Managing automated access:

Experience from Observatorio Astrofísico de Javalambre (OAJ)

Tamara Civera Lorenzo

Scientific Database Engineer [CEFCA/OAJ]

IVOA November 2025

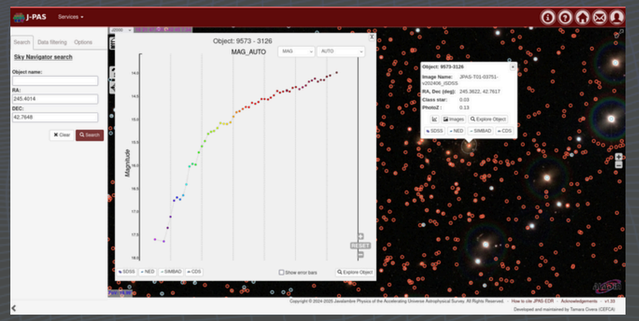
Observatorio Astrofísico de Javalambre

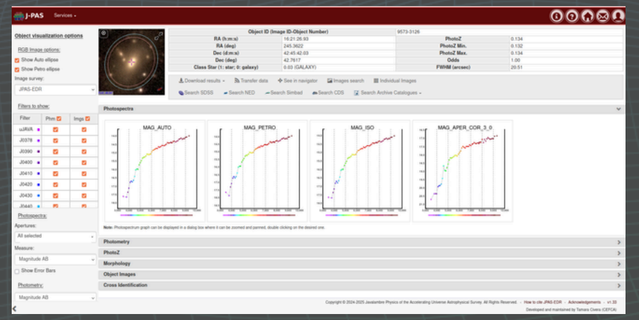
- **Spanish astronomical ICTS** (Unique Science and Technology Infrastructure)
- Located at **Javalambre** mountain range in **Teruel**, Spain
- Managed by **CEFCA** (Center for Studies of Physics of the Cosmos of Aragon]

- Conceived for carrying out **large-scale photometric sky surveys**:
  - J-PLUS and J-PAS
- **~ 20% of observing time allocated** to the broader scientific community:
  - Legacy projects and open time projects

Observatorio Astrofísico de Javalambre

- Provides **access to its data** through the **CEFCA Catalogues Portal**
  - Developed and hosted in CEFCA/OAJ
- Access services:
  - **Web interface services**
  - Virtual Observatory (**VO**) services:
    - TAP, SIAP, SCS, HiPS
- Data access levels:
  - **Public data**:
    - Open to all scientists and general public
  - **Collaborative data**:
    - Restricted to members of each project





https://archive.cefca.es

General Considerations on Automated Access

Large-scale surveys require **working with massive datasets**.

Scientists **increasingly use automated access** to efficiently query and analyze these datasets.

Non-astronomical automated clients (bots, AI tools) can also access these services, especially public datasets.

- AI systems: user queries or independently to train models.

Unexpected load and quality-of-service impacts

Need for protective strategies

OAJ: Benefits of Collaborative Protection

- CEFCA/OAJ benefits from the **protection and support of RedIRIS**, the Spanish academic and research network.
- RedIRIS provides **security and incident response** services for its member institutions.
- This **collaborative approach** represents a collective defense model that complements local service management.

Sinmalos
(“NoMalicious”)

Institutions

- Analyze its traffic, detect IPs with malicious behavior and share them.
- Can directly integrate these **IP reputation lists** into their security systems to block or mitigate malicious traffic.

OAJ: High-Load user experience

"Even with protections, unexpected events occur"

Real experience

- September 2024: some of our **services became very slow** and
  - Certain requests returned 403 error.
- Logs revealed **one IP performing very massive requests**.
- IP belonged to a **university** (it seemed to be a legitimate user].
- We **updated our security policy**:
  - Limit number of requests per second/IP per service
  - Send a friendly message when exceeded

- Days later, the **user contacted us**: we explained the usage limits and how to proceed.

Conclusions

- **Astronomical services** may be accessed by automated clients requiring **thoughtful strategies**.
- Automation **can impact performance**, even for legitimate users.
- **Collaboration** across institutions is key for proactive protection and shared knowledge.
- Proactive monitoring, service-specific rate-limiting, and clear communication help ensure service reliability.
  - Security measures must be tailored to each service.

- Challenges to keep in mind:
  - **Distinguishing** between **attacks, intensive AI usage** and **legitimate users**.
  - Deciding **who to block** while avoiding false positives.

“Finding the right balance between protecting services and supporting legitimate users is key”

Thank you!