Registry Scanning

This feature requires either a Wiz Standard or a Wiz/Gov Advanced license. Learn more.

Wiz can scan container images in registries you connect with container registry Connectors.

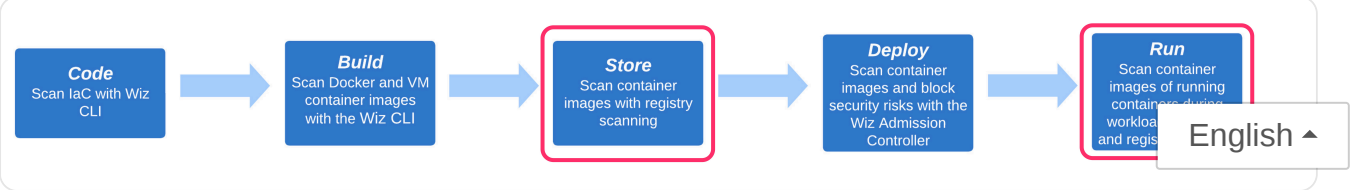
Container registries are centralized repositories for storing and managing container images, and they include all the code, runtime, libraries, and dependencies necessary to run an application. See supported registries and services.

Scanning your container registries with Wiz provides the following benefits:

- Detecting vulnerabilities and malware in container images early in the development lifecycle and before they are deployed to production, as well as in third-party container images that are pushed to your registry but don't go through the CI/CD pipeline
- Detecting new vulnerabilities and/or malware in container images that have been scanned in the CI/CD pipeline but are in use for extended periods of time
- Extending your scanning coverage to include all deployed container images running in your environment. This is especially important when Wiz does not have access to container hosts' underlying disks (e.g. ECS on Fargate or on-prem Kubernetes/OpenShift clusters), meaning they cannot be scanned via runtime (disk-based) workload scanning
- Developers and security teams gain end-to-end visibility into container images throughout the lifecycle (from the initial code phase to runtime)

How it works

Registry scanning encompasses scanning registries just before deployment and active (deployed) container images not covered by workload scanning in runtime.



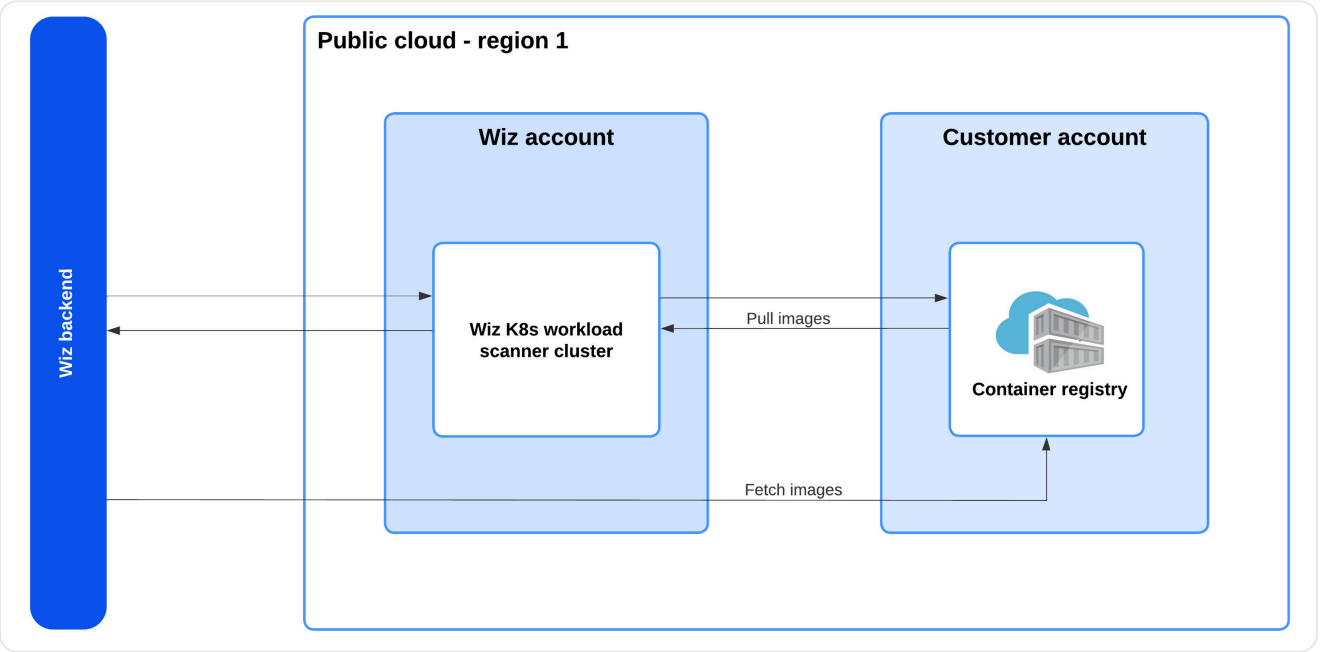
Installation types

- With internet access:
  - Registries with full internet access
    - Standard
    - Outpost
  - Registries with limited internet access
- Without internet access:
  - Private registries with no internet access

Registries with full internet access

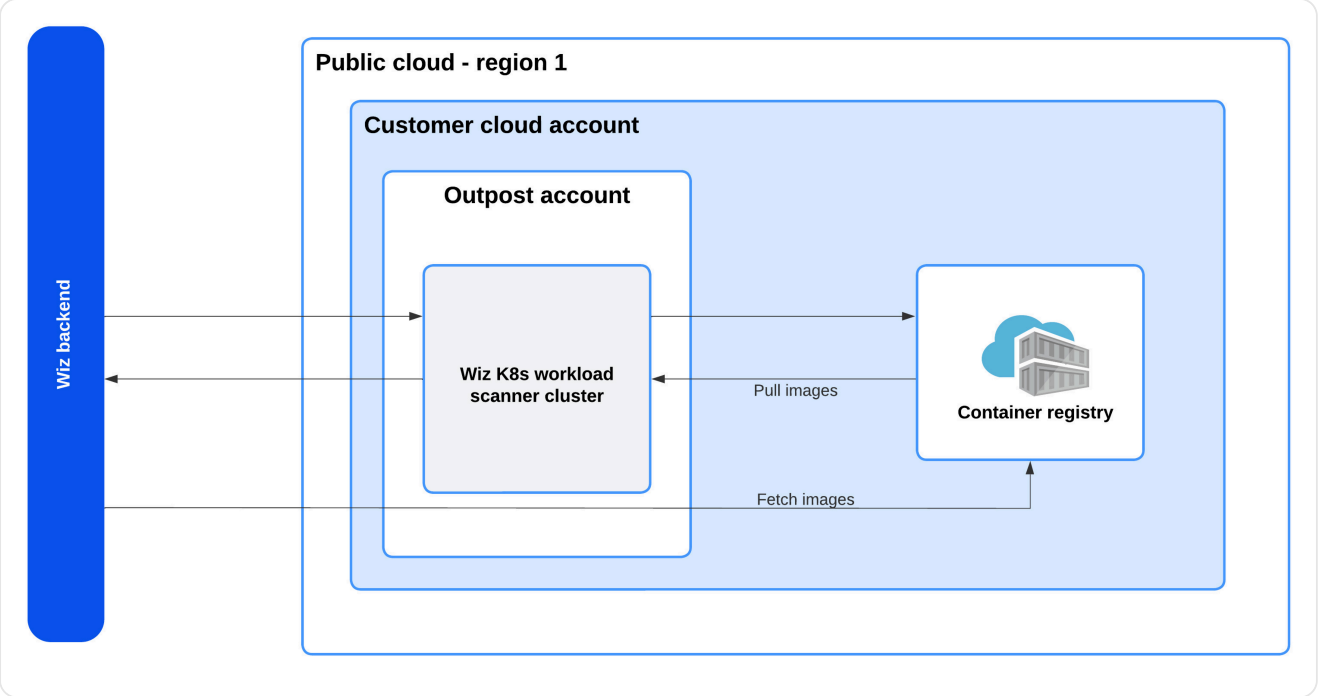
Standard

The standard installation for SaaS Deployments allows you to quickly create a new container registry Connector.



Outpost

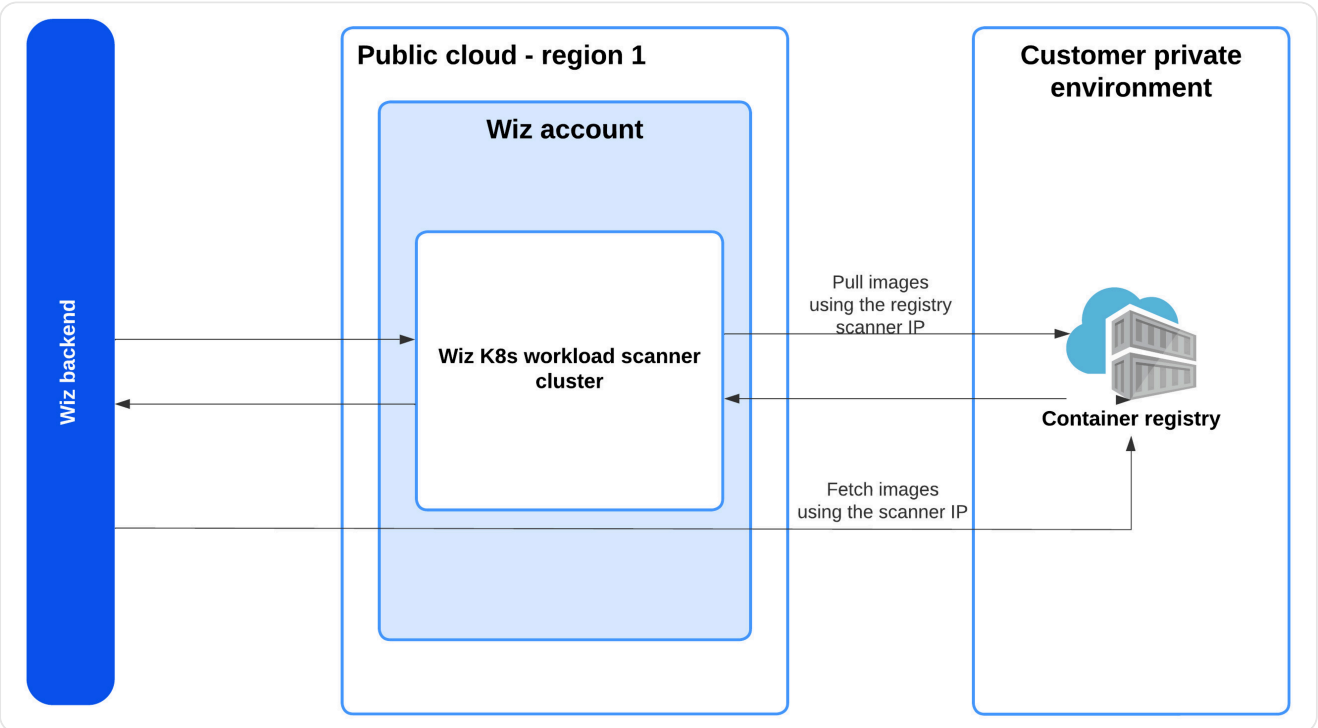
This installation is for those who want registry scanning to occur within their environment.



Registries with limited internet access

This installation is for scanning private registries, whether on-prem or in a cloud, with limited internet access. It
requires you to add the Cloud scanner IP and registry scanner IP addresses relevant to your data center to your registry's whitelist (allow list) prior to creating the container registry Connector.

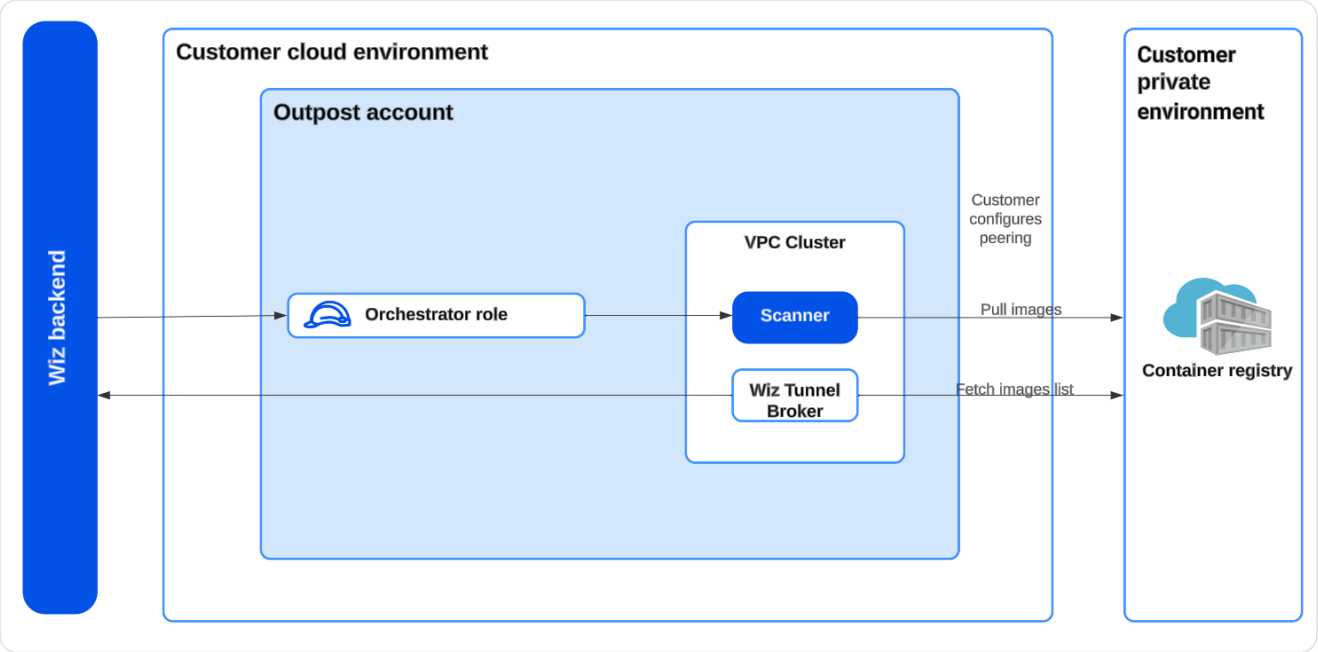
> ⚠ Wiz Outpost is not supported for this installation type.



Private registries with no internet access

This installation is for scanning private registries, whether on-prem or in a cloud, with no access to the internet. It requires a Wiz Outpost with a self-managed network. Once you establish a Virtual Private Cloud (VPC) in your Outpost account and connect it to your private registry, Wiz installs a Wiz Broker in your Outpost account. The Wiz Broker connects the Wiz backend with the registry API in order to fetch container images from your private registry.

> Since deploying a Wiz Outpost with a self-managed network requires assistance, contact your Wiz representative.



Scanning modes

When connecting your registry, you can select between two registry scanning modes. You can also change the scanning mode of an existing registry Connector. Available modes:

- Scan all container images, both deployed images running in your environment and non-deployed images that are stored in your registry.
- Scan only deployed container images running in your environment that cannot be scanned via agentless workload scanning since Wiz does not have access to their underlying hosts (e.g., ECS and EKS on Fargate or on-prem Kubernetes/OpenShift clusters).

Changing the scanning mode

To change a registry Connector's scanning mode, navigate to Settings > Deployments. From the row of the Connector, click ⋮ More Options > Scanning mode.

- If you change the scanning mode to Deployed Images Only, during the next Wiz scan, resources that were created by scanning your entire registry will be

- If you change the scanning mode to All Images Wiz sets default scan setting:
  - Scan interval = weekly
  - Maximum number of versions per image to scan in each repository = 5

> Changing the scanning mode to All Images may impact your billable workload count, since Wiz will be scanning additional images stored in the registry. For details, navigate to ⚙ Settings > Licenses.

To edit scan settings, navigate to Settings > Deployments. From the row of the Connector, click ⋮ More Options > Edit.

Auto-connect cloud-based registries

Wiz discovers cloud-based registries in your environment and automatically connects to them using the existing cloud connector role. Currently, Wiz can auto-connect to ECR, GCR and GAR registries. Support for ACR will follow.

Auto-connected registries appear on the Inventory > Container Registries Page. Filter by Connector Type = Automatic.

> For Wiz to auto-connect to your ECR/GCR/GAR registries, you must have a configured AWS/GCP cloud Connector.
>
> GAR registries require a newly added permission to the GCP role: `artifactregistry.repositories.downloadArtifacts` . To update permissions, follow GCP Permissions guide.

A newly connected registry is automatically assigned the Deployed Images Only scanning mode. You cannot edit the scanning mode of an auto-connected registry.

Customers using Outpost

If your AWS/GCP cloud Connector is connected via Outpost, all discovered cloud-based registries will connect via the same Outpost.

Scan results

Registry scan results can be viewed on the Security Graph, the Findings > Vulnerability Findings Page, and the Inventory.

> By default, registry scanning results are assigned all the Projects under the Subscription they belong to. As for on-prem registries without any associated cloud Subscription, you can manually map them to Projects;

> that way you can see the results of a registry scanning depending on the Projects to which you have access to.

Vulnerability Findings page

All Vulnerability Findings relating to container images appear on the Vulnerability Findings page and vulnerability reports.

- For example, see all Vulnerability Findings whose resource type is a container image and were generated following an All Images scan
- For example, see all Vulnerability Findings whose resource type is a container image and were generated following deployed image scanning or workload scanning

Security Graph

Container images that appear on the Security Graph are automatically correlated with other risk factors (such as network exposure, misconfigurations, and excessive permissions).

Inventory

Details related to container images scanned in All Images mode are listed on the Inventory > Registry Container Images page.

Supported registry artifacts

Wiz supports the scanning of container images in Docker and OCI formats. Scanning of all other artifacts in the registry, such as Helm charts, RPM packages, and Maven packages, is not supported.

Supported container registries & services

Supported registries

The following registries are compatible with Docker V2 API and can be scanned with our container registry Connectors:

Supported registries & services	Required Connector
ACR	Generic container registry Connector

Supported registries & services	Required Connector
Docker Hub	Docker Hub Container Registry Connector
ECR	Auto-connect, Amazon Elastic Container Registry (ECR) Connector
GAR	Auto-connect
GCR	Auto-connect
Harbor	Generic container registry Connector
JFrog Artifactory	JFrog Artifactory Container Registry Connector
Sonatype Nexus	Generic Container Registry Connector

Supported services

The registry Scanner can scan deployed images running on the services listed below, which cannot be scanned via runtime (snapshot-based) workload scanning.

If the container image running on the supported services originates from ECR/GCR/GAR, Wiz will automatically connect to the registry and scan the container image. If the container image originates from a different, private registry (such as: JFrog Artifactory, private repository in Docker hub), you must create a dedicated registry Connector for Wiz to scan the images.

- ACA
- ACI
- Cloudrun
- ECS on Fargate*
- EKS on Fargate
- GKE Autopilot
- On-prem Kubernetes clusters
- OpenShift clusters
- SageMaker Domain

*If the container images running on ECS on Fargate originate from ECR, Wiz will automatically connect and scan the images (without a dedicated ECR connector). If the container images originate from a different, private registry, you must create a dedicated registry Connector for Wiz to scan the images.

FAQ

Questions? Take a look at the FAQ.

Updated about 1 month ago

← Container Scanning

Version Control Scanning →