Feature: Identity & Access Management

Feature Overview

Operators need to manage, enforce, and track access for human and machine type users operating on network function workloads and infrastructure resources.

Problem Statement:

The requested feature addresses the following problems in a Nephio context:

(1) Nephio controls resources (e.g. clusters, workloads) according to the configuration as data approach. All the resources are versioned packages. In order to provide fine-grained access control, the package's content shall be examined to check admission to the target resources. Traditional resources as API endpoints are not sufficient to enforce this kind of access control: new mechanisms or the interaction of existing ones shall be introduced.
(2) The traffic clusters' APIs access control is often tied to the 3PP identity and access control for the infrastructure provider (e.g., every possible HCP as Google, Azure, Amazon or proprietary customer infrastructures). Kubernetes can work with a single/federated access control system; a mechanism is required for SSO and accountability.
(3) We need to define human users / application clients of the Nephio system itself, i.e., identity and access control administration and configuration.
(4) Since Nephio executes via controllers, we also need to handle workload identities and access control for these workloads.
(5) For traceability/ accountability, we need to establish the relationship between the user/client identities, the workload identities and any other authentication required to access to the traffic K8S clusters. A mechanism to keep trace of the operations flow is required. E.g., propagation of the authentication token toward the entire path in the system including the user/client request, the access to the involved workloads and remote traffic clusters.

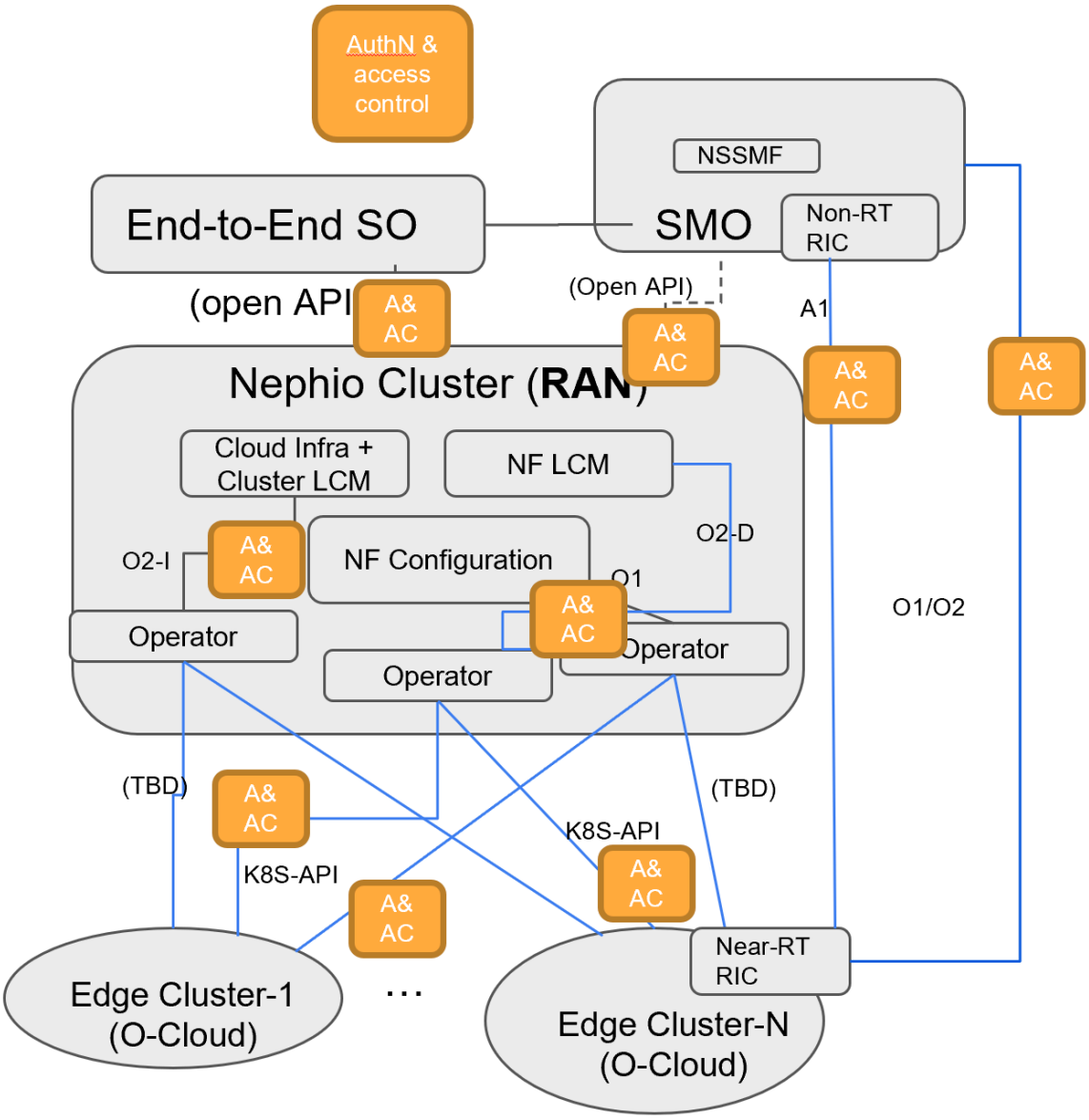


Figure 1: identity & access point in the reference architecture (with SO - SMO - Nehio - Edge examples)

Rationale

This feature is needed for Nephio to fulfill the expected identity and access management capabilities in production environments to protect the integrity of the system from any unauthorized access.

Stakeholders

- Operators, *Integrators, Vendors (of management solutions)*
- Personas (All)

Design and architectural considerations

- Feature implementation can be staged, starting with user/client identity and access.
- Define the mandatory, optional and external components/functions in the solution, with well-defined integration points for optional components and external services.
- Solution must be flexible enough to enable various access control schemes e.g., resource type (network function, infrastructure etc.), network function type, area/region, organization or tenant based, etc.

Prerequisites

- TBD

Requirements

Core functional requirements

REQ 1. The Nephio security mechanism shall support the Authentication for human users with configurable MFA, clients M2M, workloads and any resource with an identity, based on standard/open-source OIDC and/or SPIFFE.

- Provide compatibility with potential external IdP that is already available in the customer's solution.

Note: Kubernetes supports basic authentication, which is not recommended for production environments due to security concerns. In Nephio, OIDC and SPIFFE provider(s) will be integrated with Kubernetes to use credentials with the OIDC provider(s), and Kubernetes verifies the identity based on tokens (OIDC, SPIFFE) issued by the providers.

Requirement	Description	Priority

REQ 1.1	OIDC client credential flow shall be supported for machine to machine authentication with a secret as credential	Mandatory
REQ 1.2	OIDC client credential flow shall be supported for machine to machine authentication with a X509 certificate as credential	Mandatory
REQ 1.3	OIDC authorization code flow shall be supported for human user authentication with a password as credential	Mandatory
REQ 1.4	OIDC authorization code flow shall be supported for human user authentication with configured Multi-factor authentication (OTP or biometric)	Mandatory

REQ 2. The Nephio security components shall support the flexible Authorization based on OIDC/OAuth2; i.e., support for RBAC, TBAC and/or ABAC.

Note: ABAC allows to define access control policies based on attributes associated with users or groups. While RBAC is more commonly used, ABAC can be an option for more granular control over access.

Requirement	Description	Priority
REQ 2.1	OIDC authorization via UMA (user managed access) 2.0 flow	Mandatory
REQ 2.2	Roles shall be defined to give access permission to the system resources. Resources could be endpoints, workload identities	Mandatory

REQ 2.3	Target based access control shall be supported	Good to have
REQ 2.4	ABAC support. The authorization to perform a set of operations could be determined by evaluating attributes associated with the subject, object, requested operations. In Nephio context, the attributes could be contained in the data of the Porch packages	Good to have

REQ 3. For User/Client Identity and Access Control Administration and Configuration, thru the Nephio security mechanisms, the Nephio/operator admin shall be able to set up the followings for user/client Identity, access control administration and configuration:

Requirement	Description	Priority
REQ 3.1	User/client password policies configuration shall be supported	Mandatory
REQ 3.2	Support for Security defenses: timer for session, lock and disable users	Mandatory
REQ 3.3	User/client creation, update, and deletion shall be supported	Mandatory
REQ 3.4	Support for Role/permissions/policies/ attributes creation and deletion for fine-grained access control OIDC token claim manipulation	Mandatory
REQ 3.5	Support for Security logging configuration	Mandatory
REQ 3.6	Support for External IDP and user federation via LDAP	Mandatory

Note1: use of an IdAM embedded IdP is allowed, but IdP extension points shall be considered.

Note 2: A list of Nephio role type (for infrastructure, workload) examples is listed, and additional roles can be configured at the target IdAMs (e.g., management cluster, workload cluster) by operators, as needed.

- Infrastructure management and integration
- Creating base packages
- Customizing/hydrating the packages
- Deploying the package across a set of clusters

REQ 4. For Identity and Access Control Federation of Management and Workload clusters, the Nephio/operator admin shall be able to enable, configure and federate the Management and workload cluster IdAMs to support access controls between the management cluster and workload clusters

- Note: this requirement could be optional if there is no use case for multiple IdAMs across clusters.

Requirement	Description	Priority
REQ 4.1	Shall support user/client identities, groups, roles and permission across Kubernetes clusters by IdAM federation (between Nephio Management cluster IdAM and workload IdAMs) and/or centralization	Optional
REQ 4.2	Shall support users/services authentication from a Nephio cluster to be authenticated by security mechanisms, 1) within the same cluster and/or 2) at another Nephio cluster (e.g., by federation)	Optional
REQ 4.3	Shall support mapping an authenticated user's/service's role (passed through a token) for accessing workload resources	Optional

	between the source cluster and the target cluster	

Note 1: IdAM shall act as a federated identity provider with credentials from IdP.

Note 2: For workload access control, SPIFFE-based infrastructure shall/can be integrated with the federated identity providers, enabling authentication and identity federation across clusters - see REQ 5.

REQ 5. For Nephio Workload Access Control, the Nephio security mechanisms shall be able to support the workload identity and access control administration and configuration to secure Nephio workloads

- Note this requirement is fulfilled by the Workload Identity requirement,

  Workload identity user story - https://docs.google.com/document/d/1nkh7tTltwii1bY877PfzjFCBtmRos4IDh5EOJxWXRdg/edit?usp=sharing
  Workload identity design document - https://docs.google.com/document/d/1k8Hcd7tJKPIsyiYZX6hpRECuJ4IIxVnaESghU5bLNVQ/edit?usp=sharing

REQ 6. For Nephio Logging Support, the Nephio security mechanisms shall provide security log data to support logging of successful and unsuccessful access attempts (optional with low priority)

Note: Logging data collection, aggregation, persistence and visualization shall/can be handled by external open-source/3pp log-handling stacks.

REQ 7. For Nephio Auditability, Traceability and Accountability, the Nephio security mechanisms shall provide data for Auditability, traceability, and accountability (optional with low priority)

- Data related activity shall be tracked, recorded, throughout its lifecycle including the identity of individuals and applications responsible for the data-related actions.
- Monitor clusters to ensure workloads are using the correct service accounts and verify that workload identity policies are being followed (e.g., Kubernetes audit logs, or equivalent)

Non-functional Requirements (scale, additional security, deployment constraints)

- Documentation (Security Overview, Admin Guides, Integration Guides etc.)
- Package authoring design rules (to enable access control functions)
- Example policy rules

Acceptance criteria (Definition of done)

- Reference Solution for identity and access management (admin, control, logging)
- Test reports verifying identity and access management functional requirements.
- Documentation

Priority

- Introduce the management cluster IdAM - Priority 1
- Define workload identities, federation and access control; shall be part of Service Mesh - Priority 1
- Audit and Tracing - Priority 2

Areas to consider (work in progress)

- Asynchronous operation identity and access control.

What's not in scope.

- Other security concerns (certificate management, data encryption, secret management, service mesh etc.)

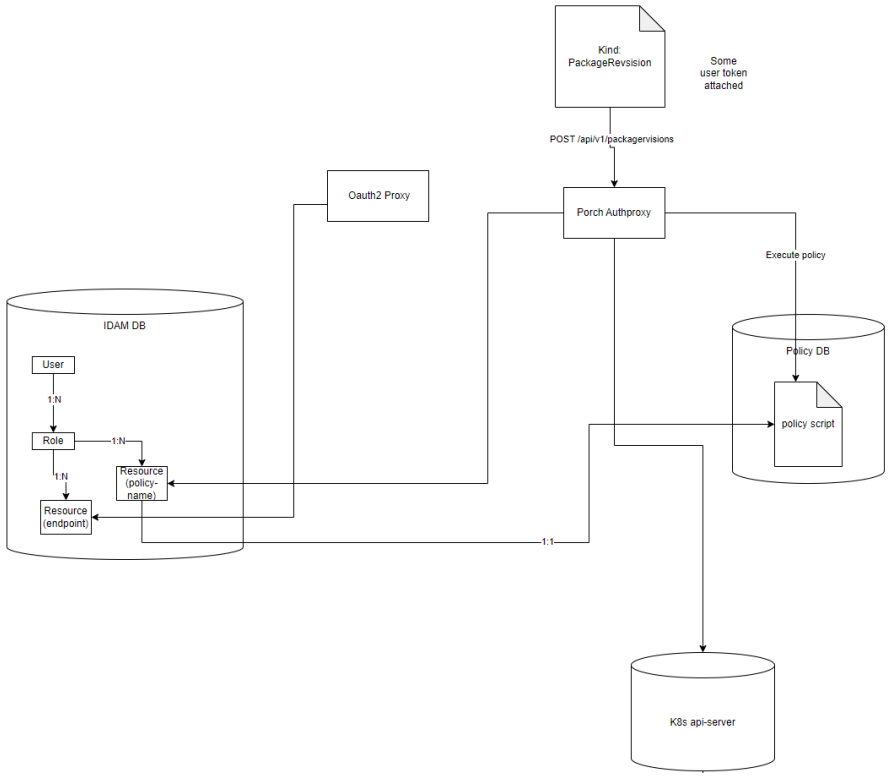
References

- https://tetrate.io/blog/why-would-you-need-spire-for-authentication-with-istio/
- https://istio.io/latest/docs/ops/integrations/spire/

Component Architecture

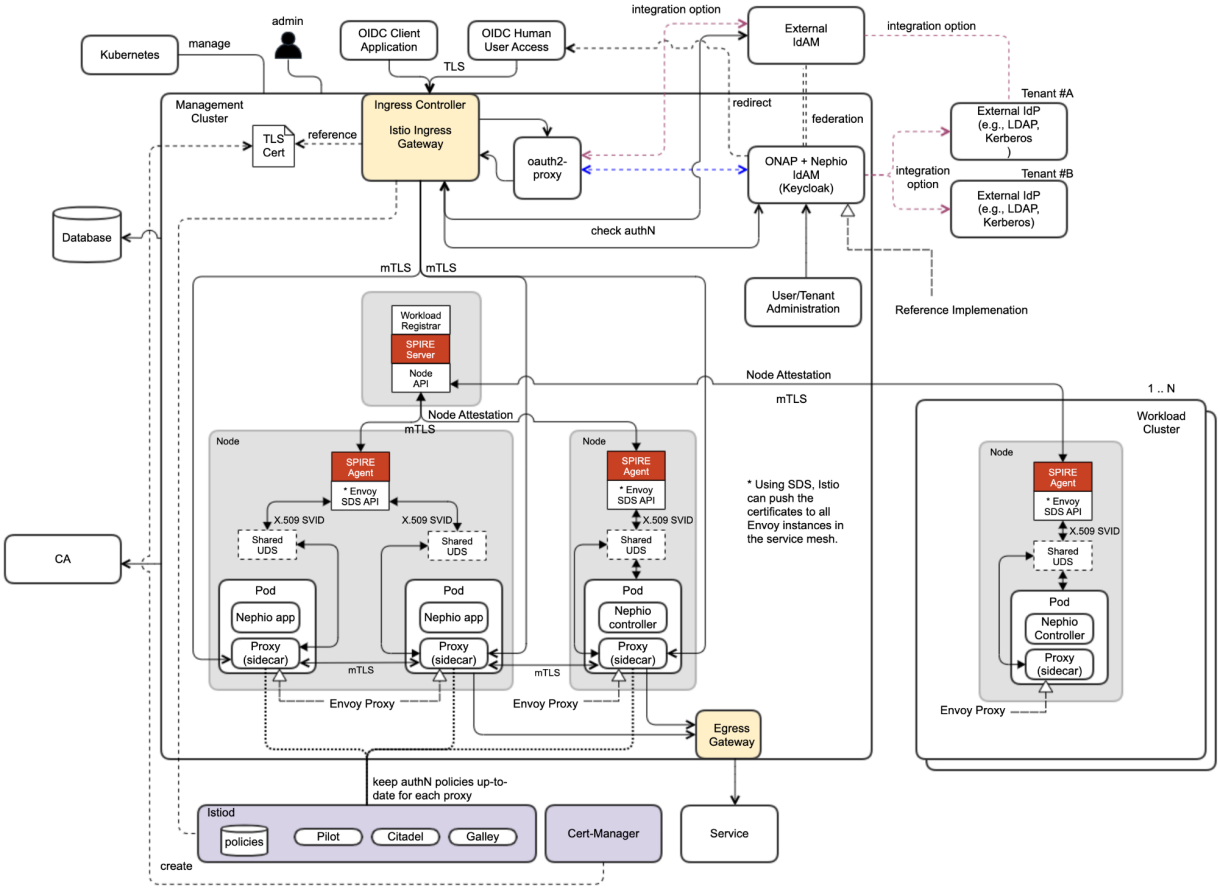
- Users/roles defined in IdAM service.

- ‘Porch Authproxy’ evaluates user authority to make a package revision based on an assigned role.



- ## Reference Architecture

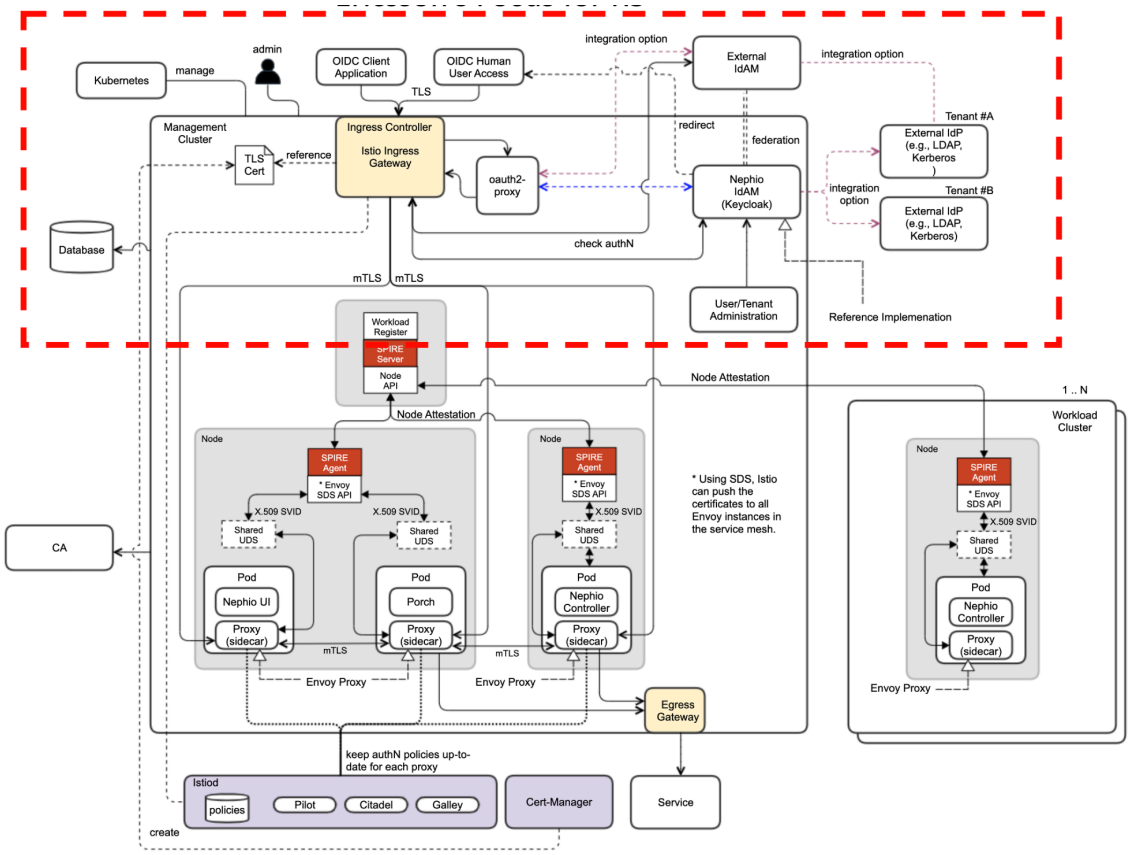
  The following diagram depicts a reference architecture for OIDC/OAuth2-based authentication and authorization.



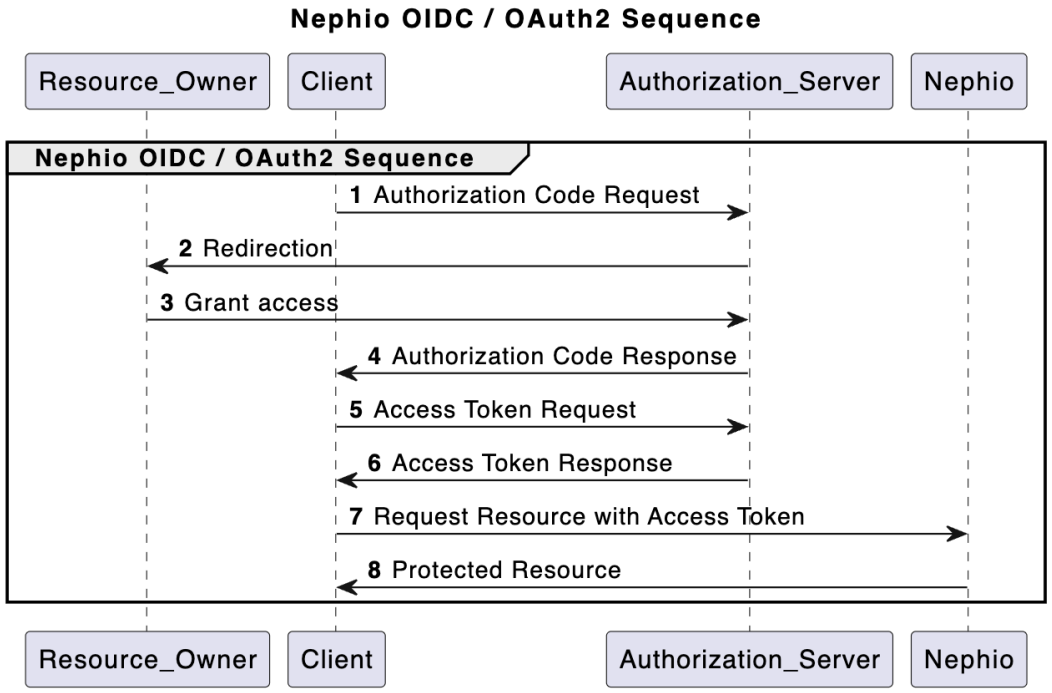
Note: the above also describes the connection between Istio Service Mesh and SPIFFE infrastructure for the node and workload attestation, and workload registration, see https://docs.google.com/presentation/d/1L79WrZ64Uar3IrH-jL_IeQTlPoLtXGZKHIIfVCXLoco/edit#slide=id.g2c18d699447_0_40 (Shiv and team)

- ## REQ 1 - 5 Focus

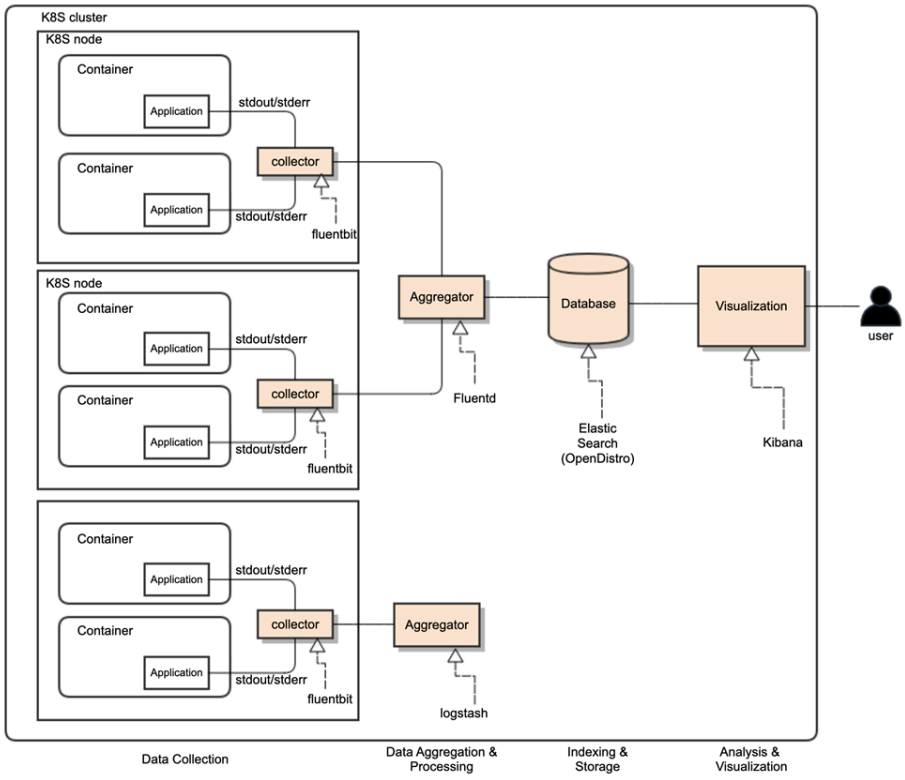
  The following diagram depicts the REQ 1 - 4 focus:



OIDC / OAuth2 Sequence Flow



- **Component Logging Architecture**
  - Allowing the logging component stack (such as collector, aggregator, persistent and visualization components) is realized by choices of vendors.
  - Nephio components are responsible for generating log data thru STDOUT / STDERR



Needed software development.

- Policy Evaluation Controller, etc.

API design

- External integration points (e.g., for OIDC flows)

E2E test environment

- IdAM service (e.g., KeyCloak), Policy Engine (e.g., OPA/Gatekeeper)

Appendix: Zero Trust Architecture