MCA DevOps Test Solution Outputs

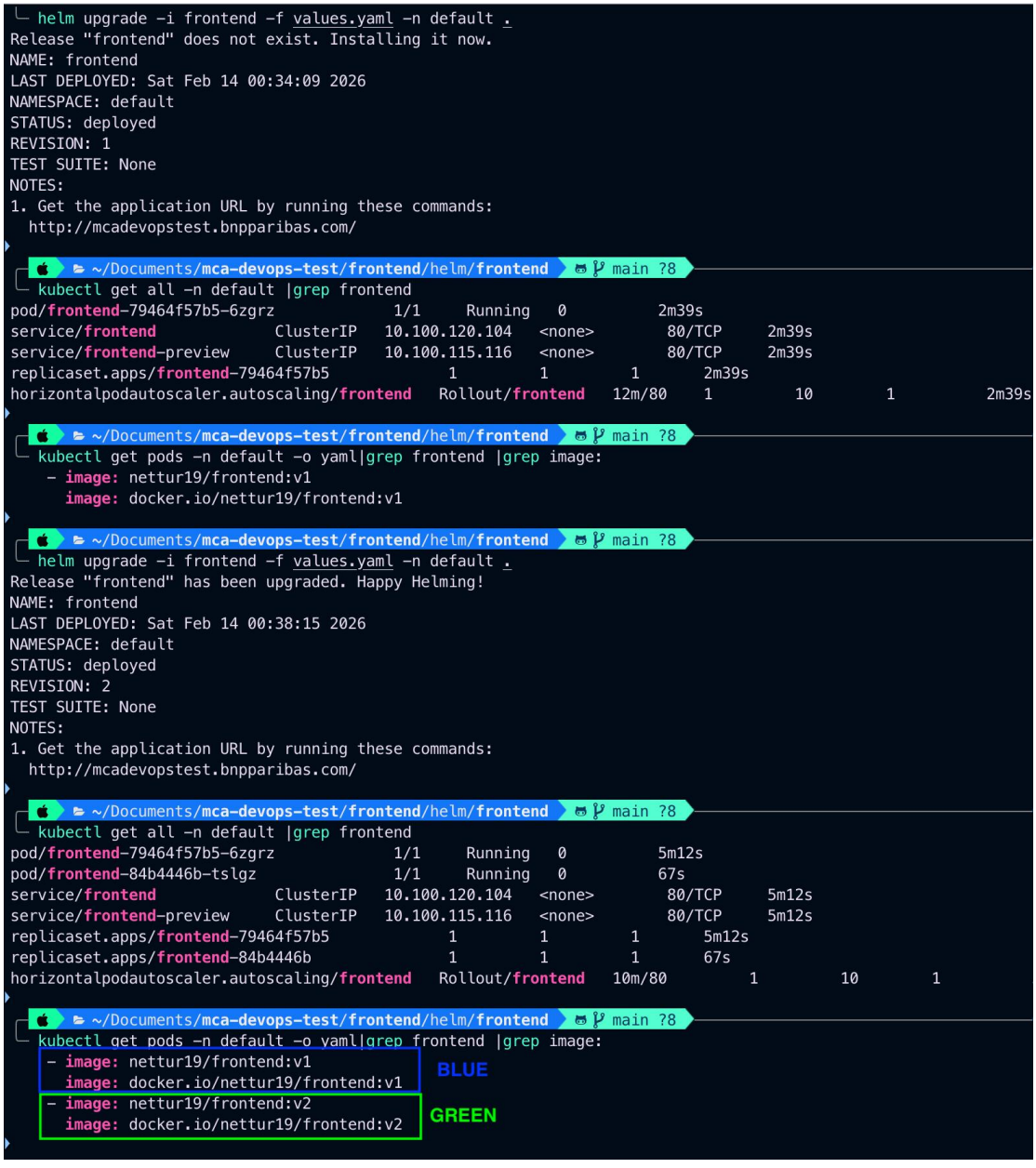
Deployment Strategy

Blue-Green Deployment

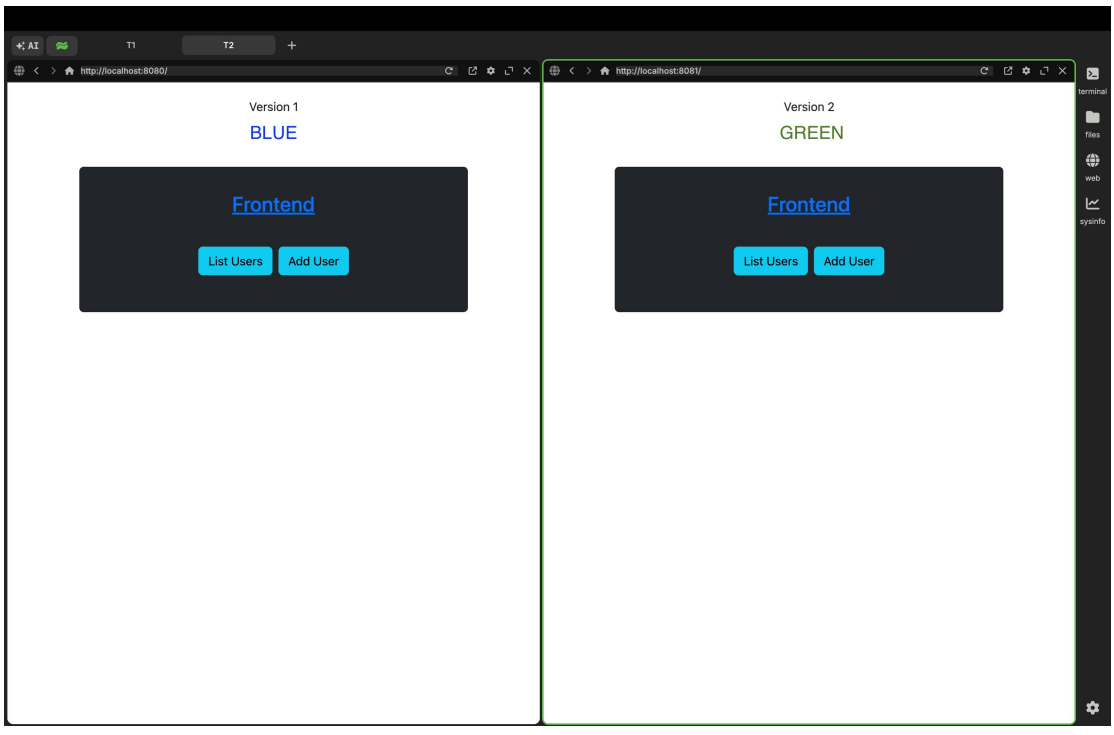
Description:
Blue-Green strategy switches traffic between two identical environments.

Steps

1. Deploy initial (Blue) version. (v1)
2. Deploy new (Green) version. (v2)
3. Switch traffic to Green by Manual/Automatic Promote.
4. Verify rollout.



```
└─ kubectl argo rollouts get rollout frontend

Name:            frontend
Namespace:       default
Status:          ॥ Paused
Message:         BlueGreenPause
Strategy:        BlueGreen
Images:          nettur19/frontend:v1 (stable, active)
                 nettur19/frontend:v2 (preview)
Replicas:
  Desired:       1
  Current:       2
  Updated:       1
  Ready:         1
  Available:     1

NAME                                KIND        STATUS     AGE  INFO
⟳ frontend                          Rollout     ॥ Paused   44m
├──# revision:2
│  └──⧉ frontend-84b4446b            ReplicaSet  ✔ Healthy  40m  preview
│     └──□ frontend-84b4446b-tslgz   Pod         ✔ Running  40m  ready:1/1
└──# revision:1
   └──⧉ frontend-79464f57b5          ReplicaSet  ✔ Healthy  44m  stable,active
      └──□ frontend-79464f57b5-6zgrz Pod         ✔ Running  44m  ready:1/1

 ~/Documents/mca-devops-test/frontend/helm/frontend  main ?8
└─ kubectl argo rollouts promote frontend

rollout 'frontend' promoted

 ~/Documents/mca-devops-test/frontend/helm/frontend  main ?8
└─ kubectl argo rollouts get rollout frontend

Name:            frontend
Namespace:       default
Status:          ✔ Healthy
Strategy:        BlueGreen
Images:          nettur19/frontend:v1
                 nettur19/frontend:v2 (stable, active)
Replicas:
  Desired:       1
  Current:       2
  Updated:       1
  Ready:         1
  Available:     1

NAME                                KIND        STATUS     AGE  INFO
⟳ frontend                          Rollout     ✔ Healthy  45m
├──# revision:2
│  └──⧉ frontend-84b4446b            ReplicaSet  ✔ Healthy  40m  stable,active
│     └──□ frontend-84b4446b-tslgz   Pod         ✔ Running  40m  ready:1/1
└──# revision:1
   └──⧉ frontend-79464f57b5          ReplicaSet  ✔ Healthy  45m  delay:17s
      └──□ frontend-79464f57b5-6zgrz Pod         ✔ Running  45m  ready:1/1


 ~/Documents/mca-devops-test/frontend/helm/frontend  main ?8
└─ kubectl get pods -n default -o yaml|grep frontend |grep image:
    - image: nettur19/frontend:v2
      image: docker.io/nettur19/frontend:v2
```

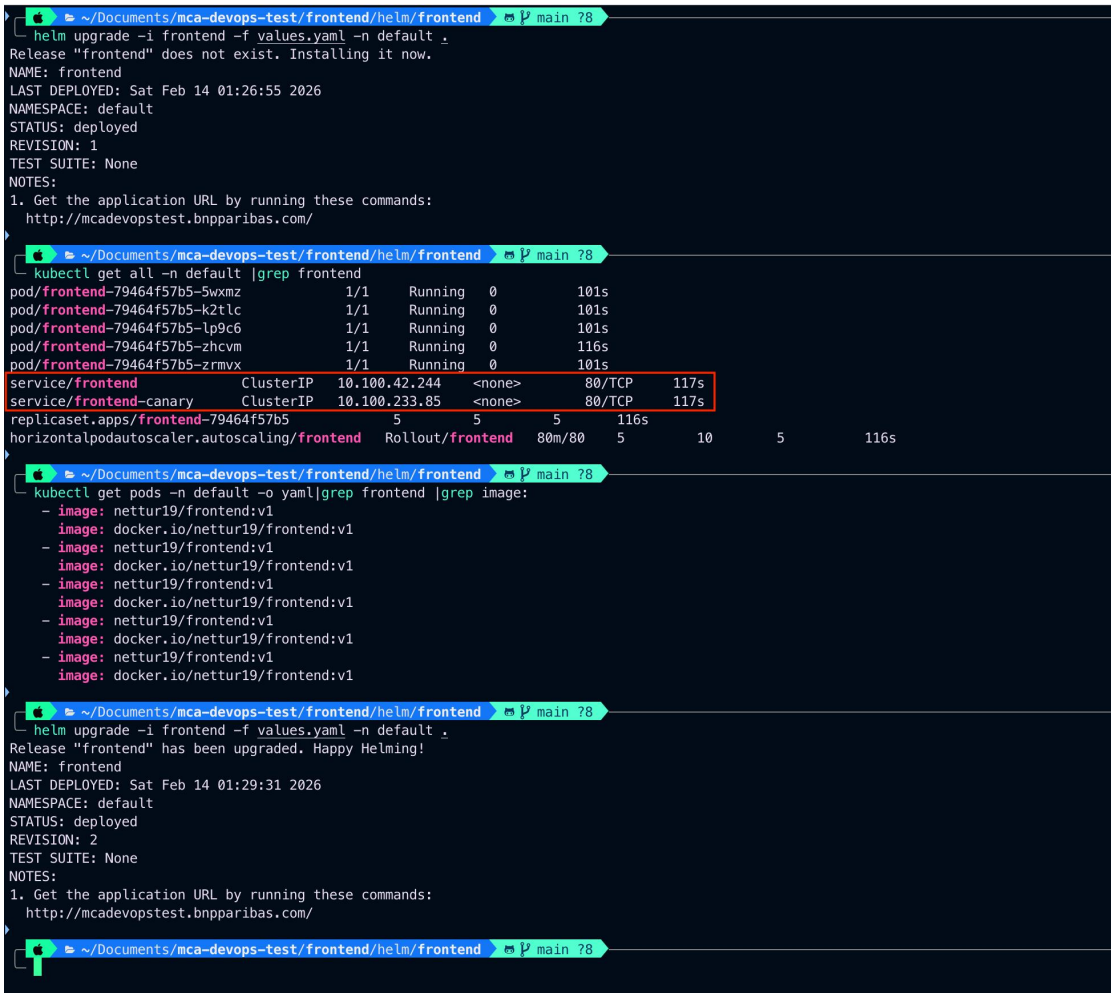


Canary Deployment

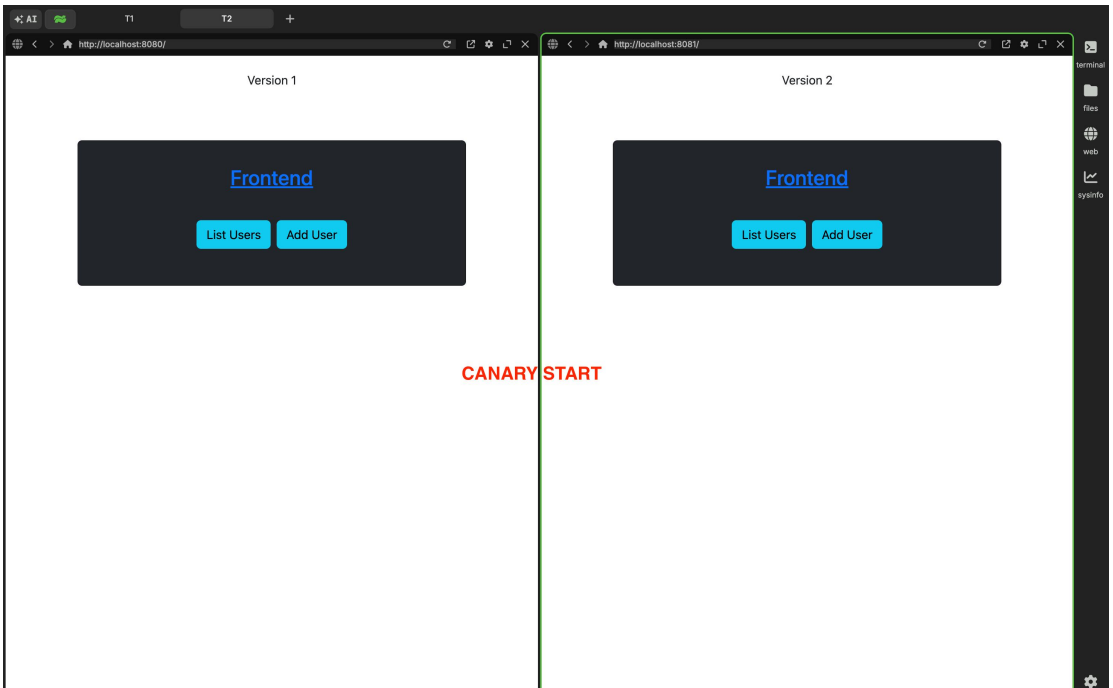
Description:
Canary strategy gradually shifts traffic to the new version.

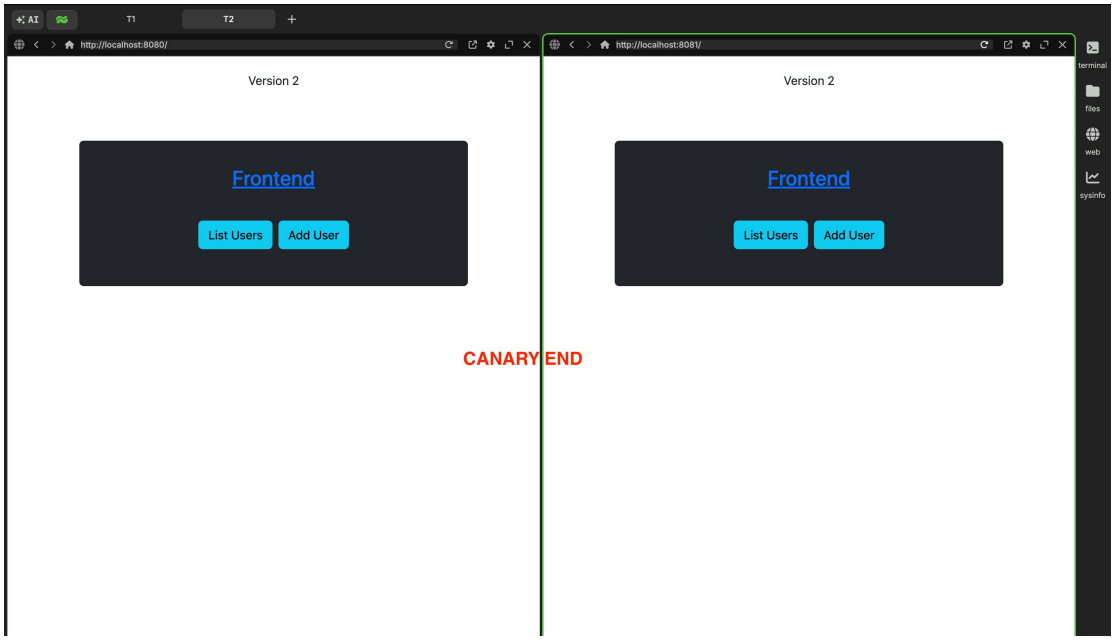
Steps

- Deploy base version.
- Release canary version.
- Increase traffic weight.
- Complete rollout.



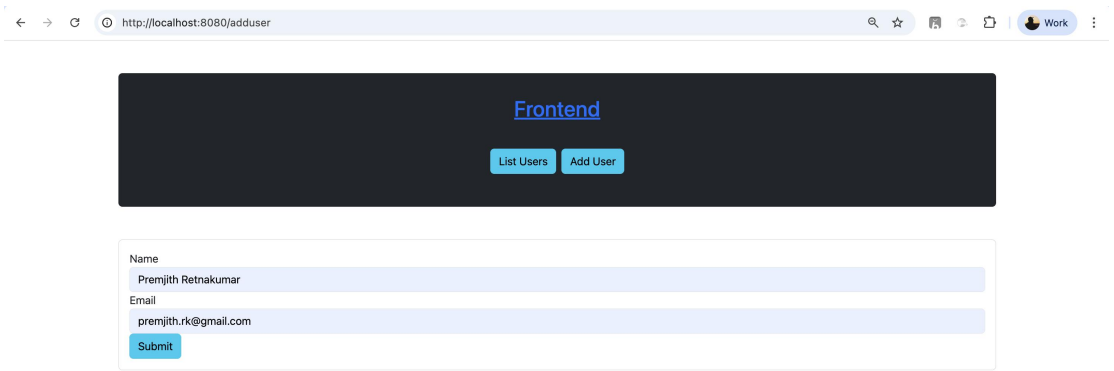
```
~/Documents/mca-devops-test/frontend/helm/frontend main ?8
kubectl get pods -n default -o yaml|grep frontend |grep image:
  - image: nettur19/frontend:v1
    image: docker.io/nettur19/frontend:v1
  - image: nettur19/frontend:v1
    image: docker.io/nettur19/frontend:v1
  - image: nettur19/frontend:v1
    image: docker.io/nettur19/frontend:v1
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2

~/Documents/mca-devops-test/frontend/helm/frontend main ?8
kubectl get pods -n default -o yaml|grep frontend |grep image:
  - image: nettur19/frontend:v1
    image: docker.io/nettur19/frontend:v1
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
  - image: nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2

~/Documents/mca-devops-test/frontend/helm/frontend main ?8
kubectl get pods -n default -o yaml|grep frontend |grep image:
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2
  - image: nettur19/frontend:v2
    image: docker.io/nettur19/frontend:v2

~/Documents/mca-devops-test/frontend/helm/frontend main ?8
kubectl argo rollouts get rollout frontend

Name:            frontend
Namespace:       default
Status:          ✔ Healthy
Strategy:        Canary
  Step:          5/5
  SetWeight:     100
  ActualWeight:  100
Images:          nettur19/frontend:v2 (stable)
Replicas:
  Desired:       5
  Current:       5
  Updated:       5
  Ready:         5
  Available:     5

NAME                              KIND        STATUS        AGE    INFO
⟳ frontend                        Rollout     ✔ Healthy     5m5s
├──# revision:2
│  └──⧉ frontend-84b4446b         ReplicaSet  ✔ Healthy     2m28s  stable
│     ├──□ frontend-84b4446b-kgkf6  Pod       ✔ Running     2m28s  ready:1/1
│     ├──□ frontend-84b4446b-vkjqx  Pod       ✔ Running     116s   ready:1/1
│     ├──□ frontend-84b4446b-fkrhb  Pod       ✔ Running     114s   ready:1/1
│     ├──□ frontend-84b4446b-zf2lb  Pod       ✔ Running     81s    ready:1/1
│     └──□ frontend-84b4446b-n6g9g  Pod       ✔ Running     78s    ready:1/1
└──# revision:1
   └──⧉ frontend-79464f57b5       ReplicaSet  • ScaledDown  5m5s
```

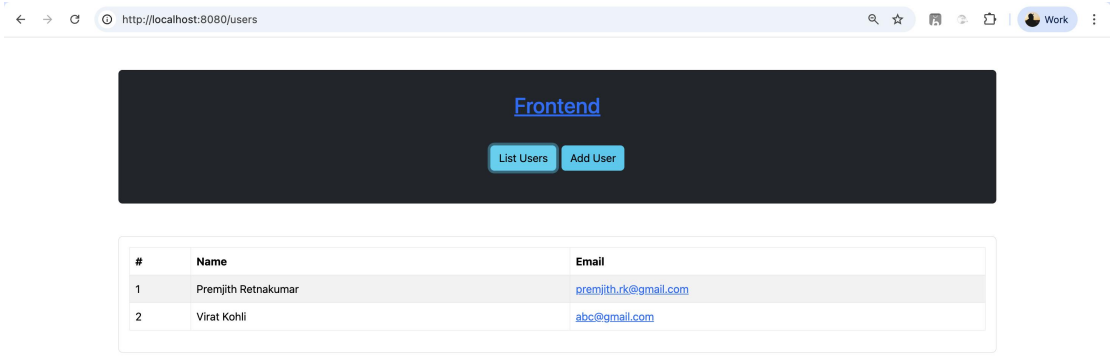




Application Functionality

Description:
Basic application functionality verified after deployment.





Query Query History

```
1 SELECT * FROM public.users
2 ORDER BY id ASC
```

Data Output Messages Notifications

	id [PK] bigint	email character varying (255)	name character varying (255)
1	1	premjith.rk@gmail.com	Premjith Retnakumar
2	2	abc@gmail.com	Virat Kohli

SonarQube Code Analysis

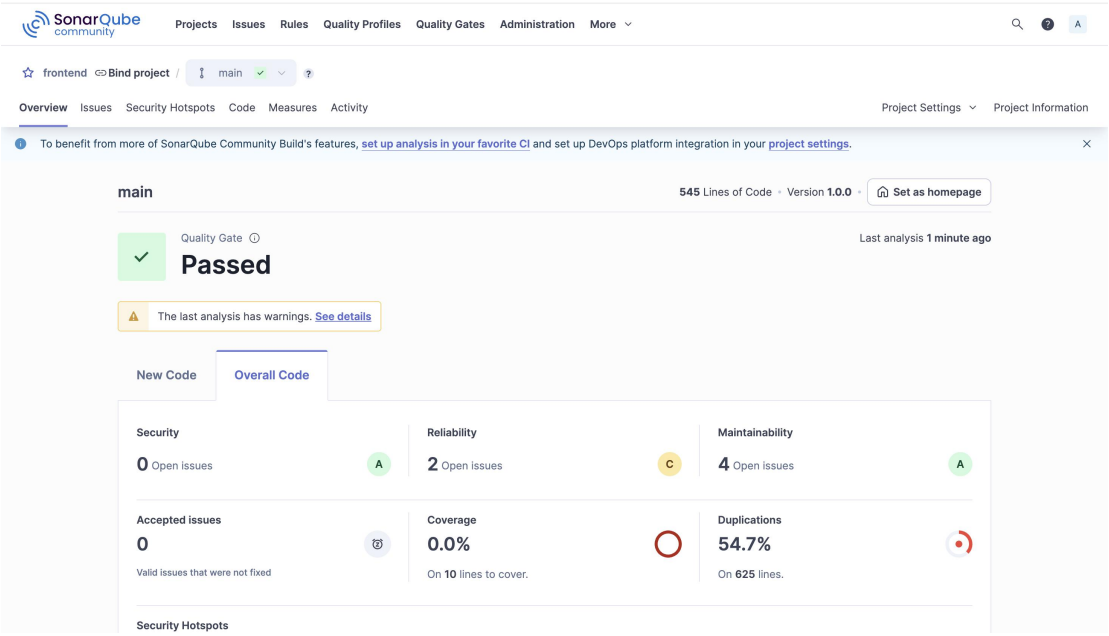
Description:
Static code analysis performed before deployment.

Checks Performed

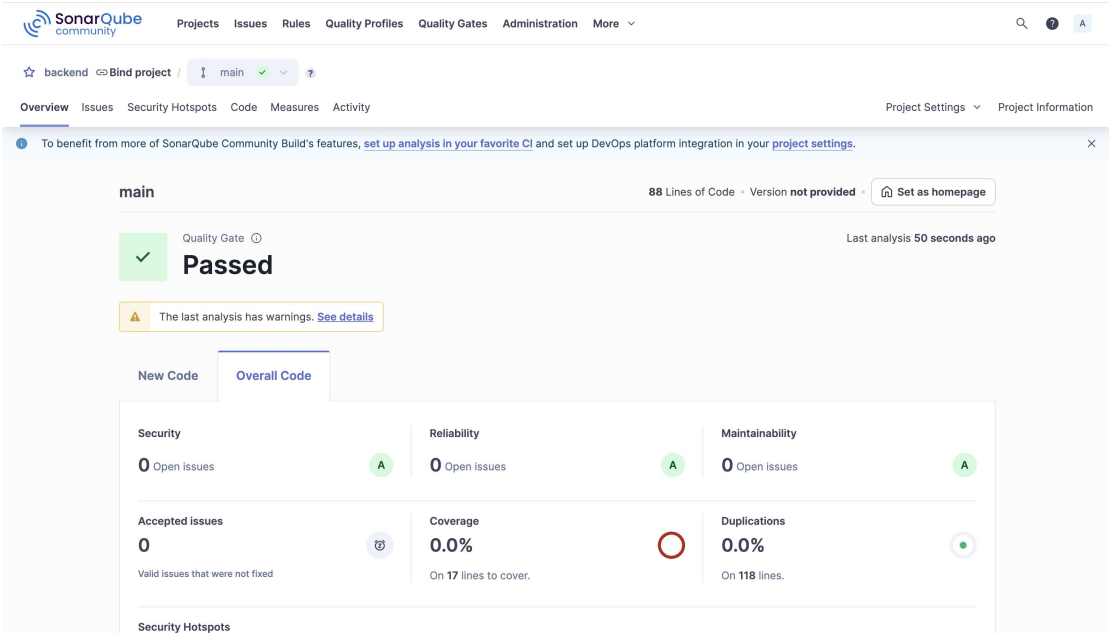
- Code Quality Gate
- Bugs & Vulnerabilities
- Code Smells
- Coverage

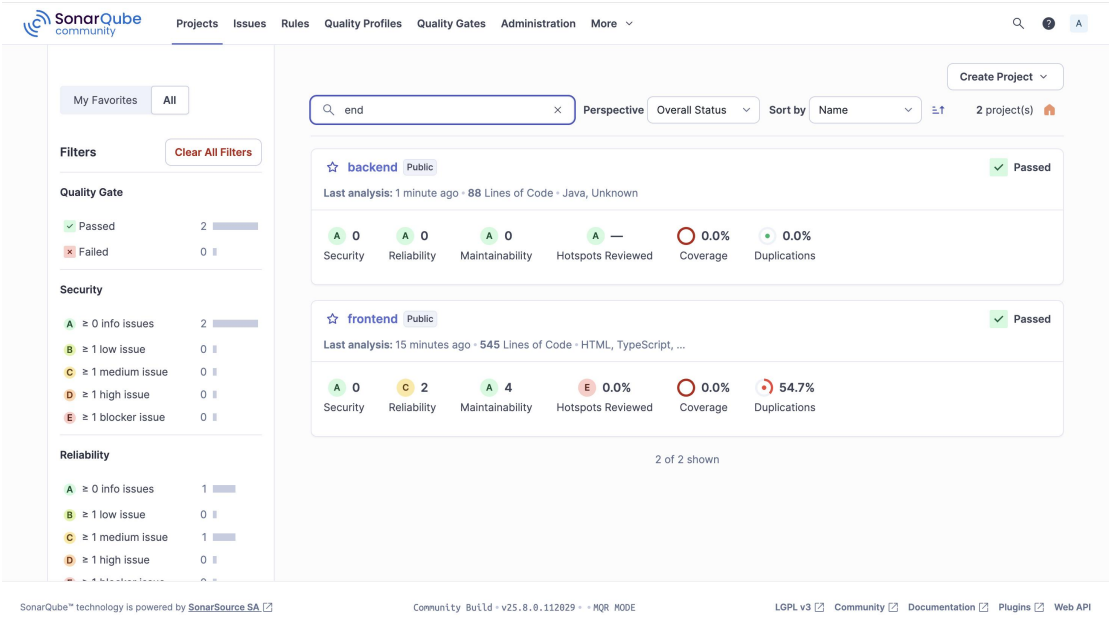
Screenshots

Frontend Sonarqube Scan Report



Backend Sonarqube Scan Report





Trivy Security Scanning

Description:
Security scans performed on both the filesystem and container images.

Filesystem Scan

Scans project source code and dependencies for vulnerabilities.

pom.xml – Trivy Report – 2026-02-14 02:45:37.320206441 +0530 IST m=+47.243644310

CRITICAL: 1 | HIGH: 8 | MEDIUM: 8 | LOW: 7 | UNKNOWN: 0

Filter by package/type | All Severities

pom						
Package	Vuln ID	Severity	Installed	Fixed	Description	Links
ch.qos.logback:logback-core	CVE-2024-12798	MEDIUM	1.5.11	1.5.13, 1.3.15	ACE vulnerability in JaninoEventEvaluator by QOS.CH logback-core upto including version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 in Java applications allows attacker to execute Show more	https://access.redhat.com/security/cve/CVE-2024-12798 https://github.com/qos-ch/logback https://github.com/qos-ch/logback/commit/2cb6d520df7592ef1c3a1 https://logback.qos.ch/news.html#1.3.15
ch.qos.logback:logback-core	CVE-2025-11226	MEDIUM	1.5.11	1.5.19, 1.3.16	ACE vulnerability in conditional configuration file processing by QOS.CH logback-core up to and including version 1.5.18 in Java applications, allows an attacker to execute Show more	https://access.redhat.com/security/cve/CVE-2025-11226 https://github.com/qos-ch/logback https://github.com/qos-ch/logback/commit/61f6a2544f36b3016e0ef https://github.com/qos-ch/logback/issues/974
ch.qos.logback:logback-core	CVE-2024-12801	LOW	1.5.11	1.5.13, 1.3.15	Server-Side Request Forgery (SSRF) in SaxEventRecorder by QOS.CH logback version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 on the Java platform, allows an attacker to forge Show more	https://access.redhat.com/security/cve/CVE-2024-12801 https://github.com/qos-ch/logback https://github.com/qos-ch/logback/commit/5f05041cba4c4ac0a627 https://logback.qos.ch/news.html#1.3.15
ch.qos.logback:logback-core	CVE-2026-1225	LOW	1.5.11	1.5.25	ACE vulnerability in configuration file processing by QOS.CH logback-core up to and including version 1.5.24 in Java applications, allows an attacker to instantiate classes Show more	https://access.redhat.com/security/cve/CVE-2026-1225 https://github.com/qos-ch/logback https://github.com/qos-ch/logback/commit/1f97ae1844b1be8486e4 https://github.com/qos-ch/logback/issues/997
org.apache.commons:commons-lang3	CVE-2025-48924	MEDIUM	3.14.0	3.18.0	Uncontrolled Recursion vulnerability in Apache Commons Lang. This issue affects Apache Commons Lang: Starting with commons-lang:commons-lang 2.0 to 2.6, and, from Show more	http://www.openwall.com/lists/oss-security/2025/07/11/1 https://access.redhat.com/security/cve/CVE-2025-48924 https://github.com/apache/commons-lang https://github.com/apache/commons-lang/commit/b424803abdb2bec818e4fbcb251ce031c22aca53
org.apache.tomcat.embed:tomcat-embed-core	CVE-2025-24813	CRITICAL	10.1.31	11.0.3, 10.1.35, 9.0.99	Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files Show more	http://www.openwall.com/lists/oss-security/2025/03/10/5 https://access.redhat.com/errata/RHSA-2025:3645 https://access.redhat.com/security/cve/CVE-2025-24813 https://bugzilla.redhat.com/2332817
org.apache.tomcat.embed:tomcat-	CVE-	HIGH	10.1.31	11.0.2,	Time-of-check Time-of-use (TOCTOU) Race Condition	http://www.openwall.com/lists/oss-security/2024/12/17/4

Trivy Report – 2026-02-14 02:39:34.441954114 +0530 IST m=+0.386795348

CRITICAL: 0 | HIGH: 0 | MEDIUM: 0 | LOW: 0 | UNKNOWN: 0

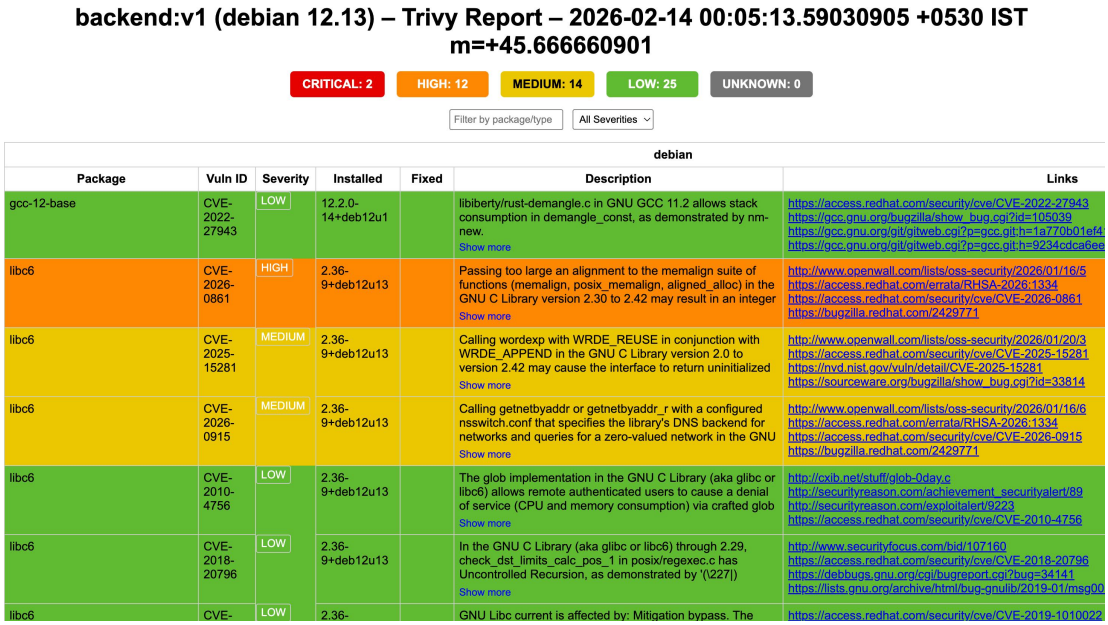
Filter by package/type | All Severities

No scan results found.

Container Image Scan

Scans the built container image for OS and library vulnerabilities.

Screenshot

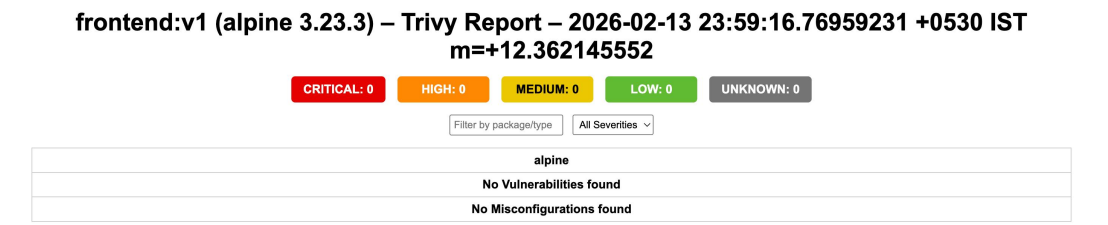


backend:v1 (debian 12.13) – Trivy Report – 2026-02-14 00:05:13.59030905 +0530 IST m=+45.666660901

CRITICAL: 2 | HIGH: 12 | MEDIUM: 14 | LOW: 25 | UNKNOWN: 0

Filter by package/type | All Severities

debian						
Package	**Vuln ID**	**Severity**	**Installed**	**Fixed**	**Description**	**Links**
gcc-12-base	CVE-2022-27943	LOW	12.2.0-14+deb12u1		libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new. Show more	https://access.redhat.com/security/cve/CVE-2022-27943 https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039 https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=1a770b01ef4 https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=9234cdca6ee
libc6	CVE-2026-0861	HIGH	2.36-9+deb12u13		Passing too large an alignment to the memalign suite of functions (memalign, posix_memalign, aligned_alloc) in the GNU C Library version 2.30 to 2.42 may result in an integer Show more	http://www.openwall.com/lists/oss-security/2026/01/16/5 https://access.redhat.com/errata/RHSA-2026:1334 https://access.redhat.com/security/cve/CVE-2026-0861 https://bugzilla.redhat.com/2429771
libc6	CVE-2025-15281	MEDIUM	2.36-9+deb12u13		Calling wordexp with WRDE_REUSE in conjunction with WRDE_APPEND in the GNU C Library version 2.0 to version 2.42 may cause the interface to return uninitialized Show more	http://www.openwall.com/lists/oss-security/2026/01/20/3 https://access.redhat.com/security/cve/CVE-2025-15281 https://nvd.nist.gov/vuln/detail/CVE-2025-15281 https://sourceware.org/bugzilla/show_bug.cgi?id=33814
libc6	CVE-2026-0915	MEDIUM	2.36-9+deb12u13		Calling getnetbyaddr or getnetbyaddr_r with a configured nsswitch.conf that specifies the library's DNS backend for networks and queries for a zero-valued network in the GNU Show more	http://www.openwall.com/lists/oss-security/2026/01/16/6 https://access.redhat.com/errata/RHSA-2026:1334 https://access.redhat.com/security/cve/CVE-2026-0915 https://bugzilla.redhat.com/2429771
libc6	CVE-2010-4756	LOW	2.36-9+deb12u13		The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob Show more	http://cxib.net/stuff/glob-0day.c http://securityreason.com/achievement_securityalert/89 http://securityreason.com/exploitalert/9223 https://access.redhat.com/security/cve/CVE-2010-4756
libc6	CVE-2018-20796	LOW	2.36-9+deb12u13		In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|) Show more	http://www.securityfocus.com/bid/107160 https://access.redhat.com/security/cve/CVE-2018-20796 https://debbugs.gnu.org/cgi/bugreport.cgi?bug=34141 https://lists.gnu.org/archive/html/bug-gnulib/2019-01/msg00
libc6	CVE-	LOW	2.36-		GNU Libc current is affected by: Mitigation bypass. The	https://access.redhat.com/security/cve/CVE-2019-1010022



frontend:v1 (alpine 3.23.3) – Trivy Report – 2026-02-13 23:59:16.76959231 +0530 IST m=+12.362145552

CRITICAL: 0 | HIGH: 0 | MEDIUM: 0 | LOW: 0 | UNKNOWN: 0

Filter by package/type | All Severities

alpine
No Vulnerabilities found
No Misconfigurations found