Metadata storage

Container Analysis provides vulnerability scanning and metadata storage for containers. This page describes metadata storage and retrieval.

A high-level piece of metadata, such as a vulnerability or build information, is called a **note**. Each instance of a note is identified as an **occurrence**.

A **provider** is a company that creates the metadata stored in notes. A **customer** can then use Container Analysis to identify occurrences of notes, such as vulnerabilities found in containers stored in the project.

Note

A note (/container-registry/docs/reference/rest/v1/projects.notes) describes a high-level piece of metadata. For example, you could create a note about a particular vulnerability after analyzing a Linux package. You would also use a note to store information about the builder of a build process. Notes are often owned and created by the providers performing the analysis. Customers that want to use the metadata can then identify occurrences of notes within their projects.

We recommend that you store notes and occurrences in separate projects, allowing for more fine-grained access control.

Notes must be editable only by the note owner, and read-only for customers who have access to occurrences referencing them.

Occurrence

An occurrence (/container-registry/docs/reference/rest/v1/projects.occurrences) represents when a note was found on an image; it can be thought of as an instantiation of a note. For example, an occurrence of a note about a vulnerability would describe the package that the vulnerability was found in, specific remediation steps, and so on. Alternatively, an occurrence of a note about build details would describe the container images that resulted from a build.

Typically, occurrences are stored in separate projects than those where notes are created. Write access to occurrences should only be granted to users who have access to link a note to the occurrence. Any user can have read access to occurrences.

Discovery occurrences include information collected from the initial scan of container images. As it scans containers, Container Analysis updates discovery occurrences to record scan status. Discovery occurrences are created for all existing images when the Container Analysis API is first activated, and then for all new images pushed to Container Registry.

Supported metadata types

The following table lists the metadata types (/container-registry/docs/reference/rest/v1/NoteKind) Container Analysis supports and provides for images in Container Registry as notes. Third-party metadata providers can store and retrieve all of the following metadata types for their customers' images.

Metadata type	Provided by Container Analysis for Container Registry images
Vulnerability, which provides vulnerability information for container images.	Yes. Container Analysis obtains the vulnerability information from external sources (#vulnerability_source).
Build, which provides information on build provenance.	Yes. Container Analysis provides this information only if you use Cloud Build to build the image.
Deployment, which provides information on image deployment events.	No
Image, which is the metadata about the container image, for example, information about the different layers of an image.	No
Package, which contains information about the packages installed in your image.	No
Attestation, which is the logical role that can attest to the images.	No
Discovery, contains information about the initial scan of images.	Yes. Container Analysis provides this information only for vulnerabilities.

Providers and customers

Providers are the companies that provide metadata for their customers' images. Providers can use Container Analysis to store and retrieve metadata for their customers' images. For example, a company that provides security management for their customers' Docker containers can use Container Analysis to store and retrieve security-related metadata for the images. For more information see Providing metadata for Projects (/container-registry/docs/provide-metadata-for-projects).

Customers use the metadata provided either by Google for the images in Container Registry or by third-party providers.

What's next

- Provide metadata (/container-registry/docs/provide-metadata-for-projects) for your images.
- Learn more about vulnerability scanning (/container-registry/docs/vulnerability-scanning).

Last updated 2020-06-26 UTC.