What is the issue legacy authorization on clusters enabled in GCP?  
As of my last knowledge update in September 2021, Google Cloud Platform (GCP) uses Identity and Access Management (IAM) for authorization, which provides a robust and flexible way to manage permissions and access control. Legacy authorization refers to the older, less secure method of controlling access in GCP, which was based on Identity-Aware Proxy (IAP) and Google Cloud Identity (GCI).

The issue with legacy authorization on clusters enabled in GCP is that it is less secure and less flexible compared to IAM-based access control. Legacy authorization relies on a combination of GCI and IAP, which were designed for older GCP services and may not provide the same level of granularity and control as IAM.

Some of the issues with legacy authorization include:

1. Limited Control: Legacy authorization may not allow for fine-grained control over permissions and access to GCP resources, making it harder to implement the principle of least privilege.

2. Complexity: Legacy authorization can be more complex to set up and manage compared to IAM, which has a more straightforward and centralized approach to access control.

3. Security Risks: Because legacy authorization is less robust, it may pose security risks, especially in environments where strong access controls are necessary.

4. Compatibility: As GCP services evolve, legacy authorization may become less compatible with new features and services, potentially leading to compatibility issues or limitations in using certain GCP resources.

5. Deprecation: Google has been encouraging users to migrate from legacy authorization to IAM for several years. They have deprecated some legacy authorization features, and it's possible that support for it may be phased out entirely in the future.

To address these issues, it's generally recommended to migrate from legacy authorization to IAM-based access control in GCP. IAM provides a more modern and secure way to manage permissions and access to GCP resources. The process of migrating from legacy authorization to IAM involves creating roles, assigning permissions, and configuring access controls using IAM policies for your GCP resources.

Please note that the state of GCP services and features may have evolved since my last update in September 2021, so it's important to check the most recent GCP documentation and consult with GCP support or a GCP expert for the latest guidance on authorization and access control.