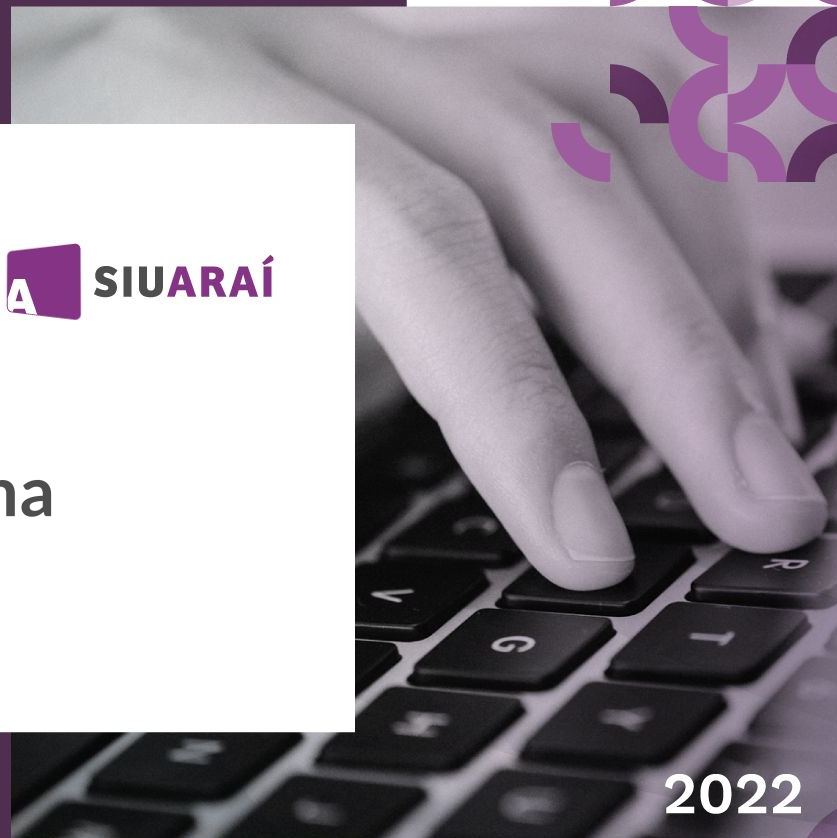




Hacia el control del Ecosistema Administración Digital (EAD)

Guillermo Diorio
Fabio Rosellini

2022

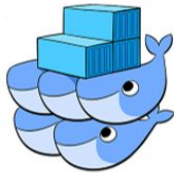
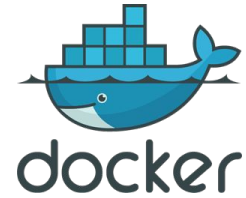
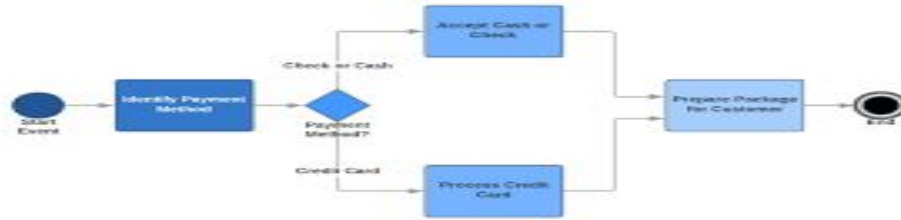


Temario

- ① EAD: Desafíos en el tiempo
- ② Monitoreo y Observabilidad: conceptos y objetivos
- ③ EAD - Mapeo visión conceptual y técnica
- ④ Condiciones necesarias para EAD Obs
- ⑤ Arquitectura de EAD Obs
- ⑥ Arai Monitor: introducción



1. EAD: Desafíos en el tiempo

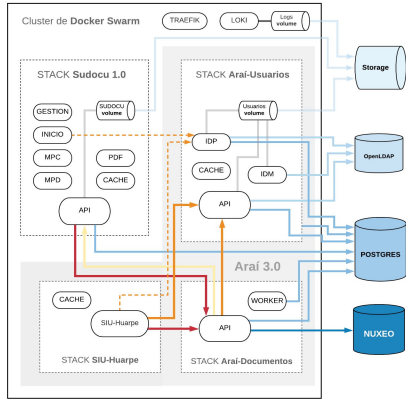


Etapa I -Iniciación



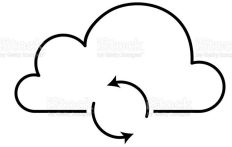
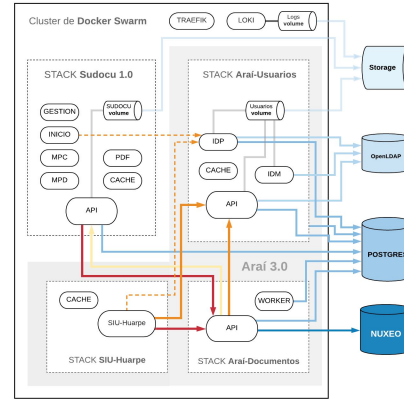
1. EAD: Desafíos en el tiempo

Pre Producción



 **GitLab**

Producción



**BACKUP &
RESTORE**

Etapa II - Puesta en producción



1. EAD: Desafíos en el tiempo



Etapa III - Evolución



tiempo



1. EAD: Desafíos en el tiempo



2. Monitoreo y Observabilidad: conceptos y objetivos

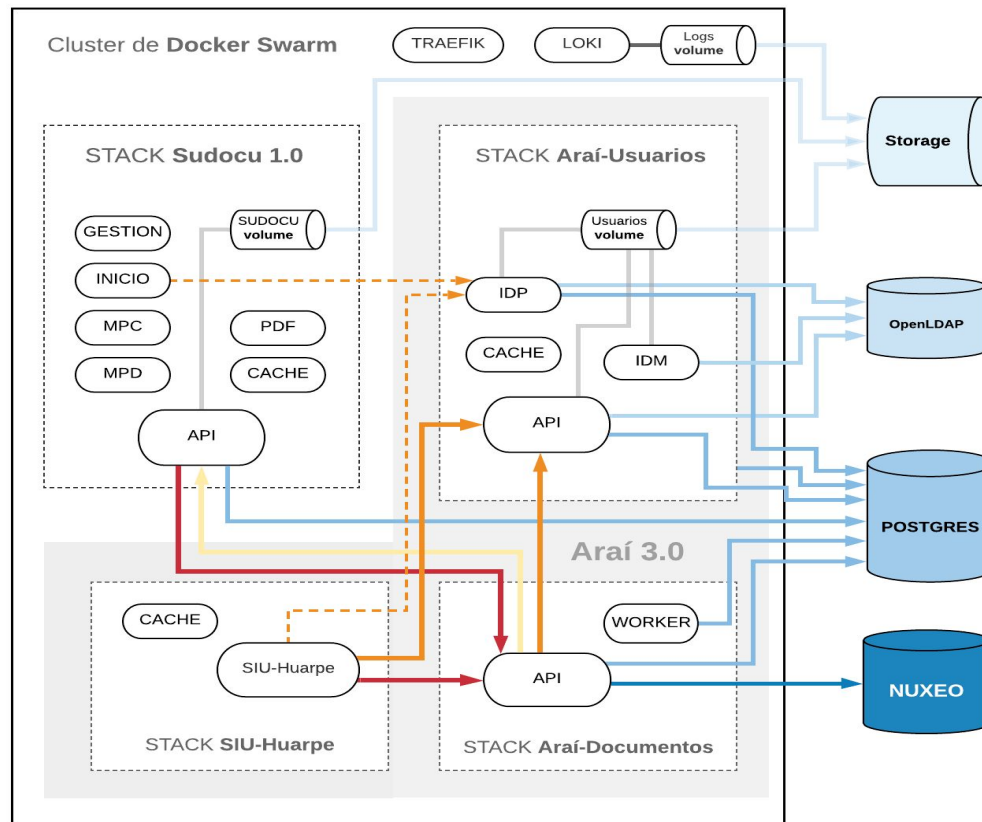
- ✓ **Monitoreo:** determinar la calidad de respuesta de un sistema en base a información externa provista por sus componentes
- ✓ **Observabilidad:** inferir “estado interno” de un sistema complejo en base a salidas externas
- ✓ **Objetivos buscados:**
 - ✓ Tener control de un sistema complejo a lo largo del tiempo ante actualizaciones de versiones, evolución tecnológica, ataques, ...
 - ✓ Disminuir el **MTTI** (investigar) y **MTTR** (resolver)



3. EAD - Mapeo visión conceptual y técnica

SIUPILAGÁ
MÓDULO ECONÓMICO, PRESUPUESTARIO,
FINANCIERO Y CONTABLE

SIUDIAGUITA
MÓDULO DE COMPRAS, CONTRATACIONES
Y PATRIMONIO



4. Condiciones necesarias para EAD Obs

- ✓ Comprensión de mapeo **visión conceptual** y **técnica** de cada componente de **EAD**



- ✓ Identificación de **métricas** disponibles y **logs** generados por cada uno de los componentes de los módulos que son parte de **EAD**, partiendo de la **visión conceptual**
- ✓ Implementación de mecanismo de recolección centralizada de métricas y logs de cada componente según mecanismo de despliegue del componente

4. Condiciones necesarias para EAD Obs

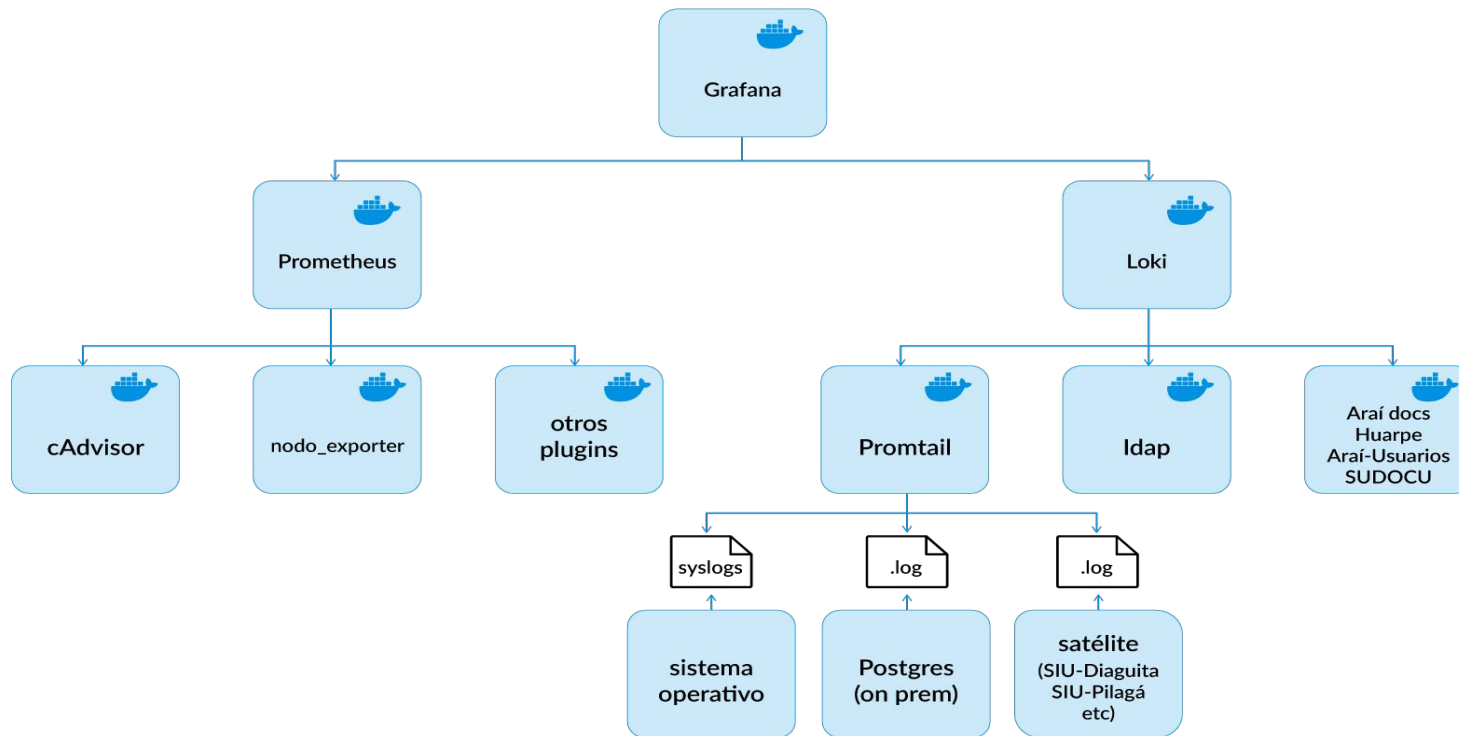
- ✔ Construcción de tableros que representen el **estado** del módulo, consolidando **salud física** (rendimiento de MVs/contenedores y software de base) y **salud funcional** (escaneo de logs para detectar errores)
- ✔ Generación de **alarmas** ante:
 - ✔ Identificación de errores en archivos de log
 - ✔ Métricas fuera de rango de valores aceptables
- ✔ **VENTAJAS DIFERENCIALES:**
 - ✔ Conocimiento detallado de los *circuitos funcionales* (ej: autorización de documentos y su asociación de los mismos a expedientes)
 - ✔ Entendimiento completo del mecanismo de *comunicación asincrónica restHooks* y sus limitaciones

5. Arquitectura EAD Obs

- ✓ Grafana como SPOF (Single Pane Of Glass)
- ✓ Exporters de Prometheus para coleccionar métricas de Sistema Operativo y de componentes de software (*node_exporter*, *postgres_exporter*, *ldap_exporter*, *redis_exporter*, *memcached_exporter*)
- ✓ *Blackbox_exporter* para test de disponibilidad de recursos HTTP
- ✓ Loki para captura de logs de componentes desplegados en contenedores
- ✓ Promtail para capturar logs de instalaciones on-premise

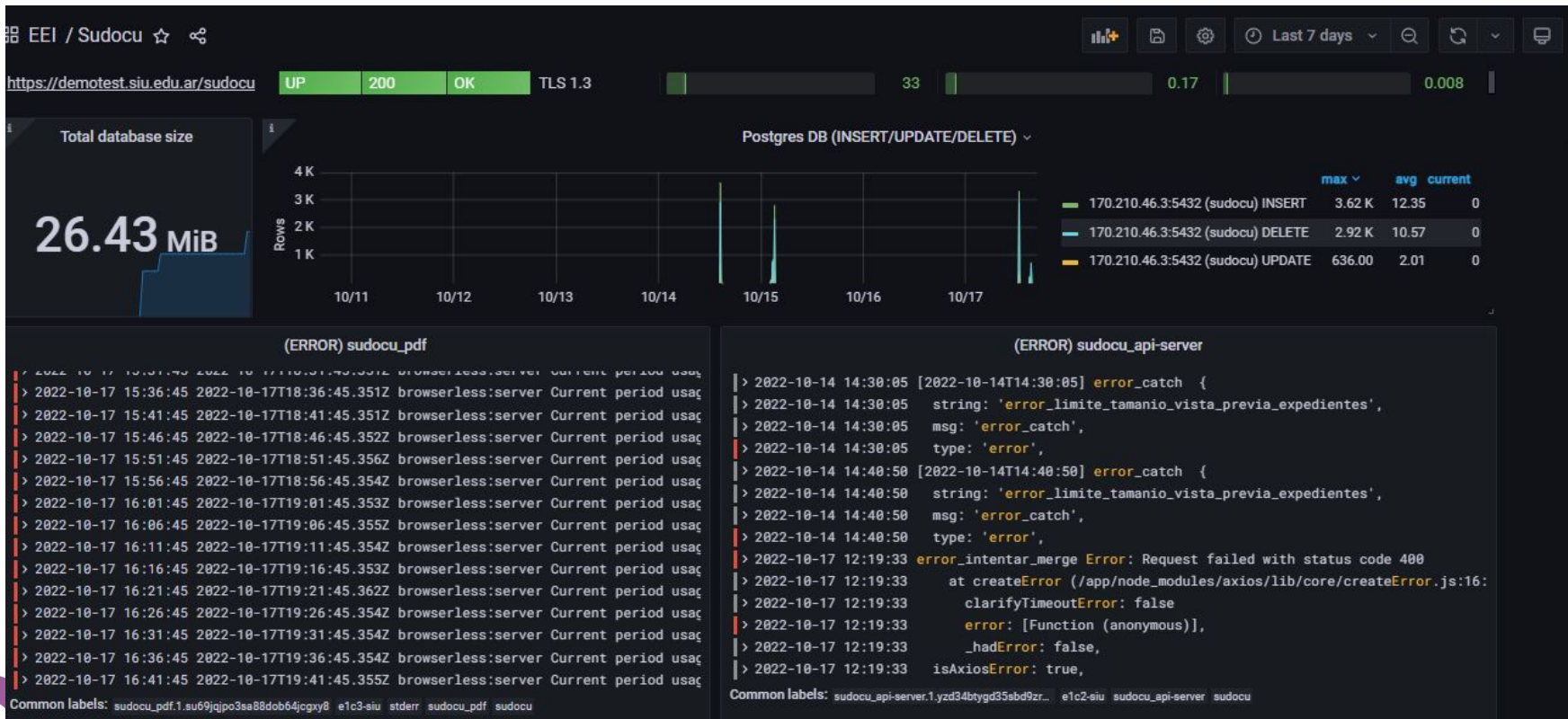


5. Arquitectura EAD Obs



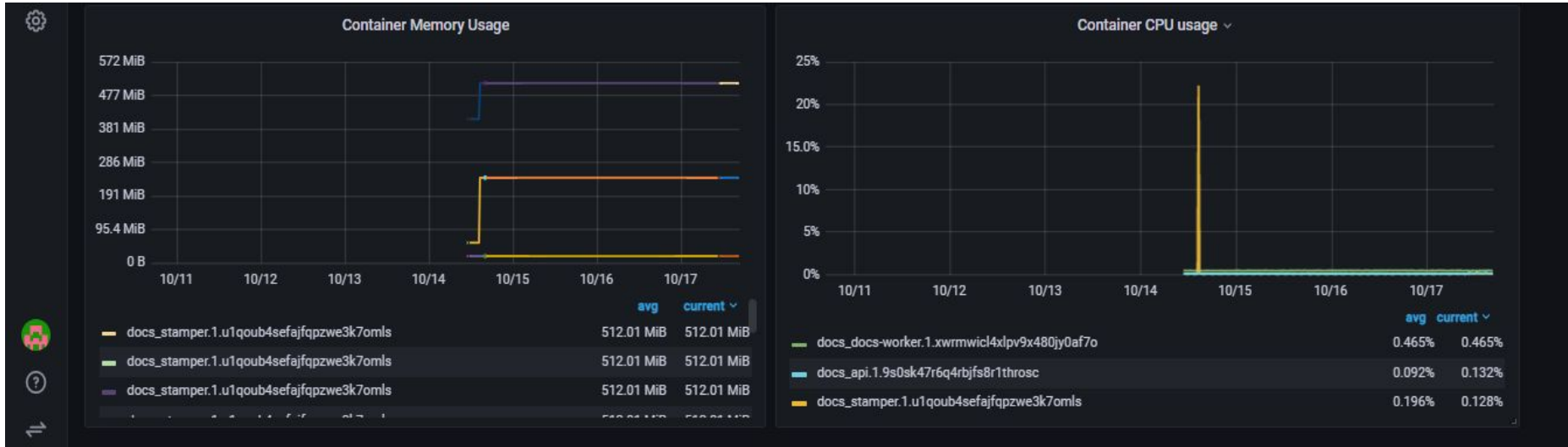
5. Arquitectura EAD Obs

Tablero Sudocu (web disponible, DB postgres y logs API server/PDF)



5. Arquitectura EAD Obs

Tablero Sudocu (métricas contenedor)



5. Arquitectura EAD Obs

Tablero Arai Documentos (HTTP rec. info/web nuxeo, DB y logs API y worker)

The dashboard displays the following components:

- HTTP Probe Overview:** A table showing the status of two probes.
- Total database size:** A card showing 47.06 MiB.
- Postgres DB (INSERT/UPDATE/DELETE):** A bar chart showing database activity over time, with a legend for different operations.
- (ERROR) docs-worker:** A log viewer showing error messages from the docs-worker service.
- (ERROR) Docs Api:** A log viewer showing error messages from the Docs Api service.

Instance	Status	Code	SSL	TLS Version	SSL Cert Expiry (days)	Probe Duration (s)	DNS Lookup Duration (s)
http://e1ap-siu-riu.edu.ar:8180/nuxeo	UP	200				0.15	0.015
https://demotest.siu.edu.ar/docs/re...	UP	200	OK	TLS 1.3	33	0.08	0.005

Operation	max	avg	current
170.210.46.3:5432 (nuxeo) INSERT	160.00	0.32	0
170.210.46.3:5432 (nuxeo) UPDATE	76.00	0.81	0
170.210.46.3:5432 (arai_documentos) UPDATE	52.00	0.05	0
170.210.46.3:5432 (nuxeo) DELETE	16.00	0.02	0


```
(ERROR) docs-worker
> 2022-10-15 02:48:38 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-15 02:48:38 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-15 03:04:37 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-15 03:04:37 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-17 12:25:03 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-17 12:25:03 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-17 12:28:07 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
> 2022-10-17 12:28:07 requests(listener, listener_name, message_id, res
VALUES (:listener, :listener_name, :message_id,
{"listener": "\endpoint": "\http://\api-server:8
```



```
(ERROR) Docs Api
> 2022-10-17 14:49:48 [Mon Oct 17 14:49:48.650198 2022] [php7:notice] [pid 47] [client 10.0.1
> 2022-10-17 14:49:48 [Mon Oct 17 14:49:48.653238 2022] [php7:notice] [pid 47] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.082251 2022] [php7:notice] [pid 24] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.089834 2022] [php7:notice] [pid 24] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.092111 2022] [php7:notice] [pid 24] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.101909 2022] [php7:notice] [pid 24] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.869822 2022] [php7:notice] [pid 25] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.873089 2022] [php7:notice] [pid 25] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.876085 2022] [php7:notice] [pid 25] [client 10.0.1
> 2022-10-17 14:51:13 [Mon Oct 17 14:51:13.878753 2022] [php7:notice] [pid 25] [client 10.0.1
```

5. Arquitectura EAD Obs

Tablero Arai Documentos (logs stamper/nuxeo y métricas contenedor)

The dashboard is divided into four main sections:

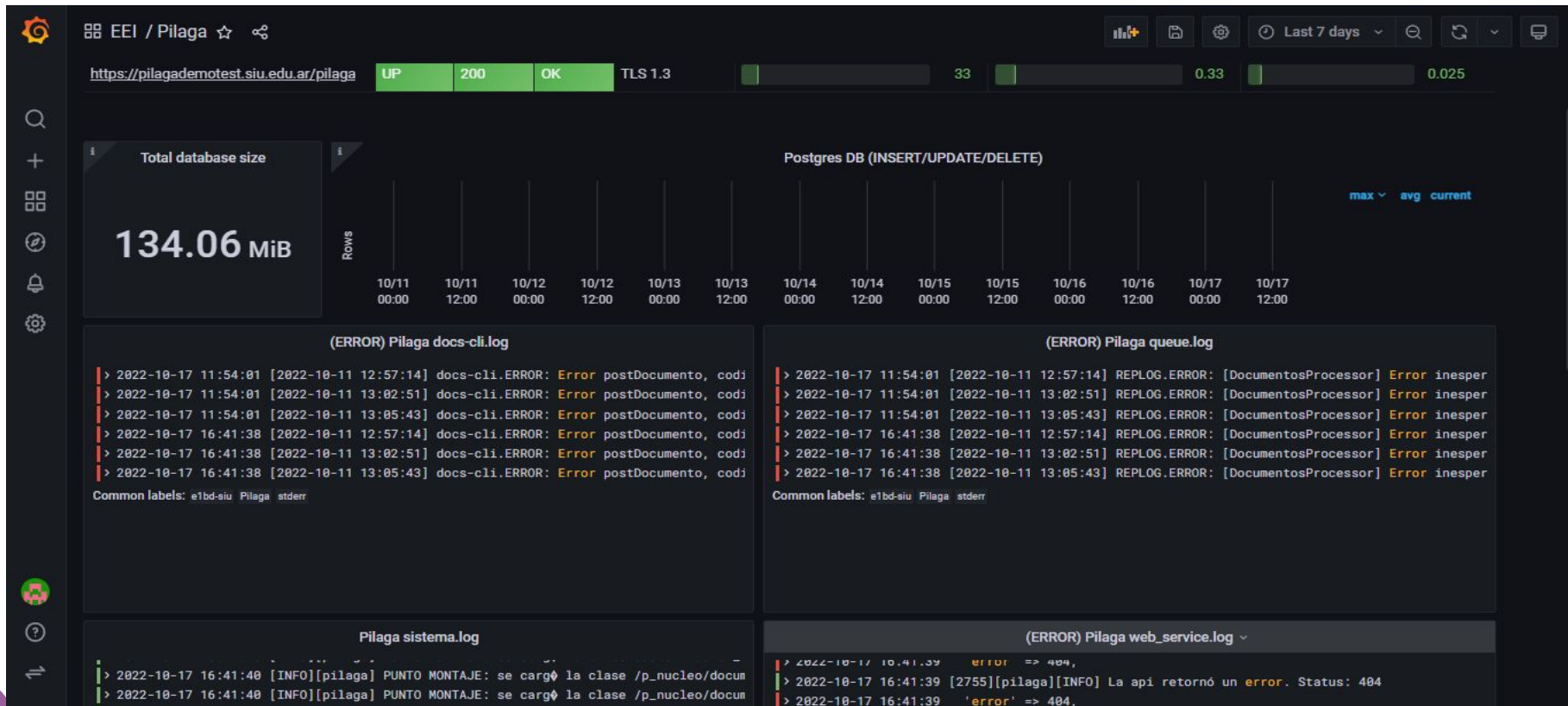
- Logs:** A list of log entries from the 'ErrorReportValve' of 'org.apache.catalina.valves'. The logs show a sequence of events from 2022-10-14 to 2022-10-18. A 'Common labels' section below the logs lists: docs_stamper.1.u1qoub4sefajfpzwe3k7_ e1c3-siu docs_stamper docs.
- Container Memory Usage:** A line chart showing memory usage in MiB from 10/12 to 10/18. The y-axis ranges from 0 B to 572 MiB. Three lines represent different containers, all showing a sharp increase in memory usage starting around 10/14/2022. A table below the chart shows the 'avg' and 'current' memory usage for each container.
- Container CPU usage:** A line chart showing CPU usage percentage from 10/12 to 10/18. The y-axis ranges from 0% to 25%. A single yellow line shows a spike in CPU usage around 10/14/2022. A table below the chart shows the 'avg' and 'current' CPU usage for each container.
- Common labels:** e1ap-siu Nuxeo stdout

Container Name	avg	current
docs_stamper.1.u1qoub4sefajfpzwe3k7omls	512.01 MiB	512.01 MiB
docs_stamper.1.u1qoub4sefajfpzwe3k7omls	512.01 MiB	512.01 MiB
docs_stamper.1.u1qoub4sefajfpzwe3k7omls	512.01 MiB	512.01 MiB

Container Name	avg	current
docs_docs-worker.1.xwrmwic4xlpv9x480jy0af7o	0.465%	0.460%
docs_api.1.9s0sk47r6q4rbjfs8r1throsc	0.107%	0.175%
docs_stamper.1.u1qoub4sefajfpzwe3k7omls	0.180%	0.116%

5. Arquitectura EAD Obs

Tablero Pilagá “satelite” (web disponible, logs docs-cli y queue)



5. Arquitectura EAD Obs

Tablero Pilagá “satélite” (logs comandos/worker y Apache)

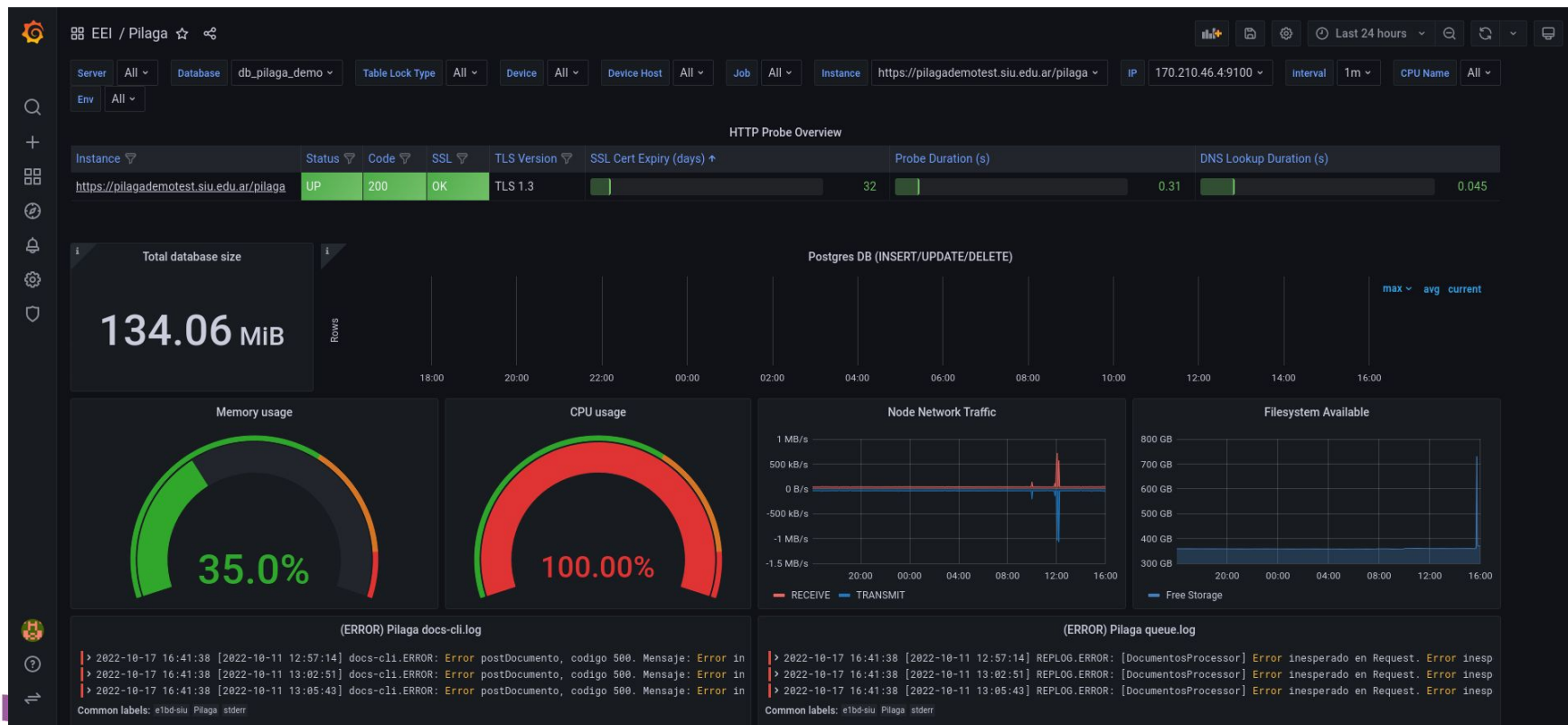
The dashboard displays four log panels:

- (ERROR) Pilaga comandos.log**: Shows a series of error messages from 2022-10-17 20:14:03 to 20:14:10. Each message states: `[ERROR][toba] PROYECTO: El proyecto 'diaguita' es invalido. (1s)`.
- Apache2 error.log**: Shows a mix of error and notice messages. Errors include `[authz_core:error]` and `[php7:error]` from 2022-10-16 16:49:36 to 2022-10-17 08:39:27. Notices include `[mpm_prefork:notice]` and `[core:notice]` from 2022-10-17 00:00:02.
- Pilaga worker-documentos-err.log**: Shows PHP fatal errors from 2022-10-17 16:41:38. The error message is: `PHP Fatal error: Uncaught Dotenv\Exception\InvalidFileException`.
- Pilaga worker-documentos-stdout.log**: Shows timing and error messages from 2022-10-17 16:41:39. It includes `TIEMPO: 3,613 segundos` and `TIEMPO: 0,015 segundos`, followed by the message: `Existe un problema con la base de datos, por favor verifique los logs`.

Common labels: e1bd-siu stderr Pilaga

5. Arquitectura EAD Obs

Tablero Pilagá “satélite” (métricas de MV)



6. Arai Monitor: introducción

Es una **plataforma** que colecta información relevante y personalizada sobre el **estado** (salud) de cada módulo que dicho módulo quiere exponer al **Ecosistema**, trazas, por ejemplo, recolectadas por instrumentación selectiva.

Siendo consistente con **SPOF**, la información colectada se debe ver en **Grafana**.





SIUDIAGUITA 3.3.0 Ambiente Producción Área Dirección de Informática Fecha del Servidor 17/10/2022 admin / Toba: tob


Configuración de SIU-Diaguita

Descripción	Observaciones	Estado	
Dependencias de librerías y versiones requeridas		✓	
Servicio de envío de correos electrónicos		✗	
Servicio de reportes JasperReports para la generación de los PDF		✓	
Servicio Web con la AFIP		✗	
Servicio Web con SIU-Pilaga		✓	
Servicio Web con SIU-Mapuche		✓	
Rest Hooks envíos asincrónicos para web services		✓	
Interoperabilidad con un sistema de expediente externo		✓	
Librería Arai-catalogos de sincronización de catalogos de bienes y servicios		✗	
Arai-proveedores servicio de sincronización de catalogos proveedores		✓	

 [Verificar configuración](#)

 [Historial de actualizaciones](#)

 [Descargar configuración](#)

 [Enviar configuración](#)

6. Arai Monitor: introducción

Objetivo I: tablero de versiones de cada componente/módulo desplegado en instancia de EAD



The screenshot shows a dashboard interface with a dark theme. At the top, there is a navigation bar with a hamburger menu icon, the text 'General / Servicios', a star icon, and a share icon. Below the navigation bar is a search bar and a list of icons (magnifying glass, star, grid, refresh, bell). The main content area is titled 'Servicios del Ecosistema SIU' and contains a table with the following data:

Modulo	Version	Componente	Version	Descripcion
siu/arai/monitor	develop	service:siu/arai/monitor	develop	Plataforma de Servicios del Ecosistema
siu/arai/monitor	develop	api:siu/arai/monitor/v1	1.0	API para tableros
siu/arai/usuarios	v3.1.12	service:siu/arai/usuarios/idp	v3.1.12	Single Sign On
siu/arai/usuarios	v3.1.12	app:siu/arai/usuarios/idm	v3.1.12	IDM de usuarios y aplicaciones
siu/arai/usuarios	v3.1.12	api:siu/arai/usuarios/v1	1.1	API v1 IDM
siu/arai/usuarios	v3.1.12	api:siu/arai/usuarios/v2	2.2	API v2 IDM
siu/arai/documentos	v1.3.3	service:siu/arai/documentos/stamper	v1.3.3	Estampador de PDF
siu/arai/documentos	v1.3.3	app:siu/arai/documentos/worker	v1.3.3	Notificación de novedades
siu/arai/documentos	v1.3.3	api:siu/arai/documentos/v1	1.3	API v1
siu/huarpe	v3.0.3	app:siu/huarpe/	v3.0.3	Portal de Autogestión

6. Arai Monitor: introducción

The screenshot displays the Arai Monitor web interface. At the top, there are two query configuration panels. Each panel includes a 'Type' dropdown set to 'JSON', a 'Parser' dropdown set to 'Default', a 'Source' dropdown set to 'URL', and a 'URL' field containing 'http://via.sii.es/monitor/v1/monitor'. The 'Format' dropdown is set to 'Pretty - Node Graph'. Below these panels are buttons for '+ Add query', 'Query history', and 'Suspension'. The main area is titled 'Mode graph' and shows a directed graph with five nodes and two edges. The nodes are labeled as follows: 'Sistema de Expedientes de E.', 'Sistema de Expedientes de E.', 'Sistema de Expedientes de E.', 'Sistema de Expedientes de E.', and 'Sistema de Expedientes de E.'. The edges represent dependencies between these systems.



6. Arai Monitor: introducción

Limitaciones actuales

- ✗ Solo refleja el estado de la última colección provista por el módulo
- ✗ No soporta series de tiempo

Cómo continuar...

- ✗ incorporar SIEM



- ✗ integrar wazuh con Grafana



