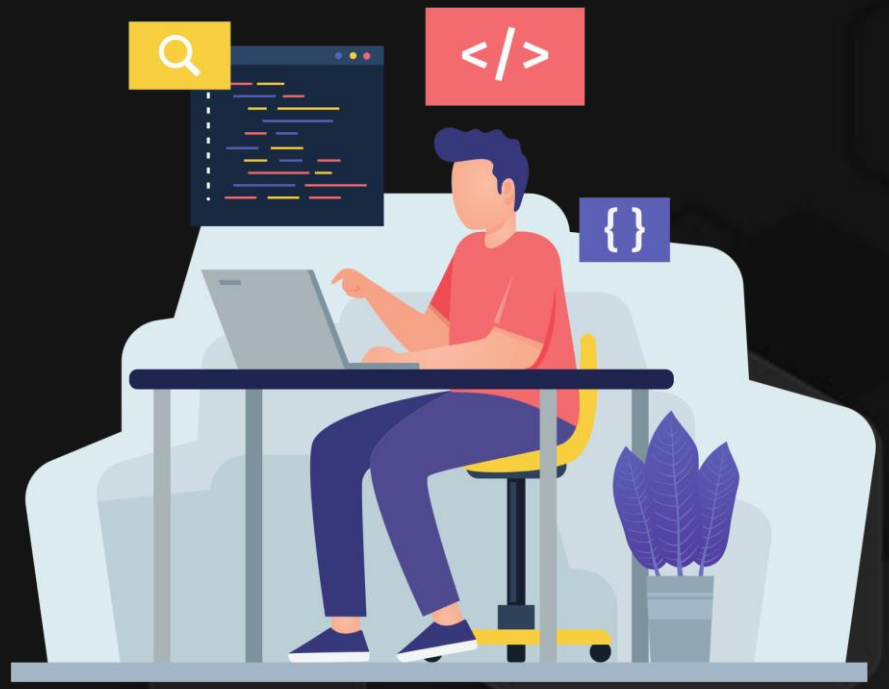
28th International Scientific Conference of Young Scientists and Specialists (AYSS-2024)

Development of Information Systems' Infrastructure for BM@N Data Processing

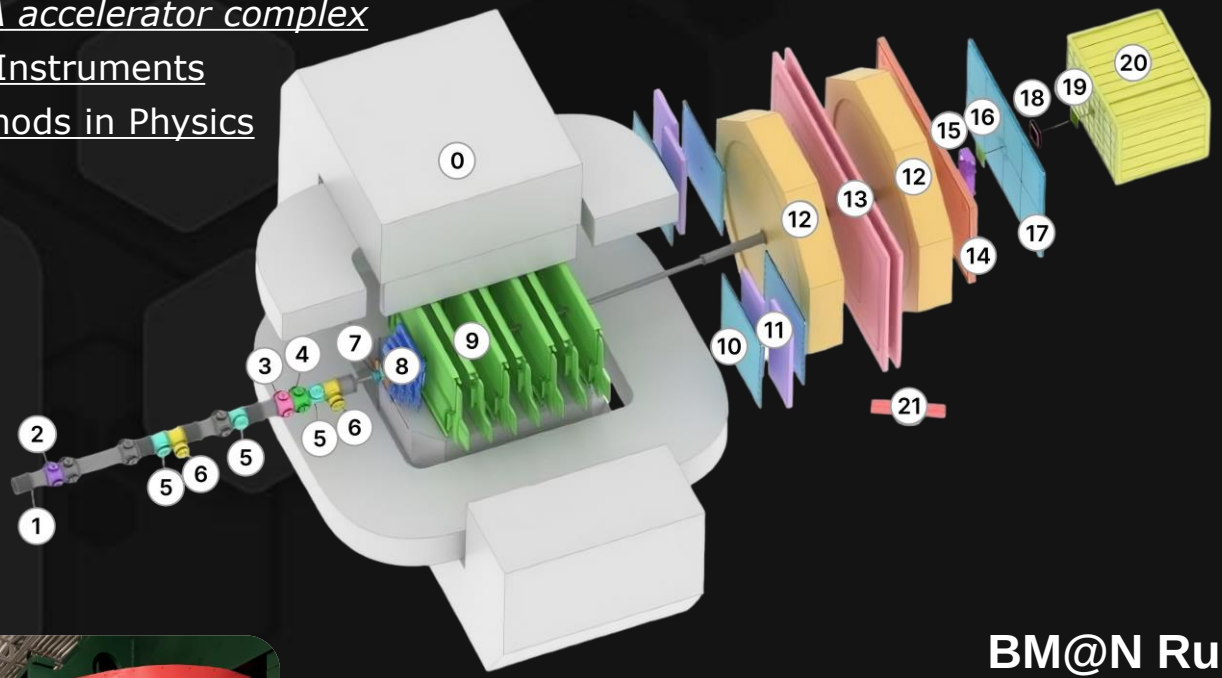


Alexander Chebotov
Konstantin Gertsenberger
Ilya Romanov
JINR, LHEP

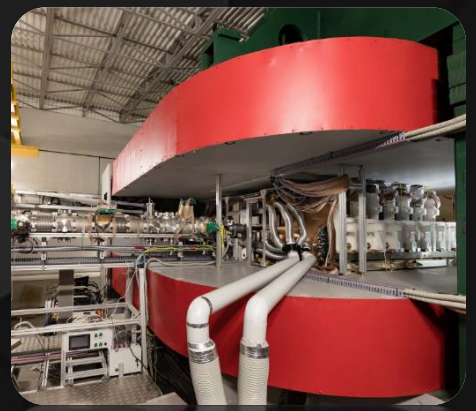
29/10/2024

Baryonic Matter @ Nuclotron (BM@N)

The BM@N spectrometer at the NICA accelerator complex
Nuclear Instruments and Methods in Physics



- Magnet SP-41
- Vacuum Beam Pipe (1)
- BC1, VC, BC2 (2-4)
- SiBT, SiProf (5, 6)
- Triggers: BD + SiMD
- FSD, GEM (8, 9)
- CSC 1x1 m^2 (10)
- TOF 400 (11)
- DCH (12)
- TOF 700 (13)
- ScWall (14)
- FD (15)
- Small GEM (16)
- CSC 2x1.5 m^2 (17)
- Beam Profilometer (18)
- FQH (19)
- FHCal (20)
- HGN (21)



BM@N Runs (2015 – 2023)

- ❖ Session №51 (d,C) Feb. 22 – Mar. 15, 2015
- ❖ Session №52 (d) June 29 – June 30, 2016
- ❖ Session №53 (d, $d^{\uparrow}$) Dec. 9 – Dec. 23, 2016
- ❖ Session №54 (C) Mar. 7 – Mar. 18, 2017
- ❖ Session №55 (C,Ar,Kr) Mar. 3 – Apr. 05, 2018
- ❖ Session №56 (C) (SRC) Mar. 7 – Mar. 28, 2022
- ❖ Session №57 (Xe) Dec. 12 – Feb. 02, 2023

OUTLINE

01

Systems, services

Provide tools for storage, processing, and management of BM@N experiment data.

02

Cluster, Proxmox

Virtualization of services on the DAQ C4 Cluster under Proxmox management, ensuring a stable infrastructure for continuous operation of systems.

03

Docker, CoDeS

Automation of deployment processes through containerization using Docker and CoDeS, enabling rapid and scalable updates of system components.

04

Single Sign-On

The integration of a Single Sign-On (SSO) system using Keycloak provides centralized access management for all services and systems.

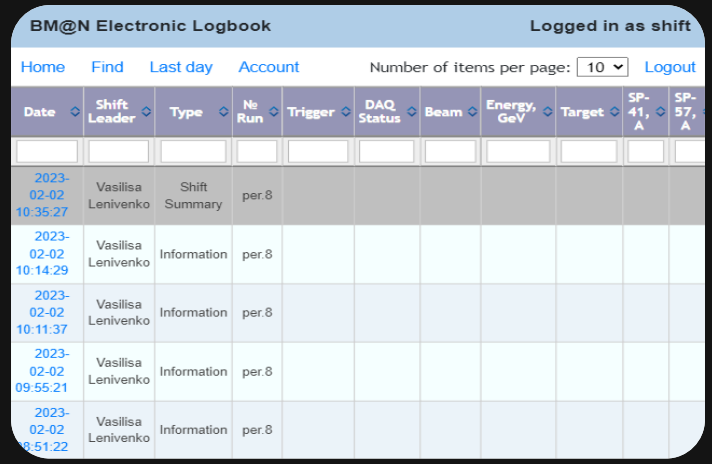
05

Security, Gateway

The implementation of a centralized gateway provides secure and controlled access to all systems within the infrastructure. This gateway acts as a single point of entry .

Electronic Logbook (e-Log platform)

The Electronic Logbook allows collaboration members to record information on events, system states, and detector operation during experiment runs, such as particle types, energies, magnetic field, and triggers. The data is crucial for the further processing and analyzing of BM@N collision events.



Condition Database (UniConDa)

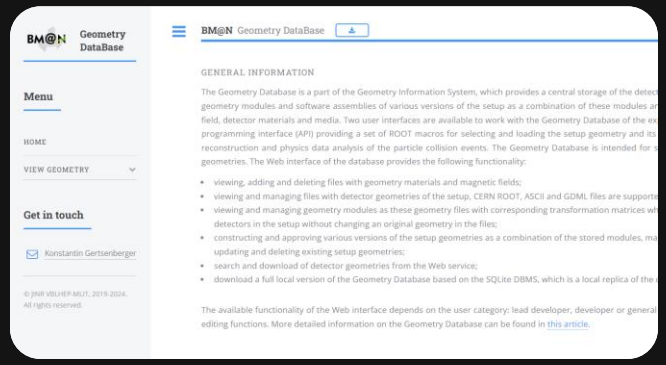
The Condition Database is designed for storing and managing parametric information related to the experiment systems to be further used in simulation, reconstruction and physics analyses.

Event Metadata System (Event Catalogue)

The Event Metadata System is based on the Event Catalogue, which contains summary information on recorded particle collision events and allows for the quick selection of only those events needed for a particular physics analysis.

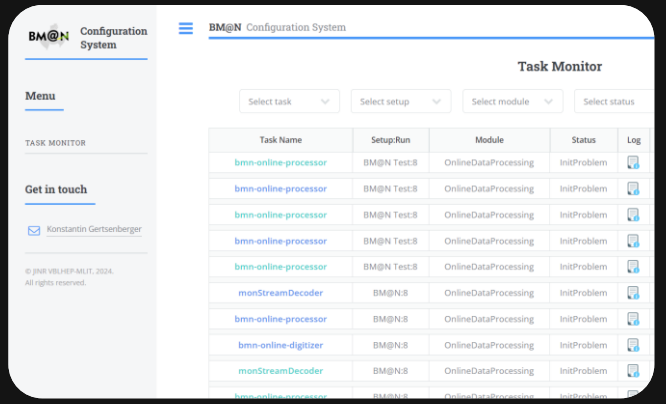
Geometry Database

The Geometry Information System is based on the Geometry Database, which is intended to store and manage data on geometric models of detectors, and to provide a centralized repository for detector geometries.



Online Configuration Platform

The Configuration Information System is used to store and provide data on the configuration of hardware and software systems of the experiment during online data acquisition from the detectors.



Official BM@N Website

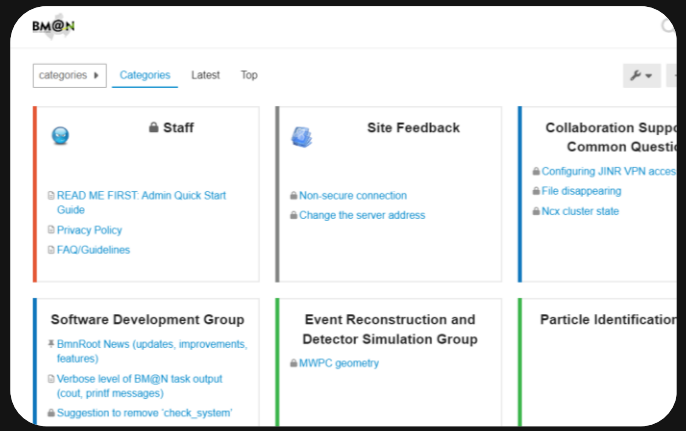
The official website of the BM@N experiment serves as a important source of information on the experiment, participants, results, and project-related news.

BM@N Forum

BM@N forum has been developed to provide the collaboration members with discussion platform, exchanging ideas and experience, and collectively addressing important questions.

NICA-Scheduler Interface

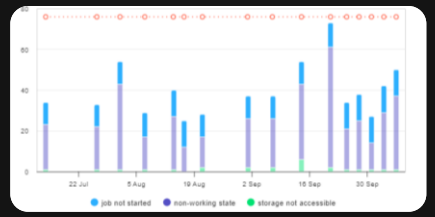
NICA-Scheduler is a package that simplifies task running on clusters using existing batch processing systems (SLURM, SGE, Torque) without knowledge of these systems.



Tango Parameter Viewer

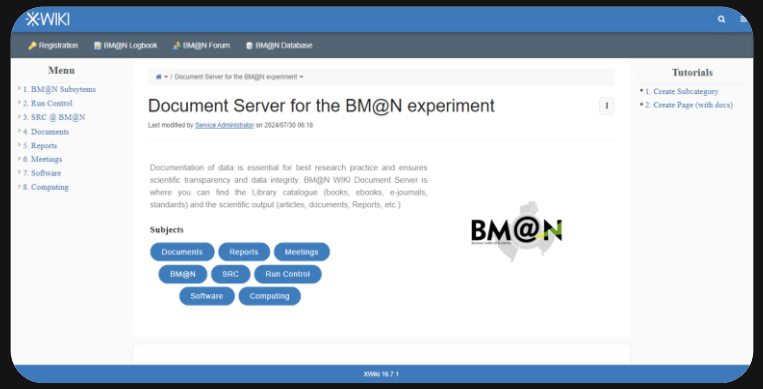
Tango Viewer is a viewer for hardware parameters of the Slow Control System.

Cluster Inspector File Inspector



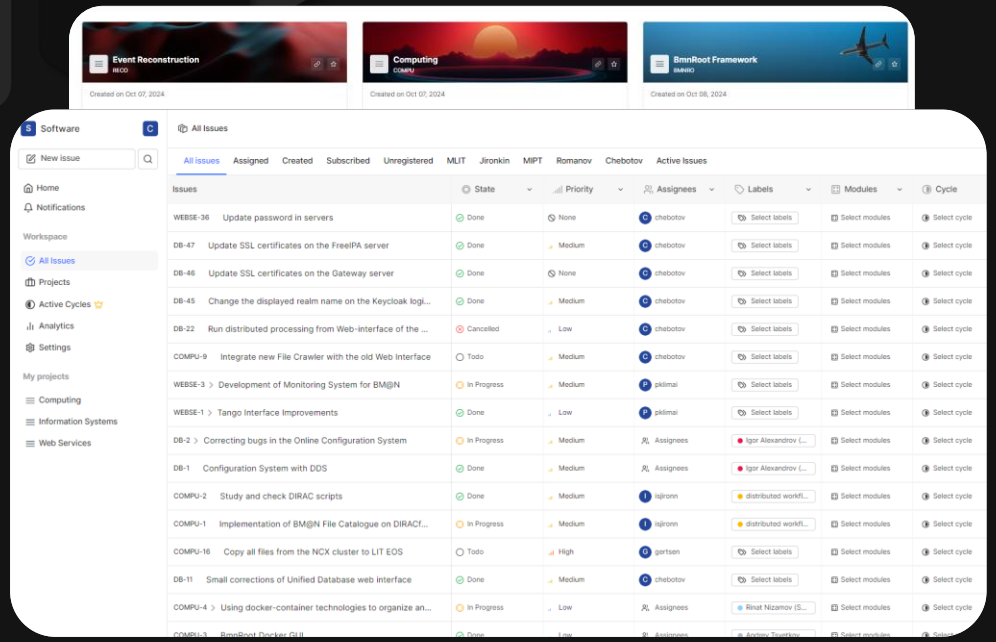
BM@N WIKI

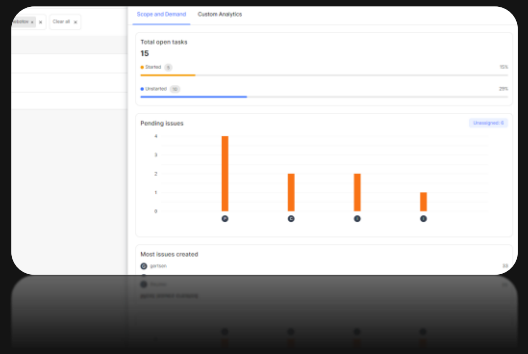
The BM@N Wiki System ensures a document server for the experiment, which provides centralized storage and access to a variety of materials and documentation.



BM@N Project Management System

BM@N Project Management System is a tool that enables efficient task coordination and tracking the software progress.





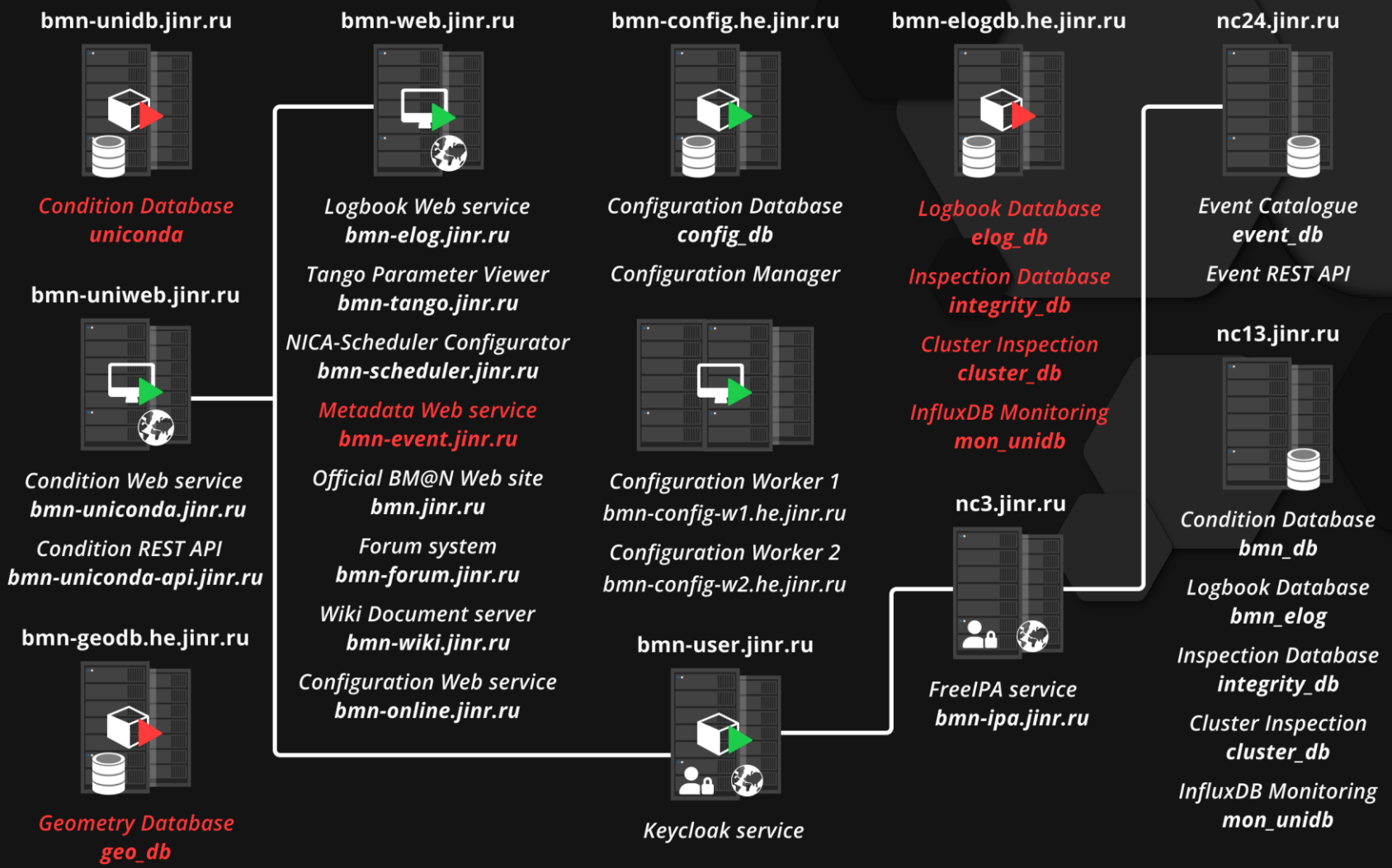
Plane

- Intuitive Interface
- Progress Tracking
- Real-time task updates
- SSO-enabled

- Kanban boards
- Lists
- Timelines

Old Infrastructure

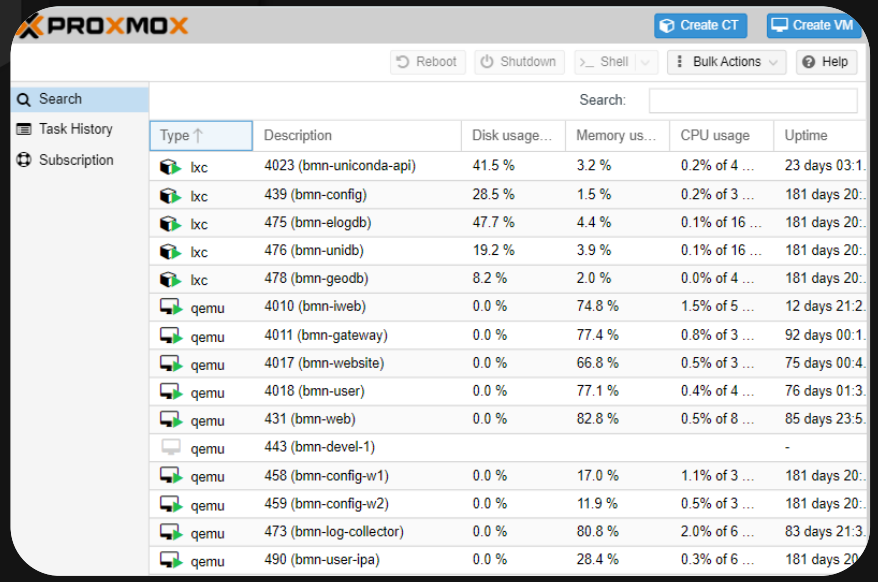
- Security vulnerability
- Difficult to control
- Limited scalability and conflicts
- Lack of modern technologies



DAQ C4 Cluster

LHEP
Building 201

Proxmox is a virtualization and resource management platform that allows one to create **VMs** and containers using virtualization technologies such as **KVM** for **VMs** and **LXC** (Linux Containers) for containers.



- Versatility: Support for virtual machines and containers.
- High-Performance Storage: Utilizing Fast SSD Storage.
- Convenient Interface: Web interface for managing all aspects of virtualization.
- Backups and Recovery: Integrated tools for creating backups.
- Performance: Good performance for virtual machines with KVM.
- Free Software: Software based on open-source code.

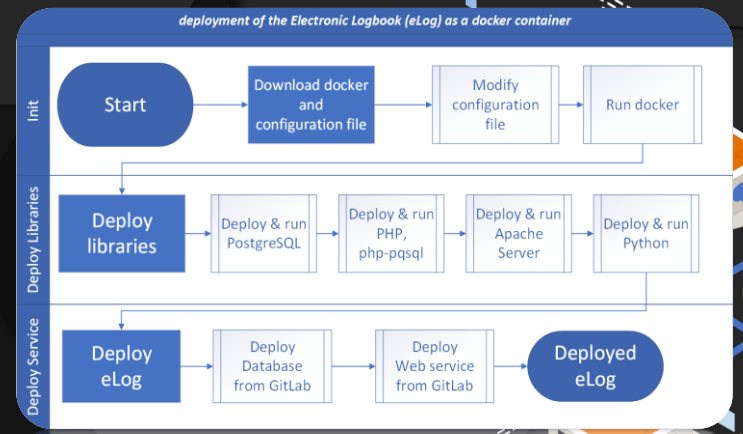
Deployment and Service Management with Docker and CoDeS

We use Docker containerization and the CoDeS system for efficient deployment of BM@N software systems

- **Isolated environment**
- **Image portability**
- **Resource efficiency (lightweight)**

- **Centralized configuration management**
- **Updates and scaling**
- **Uniformity**

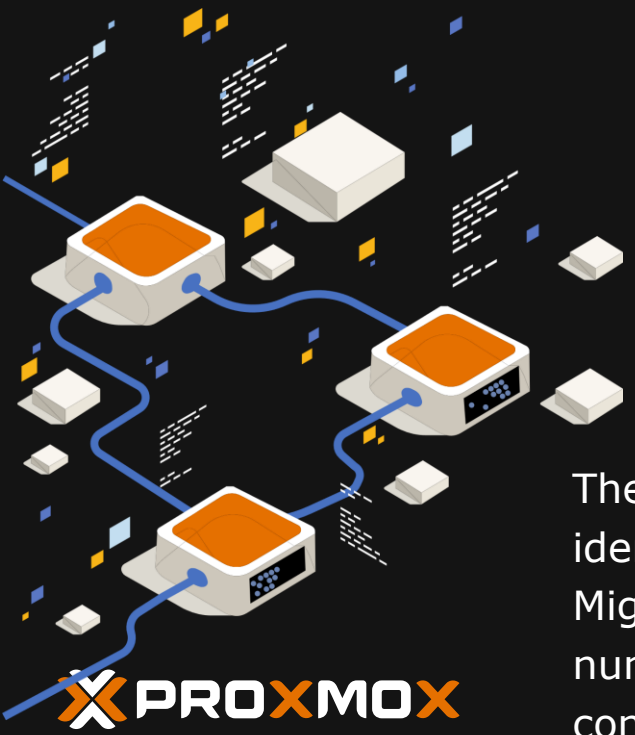
Run deploy script




```
elog_platform]# docker ps -a
IMAGE     COMMAND                  CREATED             STATUS             PORTS                                   NAMES
nginx     "/docker-entrypoint.…"   About an hour ago   Up About an hour   0.0.0.0:80->80/tcp, :::80->80/tcp       elog_web
web_php   "/entry-elog-php.sh …"   About an hour ago   Up About an hour   9000/tcp                                elog_php
```

```
~]# docker ps -a
IMAGE           COMMAND                  CREATED       STATUS       PORTS                                       NAMES
postgres:12.4   "docker-entrypoint.s…"   2 hours ago   Up 2 hours   0.0.0.0:5432->5432/tcp, :::5432->5432/tcp   elog_db
```

The Common Deployment System is based on Docker containers and python scripts

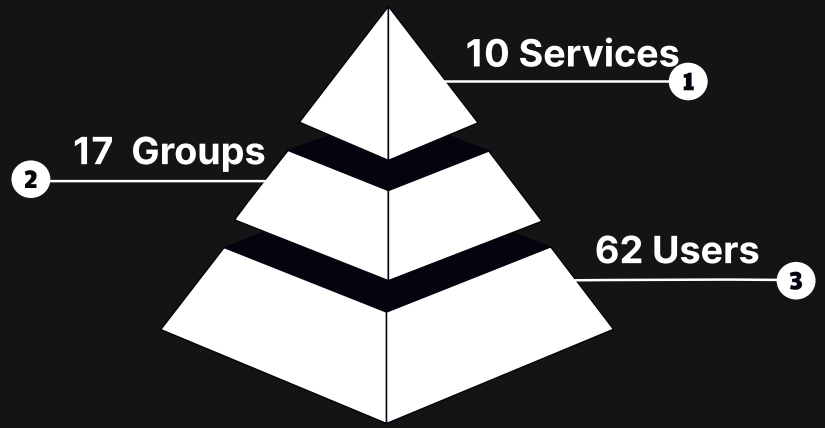


Implementation of a Single Sign-On (SSO)

FreeIPA

KEYCLOAK

The Keycloak system — a modern and reliable solution for identity and access management.
Migrating to Keycloak for implementing Single Sign-On offers numerous benefits, including centralized management, user convenience, and enhanced security.



- User Convenience
- Enhanced Security
- Centralized User Management

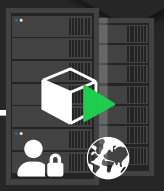
Keycloak ensures two protocols such as OpenID Connect and OAuth 2.0

User Federations

bmn-user-ipa.jinr.ru

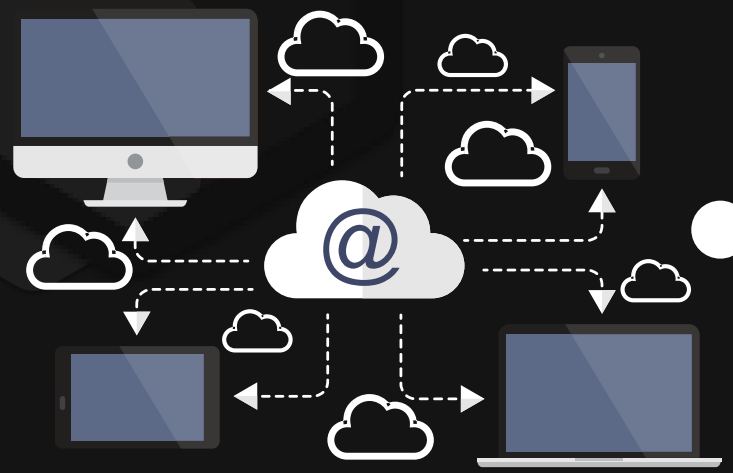
FreeIPA service
bmn-login.jinr.ru

bmn-user.jinr.ru



Keycloak service

Gateway Implementation



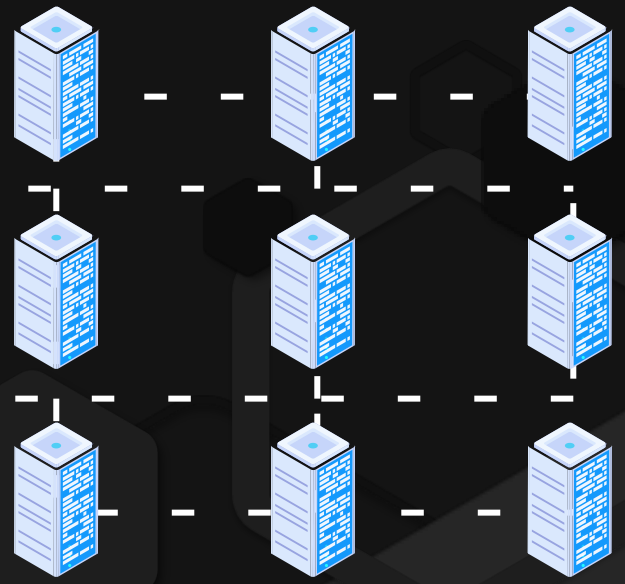
API GATEWAY

The **Gateway** acts as a single entry point, managing and controlling all incoming requests to internal services.

Centralized Access

- **Single External IP Address**
- **Traffic Routing**
- **Reverse Proxy (nginx)**

~~❑ Public Servers~~



XML-RPC is a remote procedure call protocol.

Details of implementation

NGINX is a high-performance web server and reverse proxy that plays an important role in managing traffic and ensuring security within BM@N infrastructure.

NGINX not only helps manage traffic but also protects the infrastructure, ensuring flexibility, security, and scalability.

Reverse Proxy

- SSL Termination
- Reverse Proxying
- Traffic Protection and Filtering
- Performance Optimization(**GZIP**)
- Centralized Logging

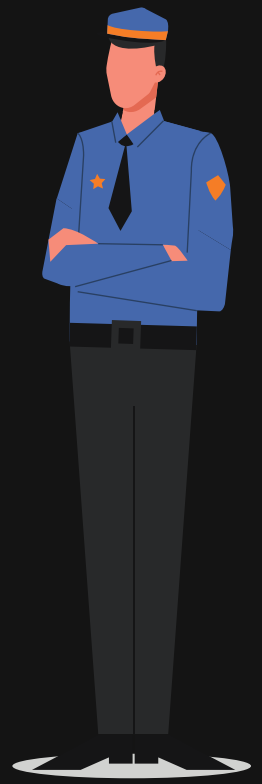
LOG

GZIP

Details of implementation

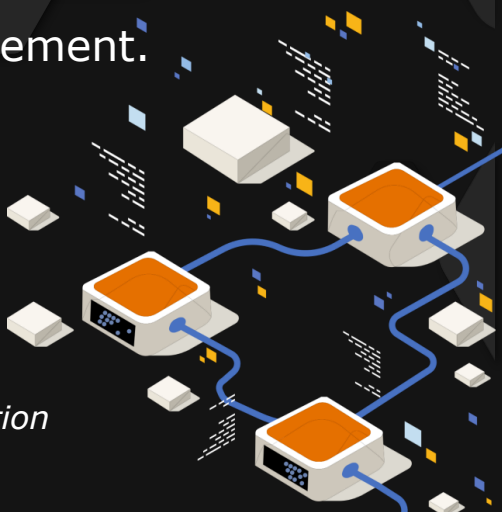
More then 2000+ banned

- IPTABLES: Traffic filtering at the Linux kernel level.
- Fail2Ban: Automated IP blocking on suspicious activity.
- Regular Updates: Keeping systems and packages up to date to patch vulnerabilities.
- Logging and Analysis: Monitoring and analyzing all events to prevent threats.



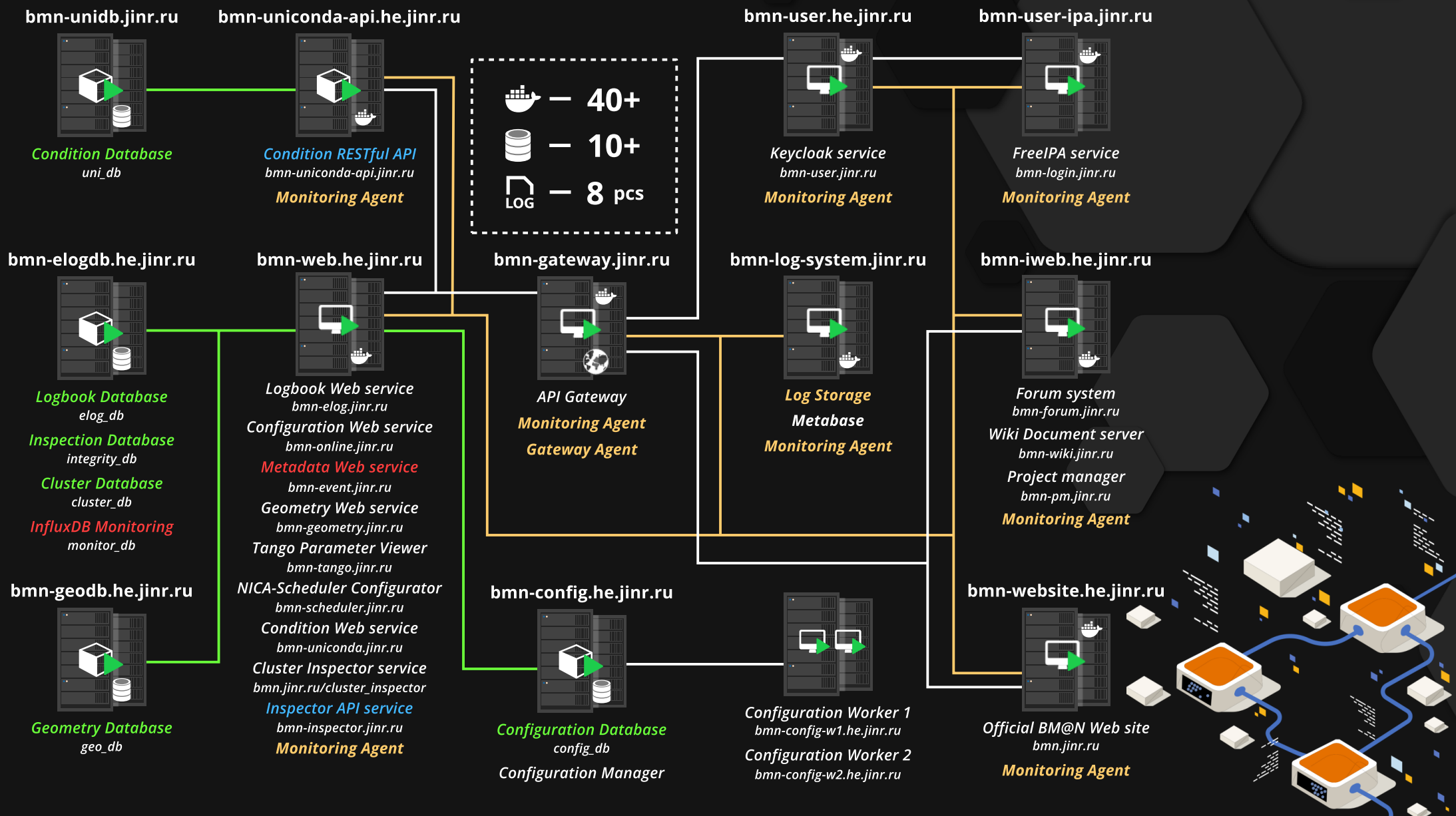
- Rate Limiting
- Authentication Protection
- Malicious Bot Detection
- Sensitive File Protection
- Traffic Filtering

- Optimized performance.
- Simplified system management.



Ilya Romanov

Current Infrastructure



Conclusions

- Significant progress has been made in deploying new services, systems, and databases, as well as in smooth transition to the new software infrastructure.
- The integration of these services with Keycloak authentication and authorization provides a high level of security.
- The performance of the new BM@N software infrastructure has been optimized, which ensures seamless operation for the BM@N experiment.

Thank you for your attention!