



08-10 October 2024
13th Collaboration Meeting of the
BM@N Experiment at NICA

Development of Infrastructure for BM@N Information Systems



Alexander Chebotov
Konstantin Gertsenberger
Ilya Romanov
JINR, LHEP

OUTLINE

01



Systems, services

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

Cluster, Proxmox

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



02

03



Docker, CoDeS

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

Single Sign-On

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



04

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)

The Online Logbook System allows collaboration members to record information about events, system states, and detector operation during experiments, such as particle type, energy, magnetic field, and triggers. This data is crucial for analyzing particle collisions, making multi-user access essential for high-energy physics experiments.

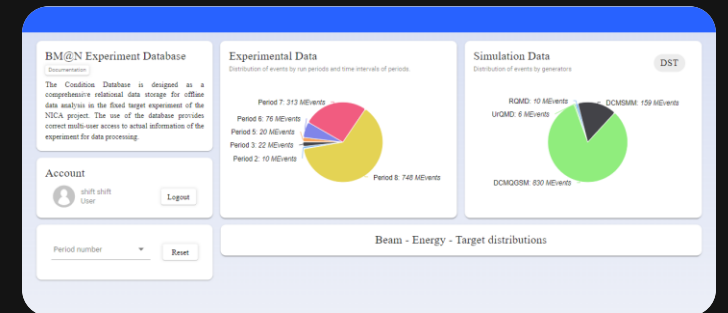
BM@N Electronic Logbook Logged in as shift

Home Find Last day Account Number of items per page: 10 Logout

Date	Shift Leader	Type	Ns Run	Trigger	DAQ Status	Beam	Energy GeV	Target	SP-41, A	SP-57, A
2023-02-02 10:35:27	Vasilisa Lenivenko	Shift Summary	per 8							
2023-02-02 10:14:29	Vasilisa Lenivenko	Information	per 8							
2023-02-02 10:11:37	Vasilisa Lenivenko	Information	per 8							
2023-02-02 09:55:21	Vasilisa Lenivenko	Information	per 8							
2023-02-02 9:51:22	Vasilisa Lenivenko	Information	per 8							

Condition Database(UniConDa)

The Condition Database is designed for storing and managing parametric information related to the experiment systems, which is essential for data processing.



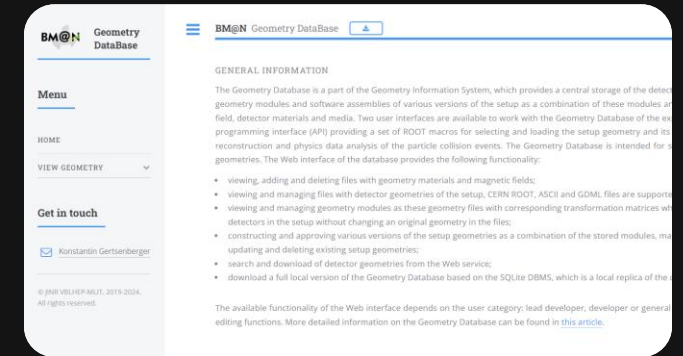
Event Metadata System

The Event Metadata System is built on the Event Database (Event Catalogue), which contains summary information about recorded particle collision events and allows for the quick selection of only those events needed for specific physical analysis.



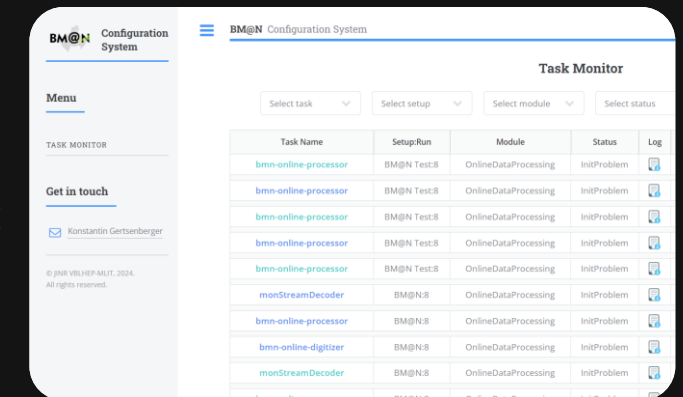
Geometry System

The geometry information system, based on the geometric database, stores and processes data about the composition and geometric structure of detectors used in experiments, providing a centralized repository for geometries.



Configuration System

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 collection from the detectors.



Official BM@N Website

Our website is the official BM@N website, serving as a crucial source of information about the experiment, participants, results, and project-related news and events.

BM@N Forum

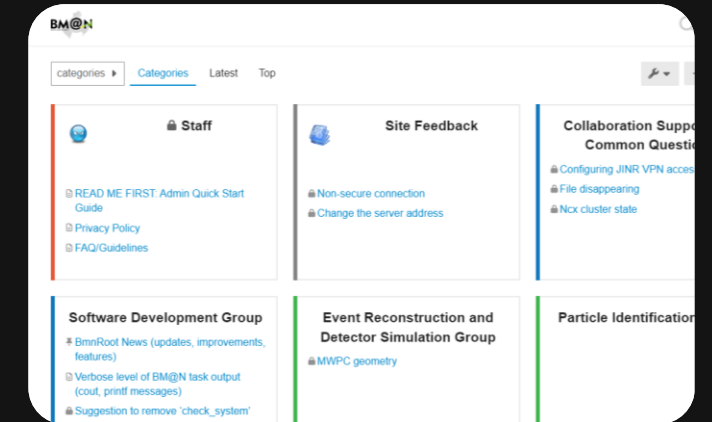
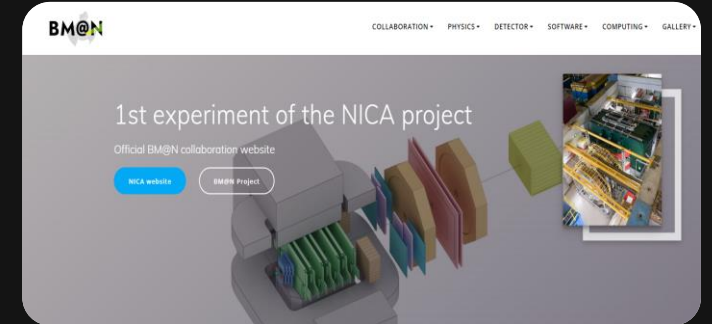
This is a place where our scientists and participants can discuss, exchange ideas and experiences, explore new directions, and collectively address important questions.

Scheduler Interface

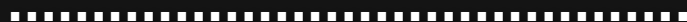
Scheduler is a module for the ROOT and FairRoot frameworks that simplifies task distribution on clusters using existing batch processing systems (SLURM, SGE, Torque) and supports parallel task execution.

BM@N Tango

BM@N Tango is a viewer for hardware parameters of the slow control system.



Cluster Inspector File Inspector

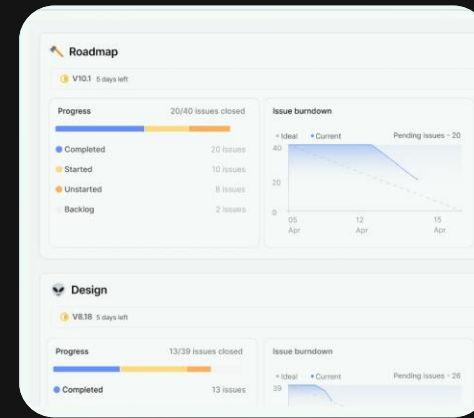
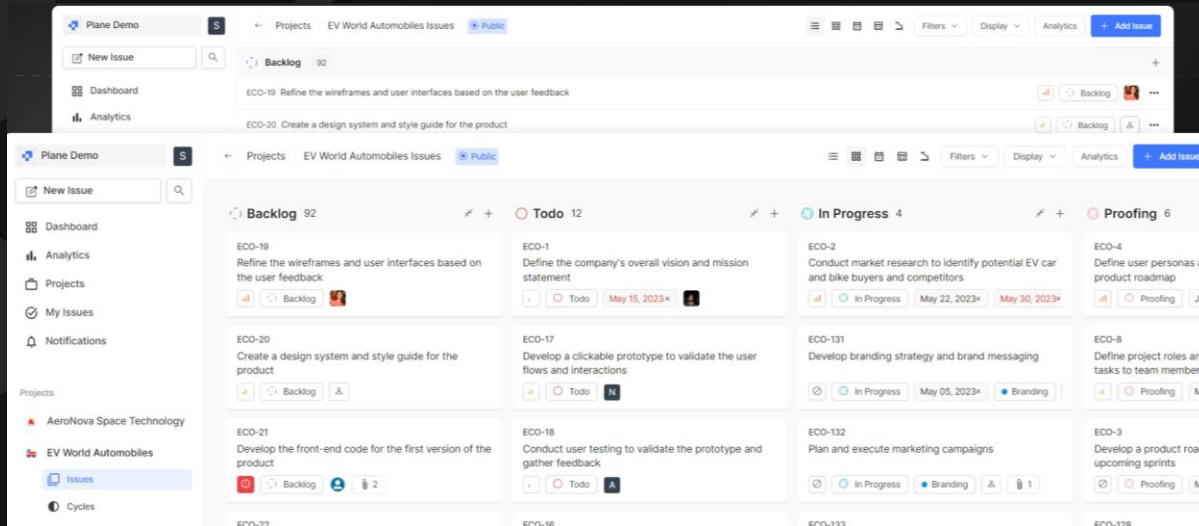


BM@N WIKI

The use of a content management system in experiments provides centralized storage and access to a variety of materials and documentation.

BM@N Project Manager

BM@N Project Manager is a project management tool that enables efficient task coordination and optimization of workflows.

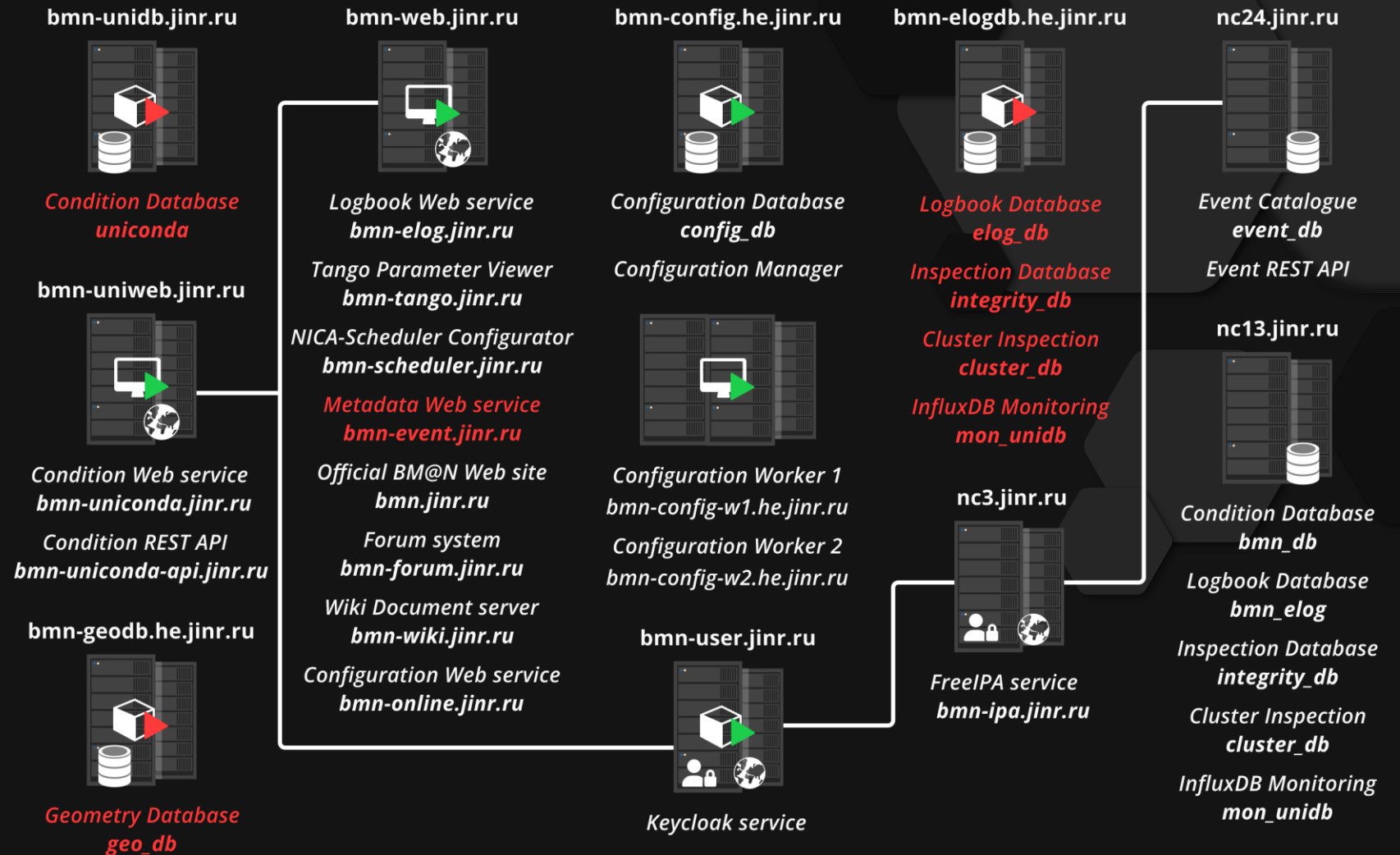


- ❖ Kanban boards
- ❖ Lists
- ❖ Timelines

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

Past Infrastructure

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



DAQ C4 Cluster

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



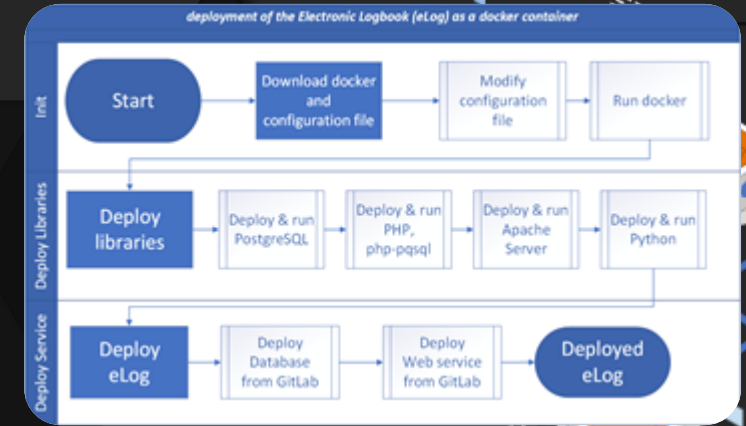
- ❖ Versatility: Support for virtual machines and containers.
- ❖ High-Performance Storage: Utilizing Fast SSD Storage.
- ❖ Convenient Interface: Web interface for managing all aspects of virtualization.
- ❖ Backups and Recovery: Integrated tools for creating backups.
- ❖ Performance: Good performance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

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime
lxc	4023 (bmn-uniconda-api)	41.5 %	3.2 %	0.2% of 4 ...	23 days 03:1
lxc	439 (bmn-config)	28.5 %	1.5 %	0.2% of 3 ...	181 days 20:
lxc	475 (bmn-elogdb)	47.7 %	4.4 %	0.1% of 16 ...	181 days 20:
lxc	476 (bmn-unidb)	19.2 %	3.9 %	0.1% of 16 ...	181 days 20:
lxc	478 (bmn-geodb)	8.2 %	2.0 %	0.0% of 4 ...	181 days 20:
qemu	4010 (bmn-iweb)	0.0 %	74.8 %	1.5% of 5 ...	12 days 21:2
qemu	4011 (bmn-gateway)	0.0 %	77.4 %	0.8% of 3 ...	92 days 00:1
qemu	4017 (bmn-website)	0.0 %	66.8 %	0.5% of 3 ...	75 days 00:4
qemu	4018 (bmn-user)	0.0 %	77.1 %	0.4% of 4 ...	76 days 01:3
qemu	431 (bmn-web)	0.0 %	82.8 %	0.5% of 8 ...	85 days 23:5
qemu	443 (bmn-devel-1)	-	-	-	-
qemu	458 (bmn-config-w1)	0.0 %	17.0 %	1.1% of 3 ...	181 days 20:
qemu	459 (bmn-config-w2)	0.0 %	11.9 %	0.5% of 3 ...	181 days 20:
qemu	473 (bmn-log-collector)	0.0 %	80.8 %	2.0% of 6 ...	83 days 21:3
qemu	490 (bmn-user-ipa)	0.0 %	28.4 %	0.3% of 6 ...	181 days 20:



Deployment and Service Management with Docker and CoDeS

We use Docker containerization and the CoDeS system for efficient deployment and management of our services.



- Isolated environment
- Image portability
- Resource efficiency (lightweight)
- Centralized configuration management
- Updates and scaling
- Uniformity



Run deploy script

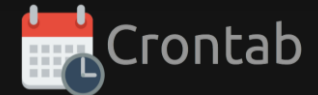


```
eLog_platform]# docker ps -a
```

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



Tracking updates



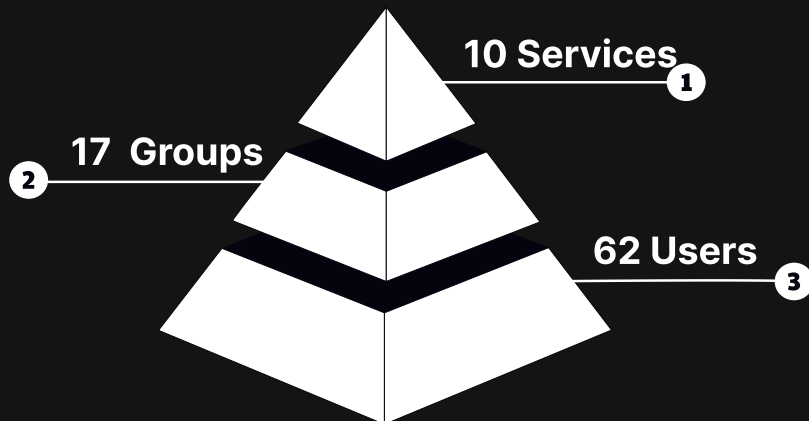
The Common Deployment System is based on Docker containers and shell scripts

Implementation of a Single Sign-On (SSO)



Keycloak—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.



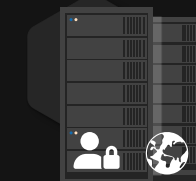
- ❖ User Convenience
- ❖ Enhanced Security
- ❖ Centralized User Management

Keycloak is based on two important protocols, OpenID Connect and OAuth 2.0



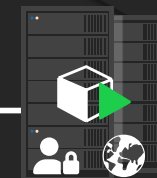
User Federations

bmn-user-ipa.jinr.ru



FreeIPA service
bmn-login.jinr.ru

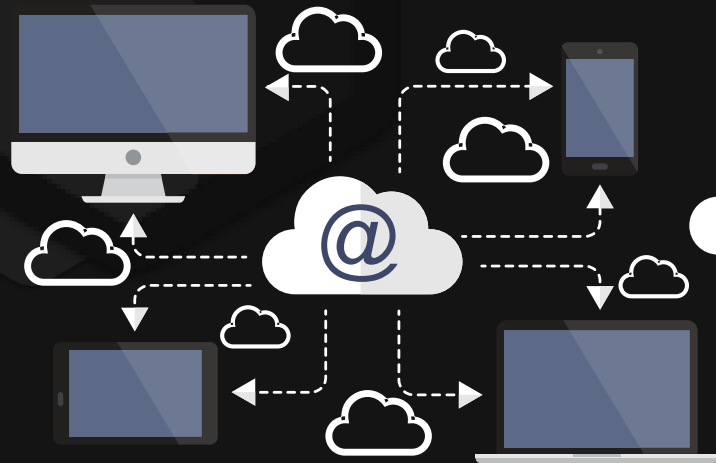
bmn-user.jinr.ru



Keycloak service

Gateway Implementation

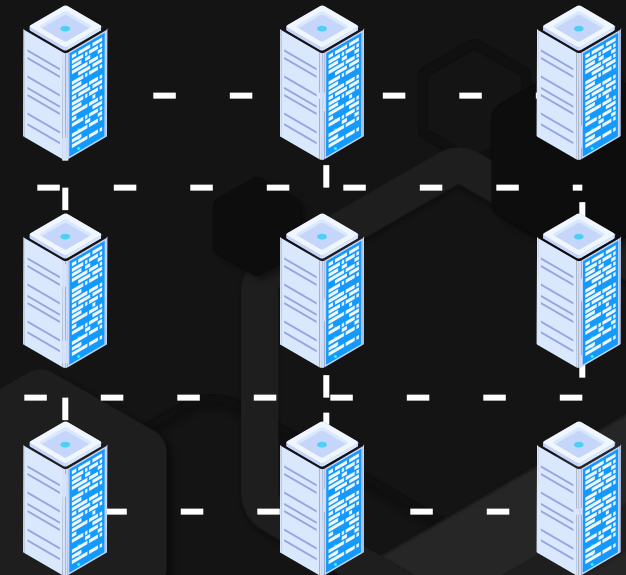
➤ Single point of failure



➤ Configuration and maintenance complexity



~~Public Servers~~




Details of protection implementation

NGINX is a high-performance web server and reverse proxy that plays a crucial role in managing traffic and ensuring security within our infrastructure.

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


NGINX




Reverse Proxy

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


LOG

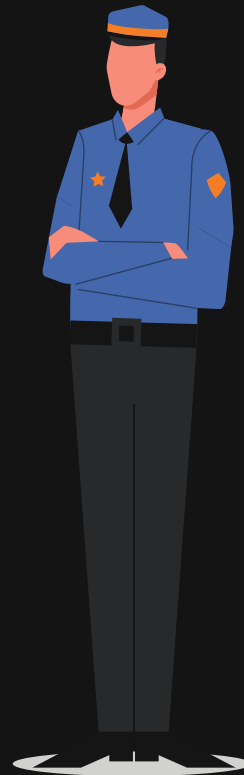

GZIP



Details of protection implementation

More than
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.



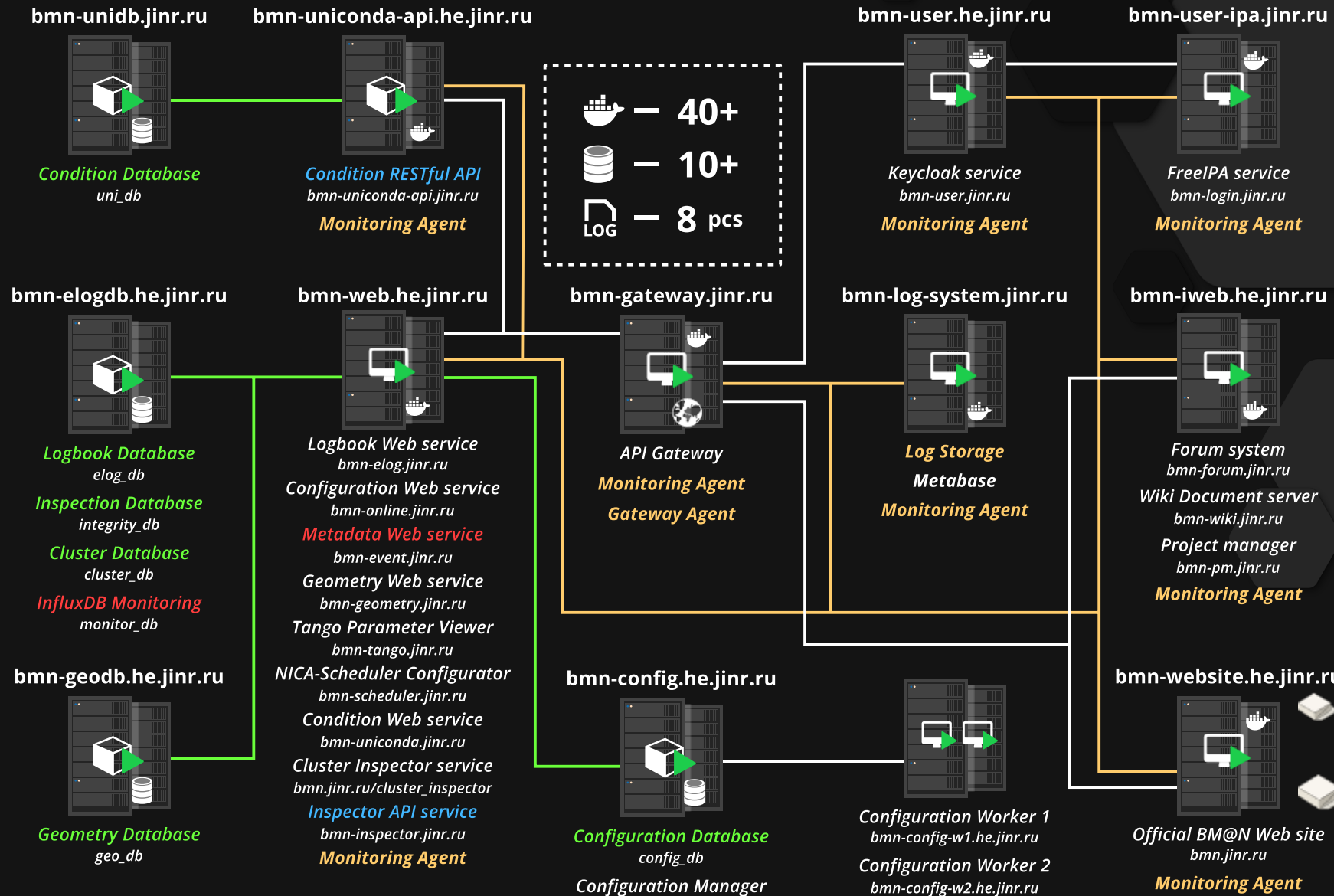
- ❖ Rate Limiting
 - ❖ Authentication Protection
 - ❖ Malicious Bot Detection
 - ❖ Sensitive File Protection
 - ❖ Traffic Filtering
-
- ❖ Optimized performance.
 - ❖ Simplified system management.

Ilya Romanov

Development of Contemporary Log Management Solution for the Information Infrastructure of the BM@N Experiment



Current Infrastructure



Conclusions



- ❖ We have made significant progress in deploying new services, systems, and databases, ensuring a smooth transition to the new infrastructure.
- ❖ The integration of these services with Keycloak strengthens authentication and authorization processes, providing a higher level of security.
- ❖ We are committed to optimizing system performance and ensuring its seamless operation for the BM@N experiment.

Focus on further development

1. New service integration: Expanding functionality with new tools and applications.
2. Enhanced security: Implementing advanced threat detection and prevention systems.
3. Staff training and external courses: It would be great if we were sent to professional courses.

HOLY JS/...



Thank you for your attention!

