docker scout

Scout Cheat Sheet

Docker Scout brings together all the information you need when working on securing your container development, including a layer-by-layer view of dependencies, their known vulnerabilities, and recommended remediation paths.

Docker Scout is designed with developers in mind and is fully integrated into the Docker ecosystem. With Docker Scout, you can spend less time searching for and fixing vulnerabilities and more time developing your code.

The `docker scout` CLI plugin provides a terminal interface for Docker Scout. It is available by default in Docker Desktop starting version 4.17.0.

If you prefer alternative installation methods or require specific versions of the `docker scout` CLI plugin, check out Docker Scout on GitHub.

COMMAND	DESCRIPTION
Observability and Analysis • Gain insights into software composition • Analyze container images for vulnerabilities • Compare images and identify vulnerabilities • Customize output formats and filters	
`docker scout`	Command-line tool for Docker Scout
`docker scout quickview`	Quick overview of an image
`docker scout compare`	Compare two images and display differences
`docker scout compare --to <image_name>:latest <image_name>:v1.2.3-pre`	Compare an image to the latest tag
`docker scout compare --–to-latest <image_name>`	Compare an image to the latest one pushed
`docker scout compare --to-env <env_name> <image_name>`	Compare an image to an environment
`docker scout compare --ignore-base --to <image_name>:latest <image_name>:v1.2.3-pre`	Ignore base images
`docker scout compare --format markdown --to <image_name>:latest <image_name>:v1.2.3-pre`	Generate a markdown output
`docker scout compare --only-package-type maven --only-severity critical --to <image_name>:latest <image_name>:v1.2.3-pre`	Only compare Maven packages and only display critical vulnerabilities for Maven packages
`docker scout environment`	Lists the environment and records images to it
`docker scout config environment`	Print configuration values of the organization

COMMAND	DESCRIPTION
Vulnerability Management	
• Identify and track CVEs in software artifacts • Retrieve Docker Scout version Information • Analyze vulnerabilities by package • Import and export vulnerability data	
`docker scout version`	Show Docker Scout version information
`docker scout cves`	Display CVEs identified in a software artifact
`docker scout cves <image_name>`	Display vulnerabilities grouped by package

`docker save image_name > <image_name>.tar`
 	
`docker scout archive://<image_name>.tar`
	Display vulnerabilities from a `docker save` tarball

`docker scout cves --format sarif --output <image_name>.sarif.json alpine`	Export vulnerabilities to a SARIF JSON file
`docker scout cves oci-dir:// <image_name>`	Display vulnerabilities from an OCI directory
`docker scout cves fs://`	Display vulnerabilities from the current directory
`docker scout repo list enable <repo_name>`	Enable Scout on repositories
Remediation & Recommendation	
• Explore base image updates and recommendations • Optimize image refresh strategies • Streamline image update processes • Fine-tune recommendations with filters	
`docker scout recommendations`	Display available base image updates and remediation recommendations
`docker scout recommendations <image_name>`	Display base image update recommendations
`docker scout recommendations --only-refresh <image_name>`	Display only base image refresh recommendations
`docker scout recommendations --only-update <image_name>`	Display only base image update recommendations
Policy Evaluation	
• Ensure that artifacts align with established supply chain best practices • Visualize how small, incremental changes affect policy status • Provides out-of-the-box policies • Define Supply chain rules for your artifacts • Helps you track how your artifacts perform relative to rules and thresholds, over time	
`docker scout policy <image_name>`	Evaluate policies against an image
`docker scout policy <image_name> --platform <platform_name>`	Evaluate policies against an image with a specific platform
`docker scout policy <repo_name> --to-env <env_name>`	Compare policy results for a repository in a specific environment

Learn more at docker.com/products/docker-scout

docker scout