3.1	09/02/2024	Wim Michiels	Updates on 2.3, 4.2, 4.4, 10.3, 11, 14
V3.2	09/02/2024	Jonathan Vingerhoets	Updates on 2.1, 2.2, 2.6, 2.7, 6.4, 6.7, 9, 10.1, 10.2, 11, 14
V3.3	29/02/2024	Pascal Mingeot	Updates on 6.3, 6.6
V3.4	29/02/2024	Steven Martens	Updates on 7.1 and 7.2
V3.5	01.03.2024	Steffen Auerswald	Review and Update 7.3
V3.6	05/03/2024	Pieter-Jan Gunst	Added 7.4, Neo4J
V3.7	05/03/2024	Sven Vansteenkiste	Updates 6.3 and 8 - devops
V3.8	25/03/2024	Eric Raepers	Complete the Cloud Section 15.x
V3.9	21/04/2024	Eric Raepers	Version adapted based on comments.
V3.10	25/7/2024	Bert Van de Merckt	Major review on multiple sections (2-3-4-5)
V3.11	12/11/2024	Pieter-Jan Gunst	Addition of Section 7.5
V3.12	16/12/2024	Wim Michiels	Review Sections 2.3, 2.4, 4.2, 4.3, 4.4, 10.3, 12, 13, 16

V3.13	17/12/2024	Wim Vercammen	Accept all previous changes to make the document readable again
V3.14	20/01/2025	Jonathan Vingerhoets	Correct some mistypes + review fileshare section
V3.15	26/02/2025	Wim Michiels	Update section 8 about the installation of external software on servers
V3.16	12/03/2025	Steffen Auerswald	Review and Update 7.3
V4.01	24/03/2025	Wim Vercammen	New major version that is published

Contents

1 Introduction

The goal of this document is to give an overview of the Elia Group IT standards on servers – operating systems - back office ("infrastructure") applications. New developments or new installed applications will be installed on these proposed platforms.

The audience of this document are all (internal+external) clients of the Elia Group IT Server Team (Steam). Detailed operational info for the team-members of Steam will not be documented in this document.

The reader of this document has to ensure he or she is using the latest version, which is always available in Sharepoint Online (link), and on the Server Team website http://steam.elink.elia.be, in Public/Steam Doc/Documents Sharepoint (like some other useful documents).

If an application (or development) cannot be installed because the pre-requisites of that application are not in line with the Elia IT standards, then the ITAM (IT Application Manager previously named ITAL) must contact the server team responsible *before* developing or buying the application. Not respecting these standards will lead to a NO GO for installation (acceptance and production) as the Elia IT Server Team will not be able to guarantee availability or support.

1.1 How to contact us?

All questions, problems and remarks should be communicated to our SPOC, preferably requested with a HEAT-Service Portal ticket.

The Server Team SPOC can be contacted via telephone (+32 2 249 5535 or 97/5535) or email (Server Team IT Transport <server.team@elia.be>), every Elia working day between 07:00 and 17:00. At any other time, Server Team only supports the critical applications (see §9.3 Critical Applications), through IT Duty (http://itduty.elia.be). A ticket can be created by the requestor or via the IT Helpdesk in the ServicePortal (https://serviceportal.elink.elia.be/HEAT), It's the preferred method to contact the Server Team. You can create a ticket for Steam via the "Service Catalog" and then select "IT Services" – "Datacenter Services". Then depending on the nature of the request a selection needs to be done. These are all Steam-requests. The most generic is the "Internal Steam request" – to be used when none of the others is applicable. For cloud requests, "General Services' – "Steam Generic Cloud Request" needs to be selected.

1.2 Steam Public Information

Server team provides some information about the server configurations. It's available in read-only for everybody on the Steam website (https://steam.elink.elia.be) in the Public section.

- Change Management (a simple log of all changes in Belgium only)
- Links to public documents in Sharepoint
- Server Info (CMDB of all servers with some configuration details)
- SQL Alias
- Server reboot times info

The Application(s) installed on the server. There can be one or more Applications on the server, in case of shared servers....

2 Server Standards

2.1 Standard server

The standard server is a *virtual* server. For TMD applications we use *shared virtual servers*, where more than one application can be hosted. Our virtual servers are running on VMWare vSphere 8.0 platform with DRS (Dynamic Resource Sharing), and HA between datacenters. The guests are stored on our NAS storage (see further).

Servers are equipped with 2 processors, one C: of 100GB and 8 GB of memory. Applications will be installed on D: (by default 10Gb). In Belgium, a dedicated disk, P:, is reserved for the page file. More resources are possible if needed (approval by Server Team management).

Shared Application servers are equipped with 2 CPU's and 8 GB memory.

Deviations from this standard –as discussed below- must be approved by Server Team management.

Dedicated physical servers need at least 3 weeks lead time. Dedicated virtual servers need at least 5 working days.

Request should be done via the "Server Group Request" workflow in the service catalog of the ServicePortal. Each server needs to be linked to an application – this to facilitate Configuration Management.

2.2 Hardware servers

If for one of the following reasons the use of a virtual server is technically impossible, a physical server can be provided:

- Application is very CPU or memory consuming.
- Application has many simultaneous client connections.
- Pure infrastructure servers (SQL, Oracle, MongoDB, vSphere hosts, …).
- Third-party applications not validated or supported on a virtual server.

Our standard physical server is a HPE ProLiant DL380 Gen11 with the following specifications:

- Dual Intel Xeon-Gold 6448H(2.4GHz_32-core_250W)
- 128 GB of RAM
- 2x25GbE SFP28 (default)
- Smart Array SR416
- C: 480GB partitions (RAID 1 SSD disks)
- More disks can be added depending the requirements of the application which will be installed on this server (max 8)
- If more (internal) disk space is really required, a specific non-standard server hardware is required where one or 2 drive cages can be added with room for 8 more disks each; the same types as listed above. It's connected to the same controller with a SAS expander. The delivery delay is really longOnly SSD disks are in use.
- If more disk space, or shared disk space between application nodes, is needed, a connection to our SAN (storage area network) is possible. We have NetApp AFF-A400 and FAS-8300 HA controllers (in clustermode), two pairs of high available controllers in each site (Schaarbeek and Merksem).
    - We connect a SAN client redundantly with two HBA cards to the Brocade SAN Fibre Channel network, and use NetApp Data ONTAP DSM Management software to provide fault tolerance/MPIO.
    - We connect a CIFS share via the redundant network connections
    - We connect a NFS share via the redundant dedicated network connections
    - We connect an iSCSI disk via the redundant dedicated network connections

2.3 Lifecycle

The lifecycle of dedicated servers is followed up with the Server Asset Management tool on the Server Team website – each of these servers will have an owner, who will be challenged regularly about his or her servers. As of April 2024 this is only available for Elia servers however.

A server migration should be planned when the OS or the hardware is out of support.

2.4 POC (Proof of Concept servers)

Servers to be used for POC's/tests can be requested (via a ServicePortal ticket/ Helpdesk) for a period of 3 months (can be extended till 6 months maximal). If a (standard) server is used for max 3(6) months no approval is needed.

The requester will have local administration permissions on these servers with an admin account. Server team will deliver a clean installed server and will (if needed and asked) take backups of this server. The test server will stay under the responsibility of the requester/tester. Server team will give NO support on these servers. No monitoring will be done on services, SQL jobs, scheduled tasks, SQL backups etc. The security patch deployment will be done as all development servers.

A POC server can never be used for Acceptance or Production. After the period of testing the server will be decommissioned.

2.5 Operating System

2.5.1 Standard OS

The standard server operating system used by Elia Group IT is Microsoft Windows Server 2022 Standard (64-bit) (Windows 2019 is still the actual by 50HzT). RedHat Enterprise 8 is used when it's required.

These operating systems are currently in use, and are considered *restricted* (validation by Server Team management):

- Windows server 2012 R2/2016/2019
- All Windows Server Enterprise editions
- RedHat Enterprise 6/7
- OpenVMS for Itanium – only used by the Realtime systems

All other OS's are currently not supported by the Elia IT Server Team. Installations of other OS's must be black-box; Server Team can only provide rack space, power and network connectivity. An approval of ITSecurity is needed to connect unsupported OS on the Elia Group networks.

Any type of administration activity on a server must be done with an administrative account.

2.5.2 Windows Server

All Windows servers are installed in English. By default, all are joined to an Active Directory domain, which enforce security settings by GPO.

Local administration permissions are granted by default on DEV/TEST machines, but on ACC/PROD we adhere to segregation of duties principle, when serverteam is managing the application. When other parties are managing the application, the role of serverteam is only to manage the hardware & operating system. (Refer to Support Level chapter below.)

2.5.3 Windows Server Patching

Elia is using Microsoft System Center Configuration Manager (SCCM) for the distribution of patches on Windows servers. These include Microsoft security patches, service packs, but custom distributions can also be deployed. 50Hertz and Elia use different systems to schedule & deploy.

We can inform customers of the patches that will be deployed, but only globally: explicit patches for explicit servers cannot be reported.

Customers can choose to avoid this automatic patching, but they will need to patch their servers manually; we make all required patches available and they can be manually installed at a better schedule. This option does not remove the need for patching.

Emergency patching (zero days, out-of-band) are still possible.

2.5.3.1 Belgium

The patches released on patch Tuesday will be deployed only the month after release. All servers are assigned to a week+day group. Each server needs at least two different days during its week. Patches are deployed between 02:00 and 04:00. Servers are rebooted by script after the patch window, and this can be chosen between 05:00-07:00.

2.5.3.2 50Hertz

The patches released on patch Tuesday will be deployed one day later to the 'low' group, and then 2 weeks later to both 'medium' groups. Servers have multiple days after this schedule to deploy new

patches. They are deployed between 02:00 and 04:00. Servers are rebooted when required during the patch window, and reboots are therefore random in that window.

2.5.3.3 Third party patching

SCCM only manages Microsoft released patches. We also offer automatic updates for a limited set of third party products. This is the current list. *(Note: this is only available in Business IT networks.)*

- 7-zip
- Adobe Flash player (chrome, firefox, internet explorer)
- CutePDF Writer 3.2.0.1 (2017)
- Filezilla Client
- Firefox
- LibreOffice
- Notepad++
- Putty 0.70
- treesize free
- winmerge
- winscp
- winzip
- WinRAR
- Google Chrome
- Adobe reader XI
- Adobe reader X
- Adobe Acrobat Reader DC
- Adobe Acrobat 10
- Adobe Acrobat 11
- Redhat OpenJDK (with known exclusions)
- Wireshark

2.5.4 Linux Server

All linux servers will be joined to the domain. The root password will not be communicated. Groups to allow SSH or SSH+SUDO will be provided. The owner(s) can ask proper permissions.

2.5.5 Patching Linux Server

RedHat Satellite is used to deploy and patch Linux servers. The maintenance windows are similar to Windows environment. For ITSI and ATI environment no central patch solution is in place. Patching needs to be aligned with app managers individually until Satellite in these zones become available.

2.5.6 Appliances

Some time, the supplier is providing a server where our access is limited. We consider these as blackbox.

Our definition:

- Steam has no root/admin access
    - Or Steam is not able to install mgmt software (Antivirus/VMtools/backup agent...)
- OS cannot be patched by our standard tools
- The server responsible (ITAM) has to pay attention to regular patching
- In Steam we describe the OS as "Linux Generic"
- Can be a virtual (provided by supplier as OVA)
    - Or can be a physical appliance

2.6 Network connectivity

2.6.1 Group-wide information

We recommend using DNS aliases (CNAME records) over server names to facilitate loadbalancing, DR situations and migrations.

2.6.1.1 Alias naming convention

Domain can either be 'belgrid.net' or 'corp.transmission-it.de':

ENV	SVC ALIAS
ACC	[APPL]ACC.[DOMAIN]
PROD	[APPL]PROD.[DOMAIN]
DEMO	[APPL]DEMO.[DOMAIN]

2.6.1.2 Load-balanced applications

The above naming convention is valid for non-loadbalanced applications. When we use the Big-IP F5 loadbalancer, the SVC and WEB alias keeps the standard name, and point to the loadbalancer. However, the aliases [APPL]_[ENV]-1, [APPL]_[ENV]-2, etc... are added to point directly to the different members of the loadbalanced farm.

2.6.2 Elia

All servers are installed in our different datacenters. These server rooms and sites are connected via high speed fiber and Ethernet connections.

- Schaarbeek (J-Green and Q-Red)
- Merksem (Red and Green)
- Emperor, the usage is limited to backup infrastructure servers.

Servers will be placed in a dedicated "server VLAN" per environment (DEV/ACC/PROD). There are several network segments: intranet – DMZ ETSO – DMZ Backend – DMZ Frontend – DMZ EMS. These are separated by firewalls, managed by IPNOC.

Each communication between different network segments must be challenged by IT Security (ServicePortal firewall ticket).

All server rooms have 1 and 25 Gbps switches. Each server has redundant network connectivity to separate switches with automatic failover (using Windows teaming or Linux bond). By default, servers are connected with a LACP of 2x 25gb fiber. The embedded management console (ILO) is connected in UTP.

For Windows: NETBIOS over TCP/IP is disabled by GPO. WINS is not used. SMBv1 is not allowed. The DNS suffix search list of all servers is set by GPO.

The Infoblox solution serves as DNS, DHCP and IPAM (IP Address Management).

For more information about the Elia IT network, we refer to the IT Exploitation Datacom team (IPNOC).

2.6.2.1 Internet access on Elia servers

By default our servers don't have internet access. If internet access is needed, an approval from IT security is needed (using a ServicePortal ticket / "Application internet access" template). An (automatic) process has been put in place to regularly review the list of servers having internet access. Application (or server) owners with internet access have to revalidate each 6 months this exception.

All network communication across firewalls; including access to internet; is checked and filtered by the Palo Alto device. All requests are logged. To access internet the request must be authenticated and "no proxy" must be configured.

2.6.3 50Hertz

All servers are installed in our different datacenters. These server rooms and sites are connected via high speed fiber and Ethernet connections.

- NQT
- Neuenhagen

Servers will be placed in a dedicated "server VLAN". There are several network segments: BusinessIT – DMZ ITSI. These are separated by firewalls, managed by Datacom.

Each communication between different network segments must be challenged by IT Security (ServicePortal firewall ticket).

All server rooms have 1 and 10 Gbps switches. Each server has redundant network connectivity to separate switches with automatic failover (using Windows teaming or Linux bond). By default, servers are connected with a LACP of 2x 25gb fiber. The embedded management console (ILO) is connect in UTP.

For Windows: NETBIOS over TCP/IP is disabled by GPO. WINS is not used. SMBv1 is not allowed. The DNS suffix search list of all servers is set by GPO.

The Infoblox solution serves as DNS, DHCP and IPAM (IP Address Management).

2.6.3.1 Internet access on 50Hertz servers

All servers can access internet, but access is allowed for specific users.

Any request should be done via the ServicePortal ('gateway connection' request).

2.7 Disaster Recovery

2.8 Support Level

2.8.1 General

All what is written here is managed by Steam. Manages = Patched, evolution, incident mgmt, Daytoday Mngt.

If not part of this standard, then the ITAM is responsible for the support of his application.

2.8.2 Support levels

Each server has a support level, chosen from the list below, as agreed at the time of server request. Any changes to this have to be approved by the Server Team Responsible.

In each level, backup can be foreseen for PROD, pending compatibility and approval.

None	Server Team provides rack space, power, network connection.
Hardware	Above + hardware monitoring and replacement of broken components. Hardware needs to be in our standards. Could be used also for steam non supported Appliances (as we are not able to install any external application)
Hardware+OS	Above + OS monitoring (through SCOM for Windows or PRTG for Linux, only for PROD) + patching + backup + antivirus + AD membership (GPO). OS needs to be in our standards.
Hardware+OS+Limited	Above, without monitoring, including installation and limited support of infrastructural components (IIS, SQL…). This category is available for certain (agreed) development servers.
Hardware+OS+Software	As 'Hardware+OS', + application deployment (see later in this document). All software has to follow our standards, and installation guidelines (7.51) have to be provided.

3 Active Directory

Elia Group is using Microsoft Active Directory for computer and user authentication. We have separate domains in each network segment, some have trusts. We have sensitive zones that need to adhere to enhanced IT Security Guidelines (ISMS). These zones are out of scope of this document.

We run Active Directory forest & domain functional level 2012r2 on Windows 2016+ servers.

Elia Group IT deploys GPO's based on CIS guidelines for users, clients and servers. Local security policies are not allowed on domain member servers.

Domain administration is restricted to the Server Team Win Core pool, delegations are made to EUD for computer & user management, and Citrix team. Domain admins are always distinct and dedicated administrative accounts.

3.1 Elia domains

- BELGRID (belgrid.net) in Intranet
- ISOEXT (isoext.dmz) in DMZ Backend
- ELIA_ETSO (elia.etso) in DMZ ETSO (private network between TSO's)
- BELGRIDEMS (belgridems.net) in DMZ EMS – secure zone

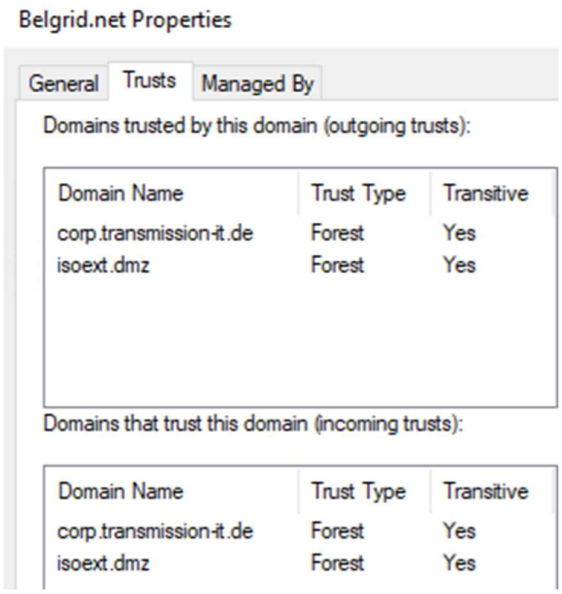
The Intranet Active Directory BELGRID is divided into two Active Directory Sites: Schaarbeek and Merksem. All IP ranges from the south part of the country are in the Schaarbeek site, all ranges from the north part in the Merksem site. Each application that calls Active Directory one way or the other needs to be AD Site aware: it needs to find out which domain controller is in its site; Microsoft provides the correct API's to discover this (via "RootDSE").

Specific rules concerning using LDAP in our environment are described in the BELGRID LDAP connections.docx document.

All servers in the BELGRID domain have the registry key for Kerberos - Maximum Token Size updated to 65535 because of the large token size within our environment.

NTLM/LM requests are disabled for all Windows Server 2016+ machines.

This tab shows the trusts with the BELGRID domain:



3.2 50Hertz domains

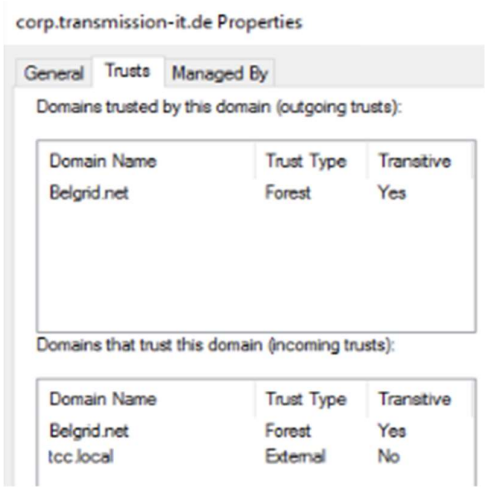
- TMIT (corp.transmission-it.de) in Intranet
- SYSOP (sysop.local) in Alte Technical-IT – sensitive zone

- NMC (nmc.local) – sensitive zone
- TCC (tcc.local)
- LEITACC (leitacc.local), LEITSUPP (leitsupp.local), LEITADM (leitadm.local), LEITPROD (leitprod.local) and LEITREF (leitref.local) – sensitive zone ITSI

The Intranet Active Directory TMIT has only one Active Directory Site.

All servers in the TMIT domain have the registry key for Kerberos - Maximum Token Size updated to 48000.

This tab shows the trusts with the TMIT domain:



3.3 Cross-domain

We have a cross-company AD domain trust between TMIT and BELGRID, permitting to grant access to resources to users of the other domain. The only exception to this is Remote Desktop access, where we do not allow cross-domain logons (GPO conflicts). Some other technologies may also disallow cross-domain administrative access.

4 Remote Access

4.1 General rule

Administrative access to servers can be given via OS specific standards (Remote Desktop Access or SSH). This access is always with a personal admin account, which may not be shared and must always be linked to an enabled regular account. (The latter must be requested through the OneSAP Check-In process.)

As noted in §3.3, this type of administrative access is not allowed cross-domain TMIT<>BELGRID.

No administrative access should be granted from user vlan connections. All users requiring administrative access need to jump through a 'jump host'. *(Note: this is not yet the case in 50Hz Intranet in June 2024.)*

Windows servers have no more than 2 simultaneous RDP connections available. It is assumed that users will manage these connections (log off instead of disconnect) adequately. Disconnected sessions may at all times be logged off to free up resources.

Service accounts are not permitted to RDP to servers.

Access from outside of Elia to servers is only allowed through secured VPN tunnel (with OTP authentication), or through B2B VPN. Only DMZ applications can be accessed from outside of Elia via the F5.

Access from outside to 50Hz servers is additionally possible through the Citrix farm.

Elia has specifically implemented a DMZ jumpserver to allow users on the internet to connect to a VPN portal with their eToken (after installation of Anyconnect VPN client), and access their PC or very specific servers from outside.

4.2 Access rights for 'Hardware+OS+Software '

The developer**/tester will have local administration permissions on these servers with an admin account. Server team will deliver a clean installed server and will (if needed and asked) take backups of this server. The development server will stay under the responsibility of the developer. Server team will give NO support on these servers. No monitoring will be done on services, SQL jobs, scheduled tasks, SQL backups etc.**

Only Server Team will have local administration permissions on ACC and PROD servers.

The goal of ACC servers is to verify the installation, configuration and correct operation of a new installed or upgraded application and the compatibility (no conflicts) with other applications; and as such resemble as much as possible the production servers.

4.3 Access rights on other support levels

Local administration permissions will be granted to the supporting team of the application.

5 Host based protection

- Elia IT is using a centrally managed, host-based protection software suite (Trendmicro Deep Security). This contains:
  - Firewall
  - Intrusion Protection System
  - Integrity Monitoring System
  - Anti-Malware protection

  (Note: the full rollout of this software suite is to be completed in 50Hz Businss IT.)
- The intrusion prevention will protect against possible abuse from not yet patched vulnerabilities and improper use of certain applications or protocols in blocking mode.
- The anti-malware protection performs by default a realtime scan of all files.
- The integrity monitoring will show reports of changed system content on the server.
- The firewall will be configured to allow all outgoing communication, but block all incoming communication, except those specified.
- Please be aware that, by default, RDP, SSH, management traffic and file shares will not be reachable for ACC & PRD servers, from any network (only via Jumpservers).
- Because of this measure, you will need to inform server team of the type of server you want. If it's a non-standard application, you will need to communicate the necessary ports to our SPOC so they can be configured (Via ticket).
- In case of issues, please contact server team so we can verify which ports are being blocked on the server.
-

5.1 Antivirus

Elia is using several layers of antivirus; on servers we use TrendMicro Deep Security, for NetApp we use TrendMicro ServerProtect, for Exchange we use TrendMicro ScanMail and Sophos for Marshal on the Mail Relays.

Policies are used to configure exclusions, and are managed centrally on the Deep Security consoles. These consoles ensure up-to-date protection on all our servers.

6 Back-office (infrastructure) applications

6.1 Mail infrastructure

Elia IT provides on-prem Microsoft Exchange 2016 as standard mail infrastructure in the intranet environments.

We provide SPF antispam protection on all our mail domains.

Primary internal email domains are "elia.be", "elia-engineering.com", "eurogrid-int.net", "windgrid.com" and "greenbid.be". External users have an "externel.be" addresses in addition to the "elia.be" address. We have a shared namespace "eliagroup.eu" which is hosted in the Exchange environments at Elia and 50Hertz.

Mailboxes are kept for 3 months maximum after users have left Elia.

6.1.1 Connections with or to the mail environment

- Applications that need to send email have to use the following alias as SMTP server: internalmailrelay.elia.be
- The SMTP protocol (port 25) is the only allowed protocol for mail. Relaying is not allowed per default. A request to the server team has to be made if relaying is needed.
- SPF record enabled for our hosted domain.
- POP3 and IMAP are disabled by default.
- For applications using the .NET framework, the following APIs are supported:

API	Support Policy
Exchange 2016 Web Services	Supported (recommended)
Microsoft Exchange MAPI and CDO 1.2.1	Supported but not recommended
Exchange WebDAV extensions	NOT SUPPORTED

Please note that application needing only to send emails without the burden to connect to the infrastructure, may use the Elia MailSender application. See TMD team for more information.

6.1.2 Microsoft Identity Manager 2016

The contacts of our colleagues from 50Hertz are imported into our Active Directory using the Microsoft FIM (Forefront Identity Manager) product (the GALSync module). This creates so-called *cross-forest* contacts, to permit us to share calendars and functional mailboxes.

6.2 SMS infrastructure

Elia provides easy sending of SMS using Fenestrae Faxination Server 2013 ("*faxination*").

Applications can send SMS messages by sending an email to "324XXXXXXX@sms.elia.be" where 324XXXXXXX is the target cell phone number.

The maximum rate of outgoing SMS that can be handled is 20 SMS/sec; each application sending SMS messages must be throttled to send less than this. We are using the Proximus RingRing platform to deliver SMS.

6.3 IIS (Internet Information Server)

6.3.1 Standards

- Our current standard is Windows 2019 with IIS 10.
- Internal FTP is still provided on the IIS 10 server.

- External SFTP is provided on Globalscape EFT Server version 8 (authentication via ISOEXT accounts).

.Net framework v4.8 is installed (Windows 2019). New approved .net Core versions is automatically deployed through SCCM. Any other version must be requested for a manual installation

- Read access is possible to the share where the website is installed.
- Read access to the IIS configuration can be given to the developer via the IIS 10 console to verify the website and settings.
- Https is used inside Elia. A wildcard certificate is set on the machine and applied on the default website. If necessary, we can provide a specific certificate. Certificates management is in the hands of Win Apps team.
- Manual installation of a web application is done by copying the sources from a repository (\\Isofile01\it\11 Apps) to the destination server. Our standard IIS config is applied by default to avoid extra costs in management. Any difference will be challenged and applied if necessary.
- Automated installation (DevOps) is possible, and it has its own standards – servers should always be requested through the Steam Application pool to ensure the correct packages are deployed, environment variables are set and the devops agent is configured on the server.
- Our standard IIS configuration includes:
- - Windows integrated security needs to be used by default.
- - Anonymous is used by default on website requesting ADFS.
- - Default application pool and website are stopped – they are not used.
- - For each developed application, a new website and a new application pool must be created. The settings of both of them must be described in the installation guide of the application (even if it's a standard configuration)
- - Port 80 is reserved for the Default web site – this website is stopped on all webservers. It cannot be used for another site. Host header names have to be used to direct clients to the correct website for Intranet servers.
- - As already mentioned, port 443 is used by default for any application deployed on a webserver.
-
- We are using the Big-IP F5 hardware load balancer device in the Intranet.
- All websites in the DMZ Backend zone have to be configured in our F5 (reverseproxy).
- All published websites need to be in https and so a certificate is purchased (DigiCert) for each of them.
- All IIS installations need to have the HTTP parameters for maximum token size adjusted because of the large token size in our environment.

6.3.2 Web Alias naming convention

ENV	WEB ALIAS
ACC	[APPL]ACC.elink.elia.be
PROD	[APPL].elink.elia.be
DEMO	[APPL]DEMO.elink.elia.be

6.4 Open JDK

- By default Java is not installed on our servers
- If Java is needed: Redhat OJDK 11 is our standard

6.5 RemoteApp +Citrix

It is possible to publish "Remote Apps" for certain applications. This is a non-standard request and has to be approved by Server Team management

This technology is based on Windows Remote Desktop Protocol, and gives end users an icon that actually launches an application on a server, instead of locally. Behind the scenes, an RDP is set up.

This could be handy to provide applications to external users (as it was done for Outsourcing partners of Engineering with the EPRM applications) – a B2B VPN allowing RDP, and correctly configured external accounts in AD, would have to be in place.

6.6 inter-applications messaging systems

We currently use 2 different systems for applications to exchange messages.

rabbitMQ: there are 2 different clusters (on each Elia site – rmqschprod & rmqmksprod) accessible through aliases and AMQP ports (5672 & 5671 for AMQPS) to hardcode in the config file of the application. The authentication is done by means of client certificates. This certificate is defined as user in RabbitMQ and must be installed on the application server.

6.7 Scheduled Tasks

We use the VisualCron 10.x software to run and manage centrally scheduled tasks on our complete environment. There is a different instance of VisualCron per domain. Local scheduled tasks are to be avoided and not allowed by default.

Server Team SPOC is alerted by email in case of failed scheduled tasks (when the ERRORLEVEL is not 0).

VisualCron is used to manage all scheduled tasks. The following task types are supported:

- Batch files
- PowerShell
- SQL
- ...

7 Database platforms

7.1 SQL Server

7.1.1 General

The server team is in charge of the administration and maintenance of all acceptance and production database servers, and the creation, deletion, updates, backups and restores of databases.

Each database update needs to be provided as an SQL script that will be executed in the DBO context by the server team, first in acceptance and - after application responsible confirmation - in production. Server team is NOT responsible for the content of the db.

Server Team will always aim to keep the amount of operational SQL versions as small as possible; so will contact application owners regularly to migrate their databases to a new platform.

7.1.2 Connections to a database

Connections to a database must always be done via a DNS alias. Physical server names or IP addresses MAY NOT BE used. Cross environment (dev <> test <> acceptance <> production) access is not allowed.

A copy-of-production environment is available on-demand for cross-platform access or other requirements: these databases are overwritten on a regular schedule. No troubleshooting is done on these databases; if a problem occurs, server team will run the restore-from-prod job again and overwrite the copy-prod database.

The authentication mode is Windows authentication (Active Directory service accounts). Active Directory security groups are used to manage access (see below). Access from the DMZ to databases should also be via Windows Authentication (Kerberos via SSPI). The use of SQL authentication is restricted.

If a permission is requested outside of the default (datareader, datawriter, db_executor), this is given on a temporary basis to admin accounts only. Only the non-default permission to read the definition of a database (defviewer) is given permanently; but only to admin accounts.

7.1.3 Microsoft SQL Server

Microsoft SQL Server 2019 64-bit Standard Edition;

- Collation "SQL_Latin1_General_CP1_CI_AS"
- Reporting Services: SSRS 2019 (dedicated servers)
- Analysis Services: SSAS 2019 (dedicated servers)
- Components installed:
    - Instance feature
        - Database Engine Services
        - SQL Server Replication
        - Full-Text and Semantic Extractions for Search
    - Shared features
        - Client Tools Connectivity
        - Integration Services
        - Client Tools Backwards Compatibility
        - Client Tools SDK
        - Documentation Components
        - SQL Client Connectivity SDK

Restricted versions:

- Microsoft SQL Server 2019 64-bit Enterprise Edition;
- Microsoft SQL Server 2014/2016 64-bit Standard Edition.

The following rules apply:

- Database log shipping is allowed, mirroring is recommended for DRP purposes (replaced by Always on as from SQL 2016 and SQL 2019), if requested.
- Linked servers are not standard.
- Access is granted on database level, using the built-in database roles datareader – datawriter – db_executor. This access is given via an Active Directory security group DB_[dbname]_[environment]_R/U.
- No access is granted to the system databases.
- No access is granted to Data Collector views.
- No DBO access is granted.
- Profile or execute permissions can be granted on simple request, for a restricted time; but only to admin accounts.
- SSIS package can be used, a proxy account will be configured. External resources can be accessed.
- SSIS Admin role is allowed on SSISDB.
- SQL agent account is NOT local server admin.

- SQL job owner is the svc account of the attached application. Each SQL job step will run as a proxy account (normal the same like the job owner).
- SQL mail and database mail may NOT be used.
- Data paths to be used:
    - Data path: K:\MSSQL\Data\<databaseName>
    - Log path: L:\MSSQL\TL\<databaseName>
    - Backup path: N:\MSSQL\Backup\<databaseName> (or CIFS, see below)
- The N: disk of most SQL servers will be a LUN on the SAN storage boxes, comprised of SATA disks. This helps the server team to provide site DRP, as these disks will be located on the storage box in the other site.
- Alternatively, a CIFS share to backup SQL exists in both sites, so SQL backups can always be taken cross-site (e.g. for SQL on VM). A CIFS share is also used for the backups of the AlwaysOn databases (HA).
- On newer servers, we are starting to add M and N drives to separate the tempdb from the K and L drive, in that case the N drive will be used to contain the transaction log of the tempdb
- The following SQL tasks are done automatically on all SQL servers:
    - Rebuild indexes: once per week on Sunday at 10:00 (reorg or rebuild decided dynamically on fragmentation levels)
    - Update statistics: daily at 22:00
    - Database check integrity : once per week on Sunday at 20:00
- SSRS: Server Team deploy the reports based on the application's documentation. By default, the browser permission is granted.
    - ITAL's (BII's) or BAL's (BBI's) can request to be Subscription Managers of certain reports, also on ACC and PROD. Given this, Server Team cannot assure availability of those subscriptions.
- The database recovery model is FULL (only for production databases).

7.1.4 SQL 2016/2019 HA (High Availability)

- SQL HA is configured in SQL2016/2019 standard edition and is dedicated to the top critical applications.
- The failover cluster feature is installed on all nodes involved in the HA (2 nodes max).
- Two Setups possible:
    - a. Both nodes are installed in Schaerbeek in two different datacenters (physically separated). A third server in Merksem will act as standby (log shipping each 15 min).
    - b. One node in each datacenter, if the application and DB-Workload supports it
- Each HA database will be hosted in one availability group.
- The replication between the 'Schaarbeek' nodes is done synchronously.
- A virtual IP and name called listener must be defined for each database. The virtual name must be used in the application connection string.

7.1.5 Backup of a SQL database

All backups are taken by SQL Jobs.

- **Production**
    - Daily Full backup at 18:14 - this backup stays 2 days on disk (Timing can differ in some case) for direct restore. These backups are stored on filers and (file) snapshots are taken .

- For databases smaller than 500Gb classic SQL backups are in place, for bigger databases we will start using (Netapp Snapshots) (2023 and later) this impacts the configuration of the server, so disk lay-out can change in this case
- A backup of the transaction log is taken each 15 minutes

- **Acceptance**
  - No backups are taken of these environments
- **Development**
  - The standard maintenance plans and SQL jobs on development servers are created by the server team during installation. Server team is not maintaining these plans and jobs, and no monitoring is done on them.
  - Daily Full backup at 17:00 - this backup stays 2 days on disk
  - Backups are stored on filers and (file) snapshots are taken .
  - For databases smaller than 500Gb classic SQL backups are in place, for bigger databases we will start using (Netapp Snapshots) (2023 and later)
  - A backup of the transaction log is taken each 15 minutes
  - Backups are compressed with the standard SQL compression.

7.1.6 Backup Retention periods

- Development:
  - To disk: full daily at 17:00 + transaction log each 15 minutes. This is configured during server build (SQL install), but afterwards it must be managed by developer (client responsible).
  - To tape: On Tuesday – Thursday – Saturday
- Acceptance:
  - No backups are taken
- Production:
  - To disk: full daily at 18:14 + transaction log each 15 minutes

7.1.7 Naming convention of SQL databases

This convention is important to avoid confusion between environment.

Database names:

- Acceptance: **ApplicationName_ACC**
- Production: **ApplicationName_PROD**

DNS aliases:

- Acceptance: **db*[ApplicationName]*Acc**
- Production: **db*[ApplicationName]*ProdP**

(final "p" indicates Primary when mirroring is used, "m" for the mirrored)

7.1.8 Naming convention for SQL HA

Cluster name:

- Elia Acceptance: **HACLxx**
- Elia Production: **HACLxx**
- **50hzt: SCSQLBPXxxx**

Availability group:

Acceptance:**AG_*[ApplicationName]*_ACC**Production:
AG_*[ApplicationName]*_PRODAvailability group listener:

- Acceptance: **ag*[ApplicationName]*acc**
- Production: **ag*[ApplicationName]*prod**

7.1.9 Naming convention of SQL jobs

Prefixes:

"sys…": System jobs created by SQL server itself

"_...": Jobs created by Server Team for all standard DBA tasks

"[DatabaseName]_[Description]": User application Jobs

Suffixes: (optional)

" nomonitoring": SCOM does not report on the result of this job.

" longrunning": SCOM ignores the duration of this job.

" nonstopping":SCOM ignores the job when continue running.

7.1.10 SQL Server Reporting Services

Standard: Dedicated Microsoft SQL Server 2014 64-bit Standard Edition or Microsoft SQL Server 2016 64-bit Standard Edition.

7.1.10.1 The security configuration on the "Home" folder

Only the hereunder mentioned accounts will receive rights at the top level folder :

- BUILTIN\Administrators Browser, Content Manager, My Reports, Publisher, Report Builder
- Domain users Browser

By implementing this configuration, we ensure the accessibility to the administrators for management purposes and to the domain users for the entire report server.

7.1.10.2 Project folder management

The goal is to configure one folder for each project.

The security is managed as followed:

- The responsible of the project receives the "Content Manager" role. By doing this, he/she is able to manage everything INSIDE his/her folder.
- If the project folder is not under the root folder, the security will be placed on the project folder only, not on the parent folder.

7.1.10.3 Responsibilities

The responsible of the project is responsible for the security and the content in his/her folder.

We advise to use MT_... groups to assign permissions on the reports.

If a new group is needed, an owner is required!

The option "Revert to parent security" will be used by server team in case of problem with the security on a folder.

Steam remains responsible for the operating system and ready to help users in deploying their reports.

7.1.11SQL Analysis services

Analysis services is installed on shared servers but dedicated for SSAS. The name of the server starts with ISOBI...

The memory must be configured as follow:

Memory \ HardMemoryLimit	50
Memory \ LowMemoryLimit	20
Memory \ TotalMemoryLimit	30

Except for server team, Administrator rights will not be granted on the server. Permissions are managed through the predefined roles "read all" (permission read definition) and "process all" (permission process database).

Data directory : K:\MSAS12.MSSQLSERVER\OLAP\Data

Log Directory : L:\MSAS12.MSSQLSERVER\OLAP\Log

Backup directory : N:\MSAS12.MSSQLSERVER\OLAP\Backup

SQL Jobs monitoring

The PROD SQL jobs are monitored by SCOM. An alert is generated in case of job failure.

Exceptions on monitoring:

- Inactive jobs
- Not scheduled jobs
- The Job name contains [nomonitoring]
- Long running SQL jobs are not alerted on when name contains [longrunning]
- Non stopping SQL jobs are not alerted on when name contains [nonstopping]

7.2 Mongo DB

7.2.1 General

The server team is in charge of the administration and maintenance of all acceptance and production Mongodb servers, and the creation, deletion, updates, backups and restores of databases/replicasets/security.

The Database(s) within a replicaset will need to be created by serverteam, to also set the security restricted to the database. ReadWriteAnydatabase is not allowed. Only read@DBname, or readWrite@DBname is allowed. Exceptions are possible but only if there is a more detailed or restrictive security model in place for the application.

All changes or new implementations need to be done first in acceptance and - after application responsible confirmation - in production. Server team is NOT responsible for the content of the db.

Server Team will always aim to keep the amount of operational MongoDB versions as small as possible; so will contact application owners regularly to migrate their databases to a newer version.

7.2.2 Connections to a database

Connection strings will be provided by serverteam. Cross environment (dev <> test <> acceptance <> production) access is not allowed.

The authentication mode is Windows authentication (Active Directory service accounts). Active Directory security groups are used to manage access (see below). Access from the DMZ to databases should also be via Windows Authentication (Kerberos via SSPI). The use of mongodb database users is restricted.

If a permission is requested outside of the default (read@dbname, readWrite@dbname), the request will be analyzed by the MongoDB DBA's, clear and complete information and argumentation is necessary.

7.2.3 Versions

We will try to follow the n-1 version of mongodb (multiple versions are possible, however in 1 environment for 1 replicaset only 1 version is possible). We will deploy it automatically replicaset per replicaset using the opsmanager, starting in ACC and after confirmation/testing in prod.

Dev is requested to test the new releases in their own dev environment.

7.2.4 Replicasets (High Availability)

- MongoDB Replicasets provide a HA setup for MongoDB
- HA is dedicated to the top critical applications.
- The new HA environment will consist of 4 data bearing nodes (2 in SBK, 2 in MKS) and 1 arbiter (Empereur as witness) ➔

7.2.5 Replicasets (Standalone)

For non-critical applications, we are providing a standalone server, with 1 datanode.

Meaning that for version-upgrades, or some deployments that demand a process restart, the databases/replicaset will be shortly unavailable.

7.2.6 Backups

Managed by opsmanager tool.

PIT restore possible up to 15 days in prod. (Backups in acc only available if configured and for testing purposes)

7.2.7 Backup Retention periods

- Development:
  - To disk:
  - To tape: On Tuesday – Thursday – Saturday
- Acceptance:
  - No backups are taken
- Production:
  - To disk: 1 full snapshot on daily basis, timing is managed by opsmanager. The transactions are stored automatically in the oplog database. And the restore operation will determine which snapshot need to be restored and what transactions need to be played back onto the database for a PIT restore

7.2.8 Naming Convention

For the replicasets, the naming convention is like:

RS_NAME_ENV

Or

RS_SA_NAME_ENV

RS= replicaset

SA= standalone (no HA)

NAME= application name (BMAP, ENIGMA, OPTIFLEX)

ENV= environment (ACC, PROD)

Ex: RS_SOROBAN_PROD, RS_SA_IDS_PROD

7.3 Oracle

7.3.1 General

Within Elia BE SQL Server is the standard, within 50Hz both SQL and Oracle are standard, but new Oracle databases are only allowed, if MS SQL is not possible.

50Hertz Oracle environments are similar and follow the defined standard.
Actual supported version: 19c (Migration to new version 23c planned after 2027, not published yet).
The databases should be migrated to (23ai) required Layout with CDB and PDB (new databases are mandatory installed as CDB/PDB.

Elia BE
Oracle database servers are hosted on Windows.

Migration to supported version 19c is planned by Elia BE DBA.

50Hz DE
Oracle database servers are hosted on on Oracle Enterprise Linux (OEL). All Database servers will be replaced from OVM to VMware with RHEL8
Tnsnames.ora: located on Netlogon share

Admin rights:

The sysdba admin rights are only reserved for Elia Group Oracle DBA internal usage and 50Hertz DBA internal usage.

7.3.2 Oracle Database Backup

The standard tool for Oracle database backup is RMAN (Recovery Manager). This tool is used to do an online backup of the database and archive logs to disk and allows to do a point in time recovery of the database.

Elia BE

Backup
Timing : 1 full/day
A second tool used for backup is the Datapump utility (new version of export utility) which allows a full dump of the database to file. These export files can be used to recover individual database objects.

50Hz DE

Backup RMAN
Timing : 1 full/week
Every 6h archive/daily
A second method to support backups is the usage of NetApp snapshot functionality. 3 times a day a snapshot of the database is taken. This snapshots can be used to recover the whole database or individual database objects.

Third is Oracle Datapumpo Utility, also usable tp backup whole databases and different Schema

Redundancy
Only for critical (actually 35 databases)
Standby with manual switchover and automated failover in case of primary database problems (passive Dataguard feature)
Implementation from Oracle Data Guard with Primary and Standby (not active Standby) DB is planned for all databases in all Zones, For Prod Databases the FSFO with HA Observer (Master and Backup) will be implemented

7.3.3 Backup Retention periods

All environments:

- 14 days (defined by management)

7.4 Neo4J

7.4.1 General

The STEAM Applications team provides Neo4j Graph Database as a platform service.

Delivering the Neo4J Graph Database as a platform enables the organization to develop, run, and manage business applications requiring transactional and analytical workloads. The STEAM applications team installs and maintains the Neo4J Graph Database infrastructure and middleware.

Lifecycle environments:

- Development
- Acceptance
- Production

7.4.2 Connections to a database

In the platform service operating model, the STEAM applications team does not actively manage the connections, databases, users or the underlying data. Instead, the application teams have users with the roles "admin" and "PUBLIC" assigned. These roles provide virtually all privileges in Neo4Js RBAC model. The latter provides the required authorizations, assigning privileges to users depending on the assigned role. Authentication depends on neo4js internal user management. LDAP / Active directory integration is not configured.
Neo4J has both bolt and http interfaces available. Encrypted versions of these protocols are unavailable as TLS has not (yet) been configured in Neo4J.

7.4.3 Versions

All lifecycle environments have neo4j-enterprise 4.3.6 installed. Its functionality has been extended with the following plugins:

- Apoc 4.3.0.3 Core
- Bloom 1.8.0

- Graph-data-science 1.6.1

7.4.4 High Availability

There is no high availability configured in our Neo4J deployment.

Our deployment consists of one standalone server per lifecycle environment.

7.4.5 Sharding

It has been requested to study the feasibility of a Fabric (sharding) deployment. The feature is currently in test in private labo. It would allow for easier management and scale-out of the current deployment. There is no request for deployment currently.

7.4.6 Backups

Daily backups are scheduled and executed from VisualCron, section 10: Backup, since 23/12/2023. These serve multiple purposes:

- to be able to upgrade our neo4j instance
- to be able to quickly recover data in case of failure
- to be able to perform routine administrative operations like database compaction
- to share data exports

7.4.7 Service assurance

- Level 1: STEAM Applications

  Monitoring is performed in PRTG.

  Alerting is performed in the form of email notifications to STEAM Applications, which are serviced during local business hours. Alerting is performed on two main categories:

  - Reactive: service assurance

    Verifies that the platform is available

  - Proactive: incident avoidance

    Verifies capacity indicators and metrics

- Level 2: Vendor support

  Our deployment is covered by a "standard" support license

  Technical support hours: local business hours only (Monday-Friday, 8:00-18:00)

7.4.8 Service operations

Neo4J servers follow standard security patching and can be rebooted at the configured

7.5 Redis Enterprise

7.5.1 General

The STEAM Applications team provides Redis Enterprise, a cache database, as a platform service.

Delivering the Redis cache database as a platform enables the organization to develop, run, and manage business applications requiring caching at scale. Its enterprise-grade functionality ensures that critical applications run reliably and super-fast, while providing integrations to simplify caching and save time and money.

7.5.2 Lifecycle environments

- Development
- Acceptance
- Demo
- Production

7.5.3 Connections to a database

The connection string to the database is provided by STEAM applications. The connection string represents the target cluster and authentication on the application database.

7.5.4 Versions

The TMD clusters run Redis Enterprise 7.2. The other clusters, including caching databases for Biple and Integration hub, run version 6.4

Upgrades will be planned and communicated to align with the vendors product lifecycle. A detailed rollout plan, following the different lifecycle environments will be presented in advance.

Security patches will be applied following STEAMs standard patching cycles, or as needed depending on criticality and as per vendor recommendation. For more detailed information on the planning and deployment of patches, please refer to the chapter Service Window in this document.

It is the responsibility of the application owner to ensure the client remains compatible with the current server version.

7.5.5 High availability and clustering

Geo-distributed replication over local multi-node clustering is available in all acceptance and production environments for critical applications.

For standard applications, acceptance and production environments provide local high-availability and clustering.

Other lifecycle environments may provide resilience at the infrastructure level only.

7.5.6 Backups

There are no point-in-time recovery backups of the data in the Redis cache database.

Rationale: a cache holds non-persisting data with a defined and limited lifespan. Backups represent the data layer at a particular point in time. A restore of expired data may yield unpredictable results for technical and market-platform applications. The infrastructure recovery procedures have all been designed to meet service availability objectives, explicitly omitting any application data in the process.

8 Application Deployment

The "Web & SQL" or "Application" Pool of the Server Team is responsible to deploy (install and update) in-house developed (by TMD) applications on Acceptance and Production environments.

Server team will NOT install or deploy any external software on our servers. This needs to be done by the IT application manager/server owner.

Maintaining this external software (patching / evolution , licenses ..) is under the responsibility of the IT application mgr/Server owner

8.1 Procedures

All demands to deploy (part of) an application must be logged in to the ServicePortal (Ivanti - HEAT) ticketing system, using the special ITAL/TMD Architect role. The Itam/Architect can use the "ITAM / TMD Application Update Request" for regular updates and use a separate Service Offering for releases through Devops : "Generic Steam DevOps Request". If the deployment will take more than 15 minutes, it is advisable to plan this in advance.

Normal deployments will only occur during business hours (08:00-17:00). Deployments will be executed on a first-come, first-served basis. Exceptions to this can only be agreed with the Server Team Responsible. No deployments in Production will be done the day before the weekend or holidays, except urgent bug fixes (with the agreement of the Server Team Responsible).

On the days following these, changes are allowed after verification that the publication process was successful.

8.1.1 TMD deployment procedure

All requests to update a component created by TMD (using TFS) must be done following this procedure.

- Each update will be a different build number;
- This build will be saved by TFS inside the "\\isofile01\it\11 Apps" folder, with the buildnumber in the foldername;
- ITAL or architect demands the update to be done to STEAM via ticket, referring to the correct folder and procedure to follow (7.51b);
- STEAM will reject any tickets requesting updates that contain files, scripts, or not refer to the build folder;
- STEAM will challenge all non-standard actions demanded in the update (permission changes, cross-environment, no documentation, ...);
- When the upgrade is done, STEAM will rename the build folder by *appending* the string "_current" (and removing it from the older);
- STEAM will clean up the 11 Apps folder, keeping only the 5 last versions;
- SQL scripts for data management (cleanup, datafix) can be send via mail until a new approach is agreed:
    - STEAM will save these scripts in a new folder 'DATAMGT' under the '_current' folder;
    - STEAM will execute these scripts with datareader and datawriter permissions.
- Only ITALS or TMD architects may request a change/update in productionGuidelines
- Each component of an application should have its own DNS alias. See below for details.
- If an application requires a fileshare, a separate DNS alias must be created for this; also see below. A DFS path is the best solution, we provide a separate namespace \\belgrid.net\FSApp for this.

- If read access is requested to the installation folder of a service or website (this is almost always the case!), this can be given through one group per environment: BELGRID\SD_Appl_Read_ACC_R for Acceptance, and BELGRID\SD_Appl_Read_PROD_R for Production servers. Modify access should never be granted. Fileshare (SMB) access to ACC and PROD Windows 2016 servers is only possible from intraclients.
- Microsoft Office is not standard (to be approved by IT Governance) on servers.
- Windows Services installed on Production will automatically be configured to restart on 1st and 2nd failure, and reset this counter after one day.
- All configuration of an application (connections, paths, …) should be made in configuration files, delivered with the package. Any other method is to be avoided (no environment variables, registry settings, …).

8.1.2 Naming Convention

Alias of server or SQL server name are available in the public part of the Steam in the Server Info and SQL Alias links.

9 Fileservers

9.1 Elia

Elia is using NetApp NAS (Network Attached Storage) for homedrives, business data and archive data. Important business data will be asynchronously replicated through our storage devices to the other site (Schaarbeek <-> Merksem).

All data is presented in fileshares that need to be mapped using the correct DNS alias given. Aliases are obsolete, the prefered way to connect the share is via the DFS link. Elia is providing a DFS (Distributed File System) in the belgrid.net domain. All new business shares will only be presented in the \\belgrid.net\Org namespace, inside the DFS folder of the top-level department of the requestor. If applications require fileshares, they will be presented in the \\belgrid.net\FSApp namespace.

Server team is monitoring disk space on the NetApp volumes closely, and will contact share owners if disk space utilization is not optimal (duplicate files for example).

NetApp snapshotting technology is used to keep 7 days of snapshots available on the primary storage; meaning users can use the 'Previous Versions' feature in Windows Explorer to find recent files themselves.

Permissions on files and shares

All files are protected by NTFS permissions. Access is granted using Active Directory security groups. Following permissions can be applied:

- **List** via SD_[sharename]_L,
- **Read** via SD_[sharename]_R and
- **Modify** (write, delete) via SD_[sharename]_U.

These groups can be managed via Group Management (Authorization Viewer - a tool that can be found on the Elia Intranet / Officezone / Practical Tools) by the owner.

No full control is given to files.

Shares are always created with Change permissions for Everyone. Only homedrive shares can be configured for offline access (synchronization to client PC's).

9.2 50HzT

50HzT is using NetApp NAS (Network Attached Storage) for homedrives, business data and archive data.

50Hzt is providing a DFS (Distributed File System) in the corp.transmission-it.de domain.

Server team is monitoring disk space on the NetApp volumes closely, and will contact share owners if disk space utilization is not optimal (duplicate files for example).

NetApp snapshotting technology is used to keep 7 days of snapshots available on the primary storage; meaning users can use the 'Previous Versions' feature in Windows Explorer to find recent files themselves.

Permissions on files and shares

All files are protected by NTFS permissions. Access is granted using Active Directory security groups. Membership of these groups is managed by ServiceDesk.

10 Backup

10.1 Standard Backup infrastructure

Elia

Elia is using Veritas Netbackup x as backup tool for physical servers and attached LUN's.

Backups are streamed in each site to a local media server, who transmits the data over the network to Emperor.

50Hz

50Hz is using windows backup for PHY servers

10.2 NetApp Backup infrastructure

Both Elia and 50Hz are using NetApp snapshot t technology to backup all NAS (CIFS and NFS) data.

10.3 Backup retention periods

All acceptance (except DB-servers) and production servers are backed up completely (incl. system state for virtual servers) daily. Development and test servers are backed up on request.

New retention policies are active since begin 2023. Overview can be found (on-prem + cloud) in

BackupRetentionGROUP20221212 .pptx

On prem :

Domain	Elia Group
Files services	14 days (every 4h) , 12 weekends (1 copy during the weekend)
Database services (Oracle, SQL, MongoDb, Sap (SQL/Saphana) (QA -ACC databases (Oracle , SQL, Mongodb, Sap*, *...) are NOT backup-ed)	14 days (1 copy/day) , 12 weekends (1 copy during the weekend)
Mail services	14 days (2 copies day) , 12 weekends (1 copy during the weekend)
VM servers	14 days (1 copy)
Physical servers	14 days (1 copy)

Cloud :

Proposal Retention Period (Azure Cloud MODE 1) / To BE

Domain	50Hz	Elia
Storage Accounts	7 days	
GIT Including: Databricks workbooks and workspaces Datafactory scripts Linked Services Logic Apps code Function Apps codes (hourly snapshots too)	30 days (configurable per project to 365d)	
Logs and Audit Information	30 days	
Integration Runtimes, Infrastructure (nsg, udr,...)	Terraform scripts stored on Files service on premise	
Wiki (our documentation)	30 days	
KeyVault	90 days	
DevOps Pipelines	30 days	
Azure Active Directory	90 days	

11 Monitoring

11.1 Elia

Server Team is using Microsoft Systems Center Operation Manager (SCOM) as monitoring tool for the Microsoft products. This is also used for disk space monitoring.

Server Team uses PRTG for Linux monitoring (via SNMPv3 only) and for Fujitsu SAP Hana hardware monitoring

HPE OneView is used as hardware monitoring system. HPSIM (HP Server Insight Management) is used for older hardware.

A watchdog (in-house developed scripts) is used for the monitoring of homemade applications. This can be accessed from the Server Team website

APC StruxureWare Data Center Expert (Schneider Electric) is used to monitor Server Room power units, temperature, humidity, cooling, …

11.2 50Hz

Server team is using Microsoft Systems Center Operation Manager (SCOM) as monitoring tool for the operating system and Microsoft products. This is also used for disk space monitoring.

Server Team uses PRTG for Linux monitoring (via SNMPv3 only) and for Fujitsu SAP Hana hardware monitoring

HPE OneView is used as hardware monitoring system.

A watchdog (in-house developed scripts) is used for the monitoring of homemade applications. This can be accessed from the Server Team website .

12 Critical Applications

A list of critical applications (the "top critical") is maintained and managed by CDO office and can be found in http://criticalapplications.belgrid.net . These applications are critical to the Elia business, and therefore need to be monitored adequately. IT Duty needs to be aware of the basic components, architecture and troubleshooting steps.

There is also a list of critical applications and critical publications on the BPA-portal.

See https://bpe-portal.elink.elia.be/Documents_tmp/Critic_applications_updateQ12024.xlsx.

To be verified which list is the most up-to-date

13 Printing

Both Elia and 50Hz are using Windows print servers to present the network printers to the end-users. These printers are currently not published in the Active Directory. The description of the printer share points to the correct location of the printer.

With the Canon Uniflow virtual (follow-me) printer system users will print to the same virtual print queues.

Printing, scanning and copying can be done on our Canon multifunctional printers . Access to the printer is done via your (access) badge .. This virtual print queue can be used on all the administrative sites of Elia and 50Hz .

.

In some cases there can be an exception to print directly to a printer without the use of Uniflow. This has to be approved by IT GOV.

14 Cloud services

For more information, please refer to our Confluence space.

14.1 Bimodal Practice

Our Azure architecture embraces the versatility of the bimodal principle, encompassing Mode 1, Mode 2, and Mode 3 environments to effectively address diverse business needs and innovation requirements.

Mode 1 (Traditional)

- Mode 1 represents our foundational systems, emphasizing stability and reliability. Management is exclusively handled by our IDS Cloud Team.
- Security measures within Mode 1 are robust, designed to protect critical assets and maintain data integrity. Oversight and management are exclusively managed by our IDS Cloud Team.
- Cost management strategies in Mode 1 focus on optimizing resources and minimizing expenditure while sustaining operational efficiency. Our IDS Cloud Team oversees cost-related initiatives independently.
- Alerting and management protocols in Mode 1 are centralized to enable swift responses and ensure regulatory compliance. Our IDS Cloud Team leads these efforts autonomously.

Mode 2 (Innovation):

- Mode 2 stands for agility and innovation, enabling rapid adaptation to market dynamics and technological advancements. The M2-Infra Team manages operations, guided by Mode 1 architects.
- Security practices in Mode 2 strike a balance between risk mitigation and agility, facilitated by the M2-Infra Team with strategic input from Mode 1 architects.
- Cost optimization strategies in Mode 2 are dynamic, led by the M2-Infra Team with guidance from Mode 1 architects.
- Alerting and management structures in Mode 2 are mainly decentralized (project lifecycle), overseen by the M2-Infra Team.

Mode 3 (Experimental/Sandbox):

- Mode 3 serves as our innovation sandbox, fostering creativity and exploration in a controlled environment. Platform maintenance is handled internally, with no support or guidance provided.
- Security measures within Mode 3 prioritize risk awareness and experimentation within defined boundaries. Our internal team ensures security protocols are in place, although no support or guidance is provided.
- Cost management strategies in Mode 3 encourage innovation while maintaining fiscal responsibility. Our team maintains budgetary oversight of projects during their definition, ensuring exploration aligns with organizational objectives.
- Alerting and management mechanisms in Mode 3 are not mandatory.

14.2 Service Catalog

Our service catalog, fully supported by our IDS Cloud Team and approved by our Steam Management, provides a comprehensive overview of all available services within our platform. This catalog encompasses a wide range of offerings, from foundational infrastructure components such as storage solutions to advanced capabilities like Fabric

suite. It enables teams to select and leverage the right resources to meet their specific requirements effectively. Additionally, this list of services is not limited and can be extended through a design review and approval process, ensuring alignment with our organization's evolving needs and objectives.

Platform Type	Category	Service Name
IaaS	Network	Express Route
IaaS	Cloud Computing	Virtual Machine
IaC	Coding	Terraform
IaC	Coding	Ansible
IaC	Coding	Biceps
IaC	Coding	Powershell
IaC	Coding	PowerCli
IaC	Coding	Rest API
PaaS	Network	CDN
PaaS	Network	Firewall
PaaS	Network	NSG
PaaS	Network	DNS
PaaS	Network	Virtual Network
PaaS	Network	Bastion
PaaS	Network	Route Server
PaaS	Network	WAF
PaaS	Event Streaming	Log Analytics
PaaS	Event Streaming	Notification Hub
PaaS	Event Streaming	Service Bus
PaaS	Event Streaming	Event Hubs
PaaS	Database	SQL DB
PaaS	Database	SQL Server
PaaS	Database	SQL Managed Instance
PaaS	Security	KeyVault
PaaS	Data Integration	Data Factory
PaaS	Data Integration	Databricks
PaaS	Big Data	Data Lake
PaaS	Automation	Logic App
PaaS	Automation	Function App
PaaS	Cloud Computing	App Services
PaaS	Cloud Computing	Azure Container Registry
PaaS	Cloud Computing	Azure Container Instance
PaaS	Cloud Computing	Azure Container Apps
SaaS	Apps	Sharepoint
SaaS	Apps	Office Suite
SaaS	Reporting	Power BI
SaaS	Messaging	Teams
SaaS	Messaging	SendGrid
SaaS	Event Streaming	Operational Insight

SaaS	Database	Mongo DB
SaaS	Identity	AAD
SaaS	Automation	Runbook
PaaS	API	API Manager
Paas	Network	Azure Front Door
SaaS	Development	Azure DevOps
SaaS	Apps	Market Place Apps
SaaS	Apps	Custom Enterprise Apps
SaaS	Coding	Power Apps
SaaS	Automation	Power Automate
SaaS	Experience Platform	Viva Engage
SaaS	Messaging	Exchange online
SaaS	Security	Microsoft Defender
SaaS	ERP	Dynamics 365

The list of services outlined above is subject to change, as it has been compiled to reflect our current needs. However, it's important to note that this list is not static. Specifically, I am referring to the catalog of Azure services currently available on our platform.

14.3 Identity

Our Azure Active Directory (AAD) operates in a meticulously chosen hybrid mode, strategically integrating with our on-premises Active Directory infrastructure, overseen by our WinCore team. This selection prioritizes security considerations, ensuring sensitive data remains under strict on-premises control while still benefiting from the cloud's agility and scalability. In this configuration, AAD refrains from storing password hashes, with user and group management primarily conducted on-premises and synchronized with the cloud.

Furthermore, our on-premises authentication mechanism is fortified by Active Directory Federation Services (ADFS), which mandates dual-factor authentication by default. This ensures an additional layer of security, bolstering our overall defense against unauthorized access and data breaches.

While Microsoft 365 (M365) groups are seamlessly provisioned in AAD, all other group creations undergo meticulous review and evaluation by our Cloud team. To streamline user and group management, we leverage advanced tools like AZViewer, with administrative oversight maintained by the business to uphold accountability and operational efficiency.

Our Azure Active Directory (AAD) also serves as a versatile platform, extending its functionality beyond internal use. It accommodates external partners with guest accounts, enabling them to securely connect to our Azure resources like Sharepoint, Teams, etc. Additionally, enterprise applications leverage AAD as their Identity Provider (IDP), facilitating Single Sign-On (SSO) authentication for seamless access to their SaaS applications. Moreover, our AAD is also configured with Cross-tenant settings to authorize other trusted tenants like EGI and Realto to interact with some of our applications in a secure and managed way.

14.4 Security

14.4.1IAM

Our Identity and Access Management (IAM) strategy prioritizes security and control, leveraging our on-premises Active Directory (AD) as the primary source of truth for user identities. All identity management activities are centralized through AD, ensuring consistency and adherence to established policies.

Exceptions to this centralized management, such as guest accounts or external partners, undergo thorough review and approval processes before being authorized in our Azure Active Directory (AAD). This approach allows us to maintain granular control over access to our platform, ensuring that only authorized and known accounts can connect.

Additionally, we enforce stringent access controls using Conditional Access policies. These policies allow us to define specific conditions under which access is granted, including factors such as user location, device health, and risk level. By leveraging Conditional Access, we can enforce Multi-Factor Authentication (MFA) and other restrictions, such as persistent browsing, to establish the most secure environment possible.

This approach not only enhances security but also ensures compliance with regulatory requirements and industry best practices. It enables us to protect our assets and data while facilitating efficient and secure collaboration with external parties.

14.4.2 Network

Our network security is fortified by a robust Hub and Spoke architecture, meticulously designed to govern inbound and outbound traffic effectively. Under the vigilant oversight of our IPNOC team, this architecture ensures comprehensive control and management of network traffic flow.

While the IPNOC team retains full control and management responsibility, our Cloud team is granted read access to Firewall (FW) logs to facilitate efficient troubleshooting in the event of issues. Moreover, to maintain the integrity of our network security posture, any proposed new FW rules undergo rigorous validation by the Cloud team before a ticket is raised and assigned to the IPNOC team for implementation. Throughout this process, all rules are subject to scrutiny by our dedicated security personnel, ensuring compliance with established security standards.

To further enhance our network security, we adhere to industry-leading design principles such as the Landing Zone and Well-Architected Framework. These frameworks provide a structured approach to network design, enabling us to build a secure, scalable, and resilient infrastructure.

Additionally, comprehensive documentation and design resources are available on our SharePoint site, offering guidance and best practices for network architecture and security implementations. This ensures alignment with organizational objectives and fosters continuous improvement in our network security posture.

At the network level, we adhere to the principle of Zero Trust, implementing stringent access controls and continuous authentication to mitigate security risks. To bolster our defense-in-depth strategy, we deploy Web Application Firewalls (WAFs) both in our on-premises DMZ zone and in the cloud, ensuring comprehensive protection against web-based threats and unauthorized access attempts. Additionally, all spokes within our Hub and Spoke architecture are fortified with Network Security Groups (NSGs) on subnets, further enhancing our network security posture.

14.4.3 Monitoring and Logging

- Log Analytics Workspaces: We utilize multiple Log Analytics Workspaces to store data from various sources such as Azure Active Directory (AAD), Network Security Groups (NSGs), serverless applications, and other critical resources.

- Alerting Criteria: Alerting is configured based on different criteria including usage patterns, traffic sources, and specific timeframes. This proactive approach helps us identify and respond to potential issues promptly.

- Purpose of Logs: Logs serve multiple purposes, including responding to management or business demands, providing predictability and forecasting, and offering insights for resource management. They are also utilized in dashboards to monitor and control resource usage effectively.

14.4.4 Data Protection

- Data Lake Security: Our environment includes Data Lakes available across four environments (tst, dev, acc, prd). These Data Lakes are accessible only privately and via secure channels, with strict access controls enforced through approval processes. Any connection to these Data Lakes must undergo rigorous validation before being granted access.

- Sensitive Data Protection: We prioritize the protection of sensitive data, such as personally identifiable information (PII) like street addresses and phone numbers. Robust processes and authorization mechanisms are implemented to ensure that access to such data is strictly controlled. Additionally, external connections, including those with external partners or SaaS integrations, undergo thorough review and validation to mitigate the risk of unauthorized access or data exposure.

- Authorization Principles: All access requests follow a standardized authorization process, adhering to principles of security, GDPR compliance, and business ownership. Each request undergoes scrutiny and approval by relevant stakeholders, including security teams, GDPR compliance officers, business owners, and the Cloud team, before any authorization is granted.

14.4.5 Least Privileges

We implement Azure Privileged Identity Management (PIM) to manage access to Azure resources, ensuring strict control and adherence to the principle of least privilege. All access assignments are orchestrated through groups established within our Azure Active Directory (AAD), allowing for centralized management and streamlined access provisioning.

To further enhance security, all PIM roles, including critical roles like Global Administrator, undergo customization to align with our organization's security requirements. For instance, upon activation of the Global Administrator role, an alert is triggered, initiating an approval process to carefully vet and authorize access.

Additionally, we enforce a time limit on the duration of PIM enablement, ensuring temporary access is granted only when necessary and for a limited period, with a maximum duration of 10 hours. This helps mitigate the risk of prolonged elevated privileges and potential security breaches.

Furthermore, we embrace the principle of least privilege across all resources provided to engineers, aiming to minimize the attack surface and vulnerabilities. To achieve this, we create custom roles within our Azure AD, tailoring permissions to specific job roles and responsibilities. This approach ensures that users have access only to the resources essential for their tasks, reducing the risk of unauthorized access and data breaches.

Overall, PIM serves as a crucial component in our security arsenal, primarily facilitating administrative access while maintaining stringent control and adherence to security best practices.

14.5 Azure Naming Convention

As part of our Azure infrastructure, having clear and consistent naming conventions is crucial. It helps us manage our resources effectively, ensuring everything is organized and easy to understand. We have detailed guidelines available on SharePoint to keep everyone on the same page."

In addition to naming, using tags is also really important. Think of tags as labels that provide extra information about our resources. They help us categorize and track everything, which is essential for keeping our costs in check and understanding our infrastructure better.

Following these conventions and using tags isn't just about convenience; it's about good practice. It helps us work more efficiently and ensures everyone knows what's what in our Azure environment. It's all about keeping things organized and making sure we're making the most of our resources.

Sharepoint Link: EliaGroup - Azure Cloud Naming Convention.docx

14.6 Architecture Design

In our Azure environment, every project begins with a meticulous architecture design process. Before any new project is onboarded, we craft a comprehensive architecture design document. This document serves as a blueprint for the proposed solution, outlining its components, interactions, and overall structure.

Once the architecture design document is ready, it undergoes rigorous review by our Architecture Board. This board comprises experienced architects and stakeholders who assess the proposed solution's alignment with our organizational objectives, compliance requirements, and best practices.

Upon acceptance by the Architecture Board, the solution proceeds to implementation in Azure. This rigorous process ensures that every solution deployed in our Azure environment is carefully planned, reviewed, and aligned with our strategic goals. It fosters consistency, reliability, and scalability in our Azure architecture, ultimately supporting our business initiatives and driving innovation forward.

Sharepoint Link: Design

14.7 M365 Suites

In our M365 suite services, including SharePoint, Teams, and OneDrive, operational management falls under the purview of the Digital Accelerators team, led by Johan Maricq. However, oversight and security control remain firmly within the domain of the IDS Cloud Team. We enforce stringent security measures to safeguard these services, leveraging Privileged Identity Management (PIM) to minimize the attack surface and mitigate the risk of human errors.

Additionally, the council, with a focus on German regulations, plays a crucial role in verifying and controlling data accessibility. They ensure that only authorized data is shared among teams and external identities, maintaining compliance with data privacy regulations.

While IDS does not manage the data within these services, we provide guidance and ensure adherence to security principles such as least privileges and zero trust. Licensing is managed through group memberships synced from on-premises, with access control handled by on-premises groups overseen by business owners.

Furthermore, Digital Accelerators is tasked with license procurement, while IDS monitors license consumption closely. We employ automated scripts to alert Digital Accelerators when license limits are nearing exhaustion, ensuring seamless license management and resource allocation.

This collaborative approach ensures the effective management, security, and compliance of our M365 suite services, enabling our organization to leverage these tools efficiently while mitigating risks effectively.

14.8 SaaS

In our approach to adopting Software as a Service (SaaS) solutions within our Azure platform, we prioritize thorough evaluation and scrutiny to ensure alignment with our security and infrastructure standards.

Before authorizing the onboarding of any new SaaS application, requestors are required to provide a completed SaaS Survey, furnished by the application provider. This survey undergoes meticulous review and commentary by IDS management, comprising representatives from security, cloud, network, and management teams. This collaborative process allows us to assess the potential impact on our infrastructure, evaluate the necessity of the application, and determine whether it should be hosted in our cloud or on-premises. These considerations are weighed against the criticality of the application and the sensitivity of the data it handles.

Security measures for all SaaS applications are rigorously enforced, with secrets defined based on various criteria such as external accessibility and data access requirements. Access to SaaS applications is controlled through group synchronization from on-premises, ensuring that only authorized individuals can access these resources. Additionally, where feasible, access to API permissions can be further restricted by modifying application settings.

As part of our governance framework, comprehensive documentation of all SaaS applications is maintained and accessible. This documentation provides transparency and insight into the SaaS landscape within our organization, facilitating informed decision-making and ensuring compliance with our established standards and practices.

For further details and documentation on our SaaS landscape, please refer to the attached link.

OneNote Link: https://dev.azure.com/EliaGroup-M1-IDSManagement/Cloud%20Projects/_wiki/wikis/Cloud-Projects.wiki/281/New-Enterprise-application-with-SSO

15 Service Window

15.1 For Elia:

Service windows have to be announced at least one week upfront.

For critical applications : need alignment via the application responsible and needs to be planned during business hours (10-16h) as our critical applications are heavily used between 16-22h .

For non critical applications : can be done after business hours – users need to be informed as well (Pulse – mail)

- Driver updates;
- Hardware or software configuration changes;
- Data or server migrations;
- …

Security updates will be deployed between 2:00 and 4:00 on the chosen patch window (see below).

All applications should support service interruptions and server reboots during this service window. Changes will be tested on acceptance servers before production if possible.

In addition, all servers are rebooted twice a month. Elia has the following server reboot slots:

- First Monday + Tuesday of the month between 04:00 and 04:45; this constitutes the patch validation group
- Second Monday + Wednesday OR Tuesday + Thursday of the month between 05:15 and 06:45; for development and acceptance
- Third Monday + Wednesday OR Tuesday + Thursday of the month between 05:00 and 06:45; first part of production
- Fourth Monday + Wednesday OR Tuesday + Thursday of the month between 05:00 and 06:45; second part of production

These reboots are necessary to activate automatically deployed patches and to guarantee servers in optimal condition (see chapter 15).

15.2 For 50Hz :

- Changes with unacceptable long downtime and high impact on business and system operation (after commitment from system operation only)
  - Every 3rd Tuesday/quarter 03:30 – 06:30
- Changes with significant risk on system operation but not on business (after commitment from system operation only)
  - Business day 11:30 – 13:30
- Changes with significant risk on business but not system operation
  - Business day 19:00 - 22:00
- Changes with significant risk or acceptable downtime on business and system operation (after commitment from system operation only)
  - Business day 19:00 - 22:00
- Changes w/o significant risk
  - All business hours outside 08:00 – 11:00

15.3 End Year Freeze

To avoid issues on our production environment, an end-year freeze is in place the 2 last weeks of every year (exact period is defined begin December). During this period no changes are allowed in production. Only critical bug fixes or business requirement updates are allowed after the GO of Server Team responsible or his deputies.