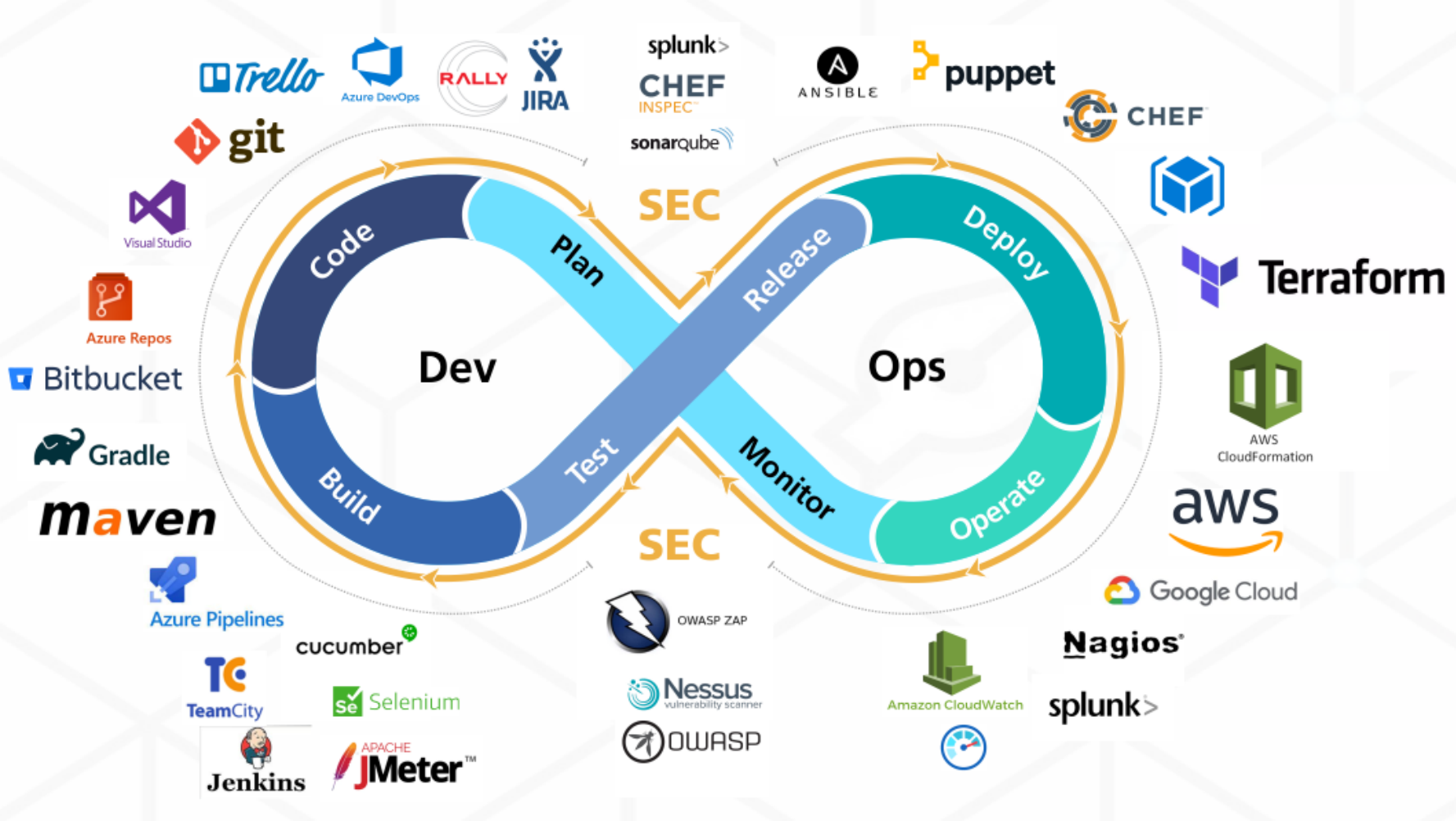
Building Trust in the Container Supply Chain

SterkIT

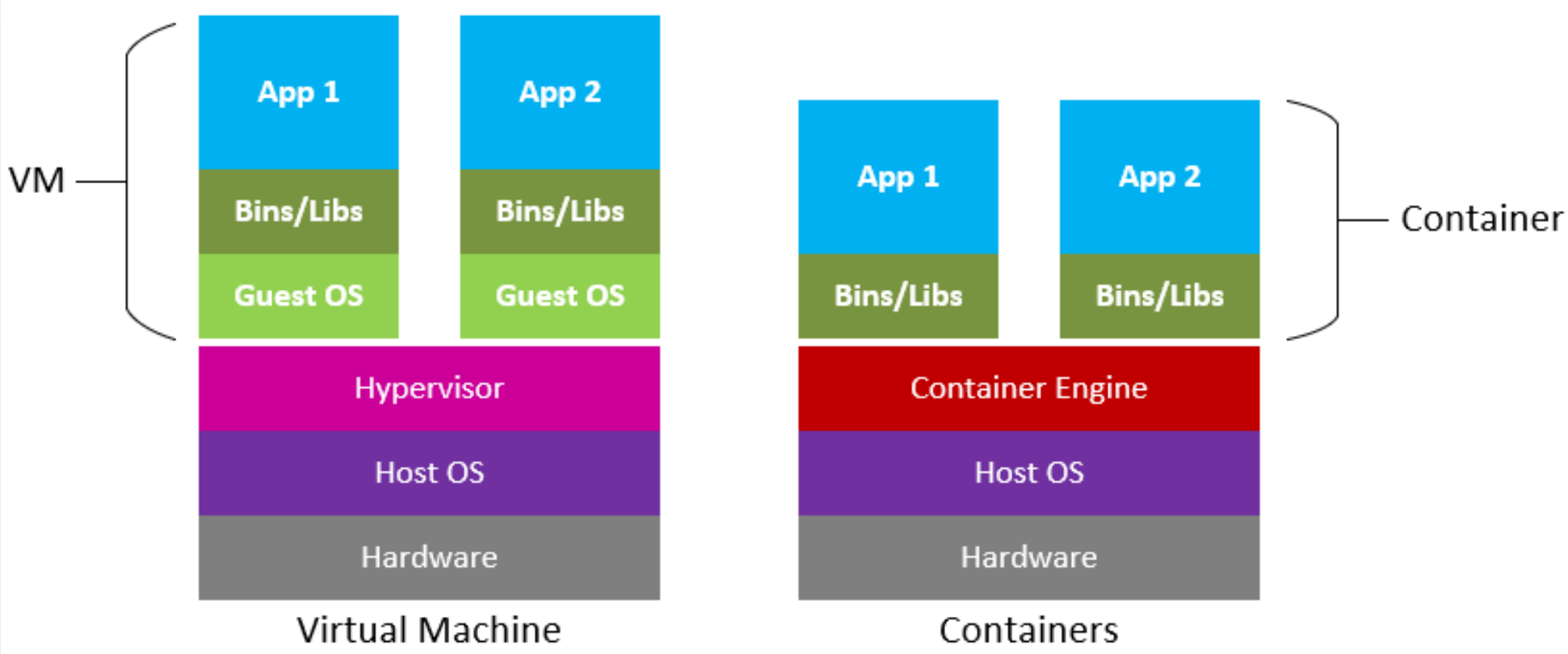
Kompetente folk, bedre løsninger

StrekIT.no

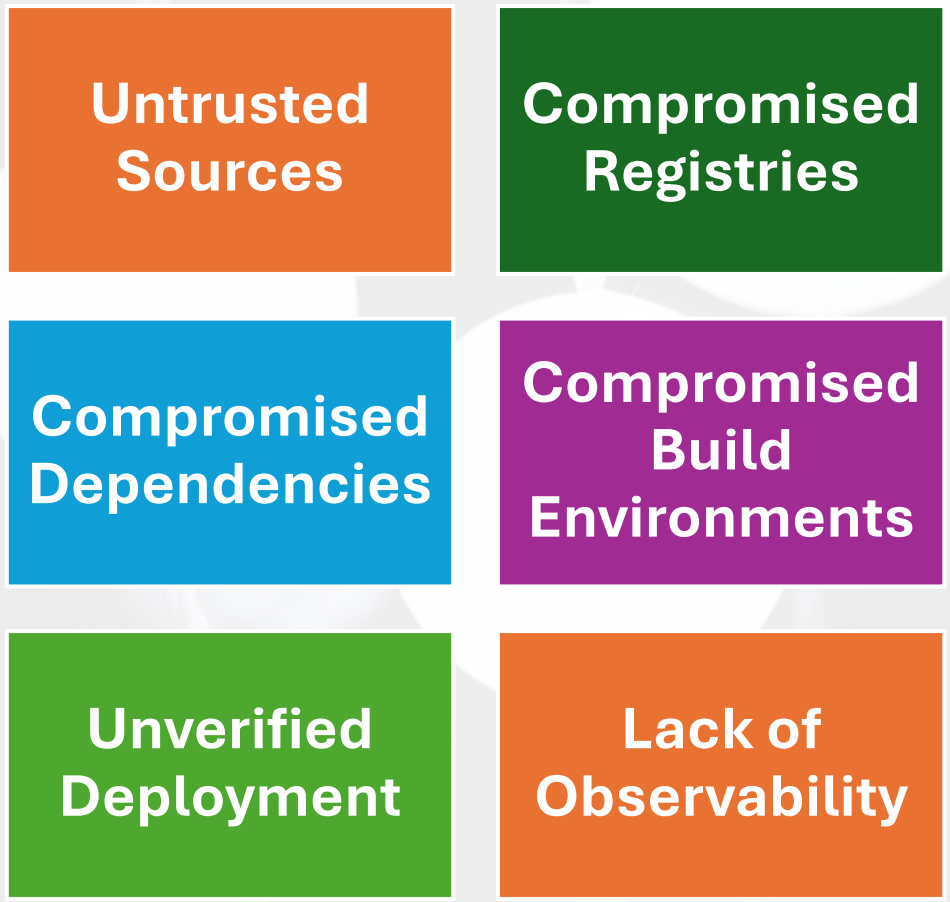
What is DevSecOps?



What are containers?



Why is the issue then?



Microsoft Containers Secure Supply Chain framework

Containers secure supply chain framework

Stage	Details
Acquire	Acquire container images from external sources or third-party vendors.
Catalog	Offer approved container images for internal consumption including builds and deployments.
Build	Produce compliant service and application images and deployment artifacts.
Deploy	Securely deploy containerized services and applications to the hosting environments.
Run	Run containers created from compliant, latest, and secure container images executing the business logic for an application.

CSSC Stages: Acquire

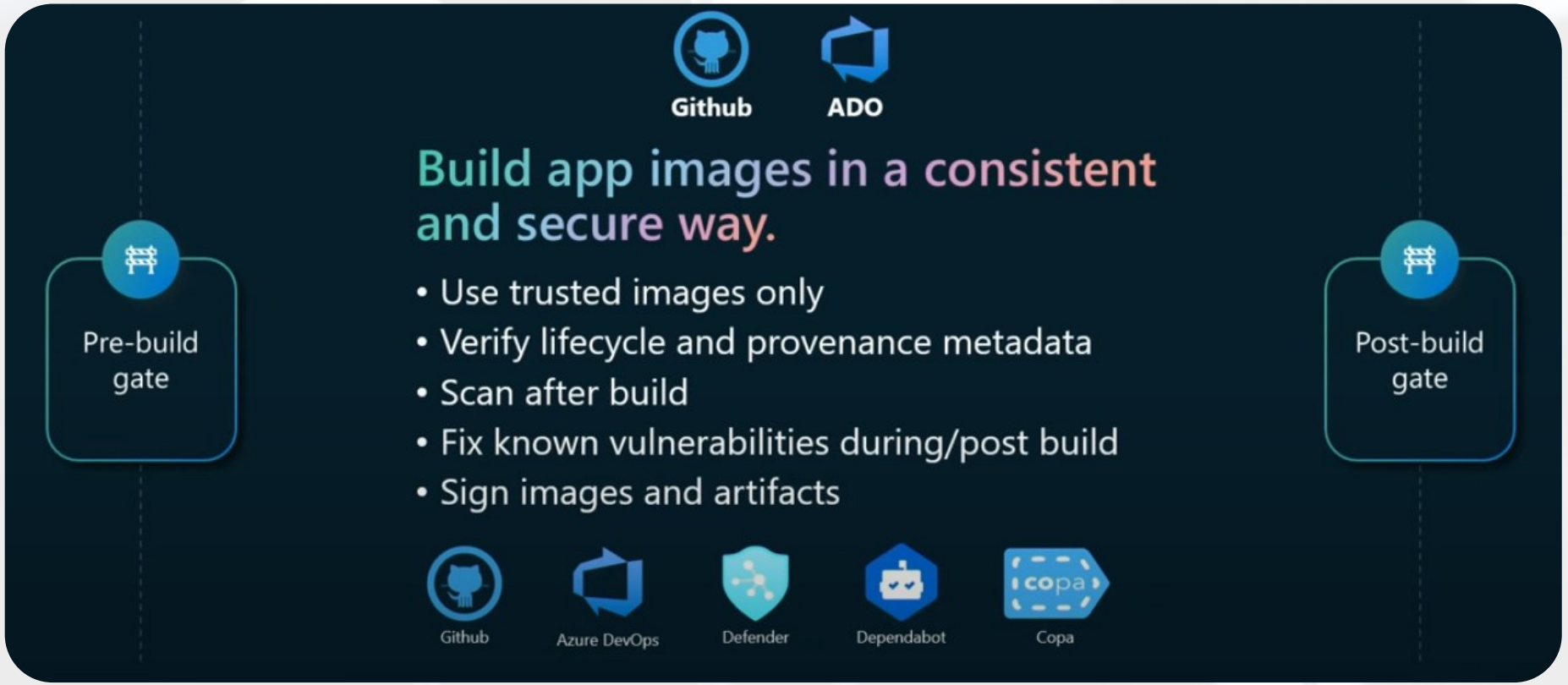
Acquire

CSSC Stages: Catalog

Catalog

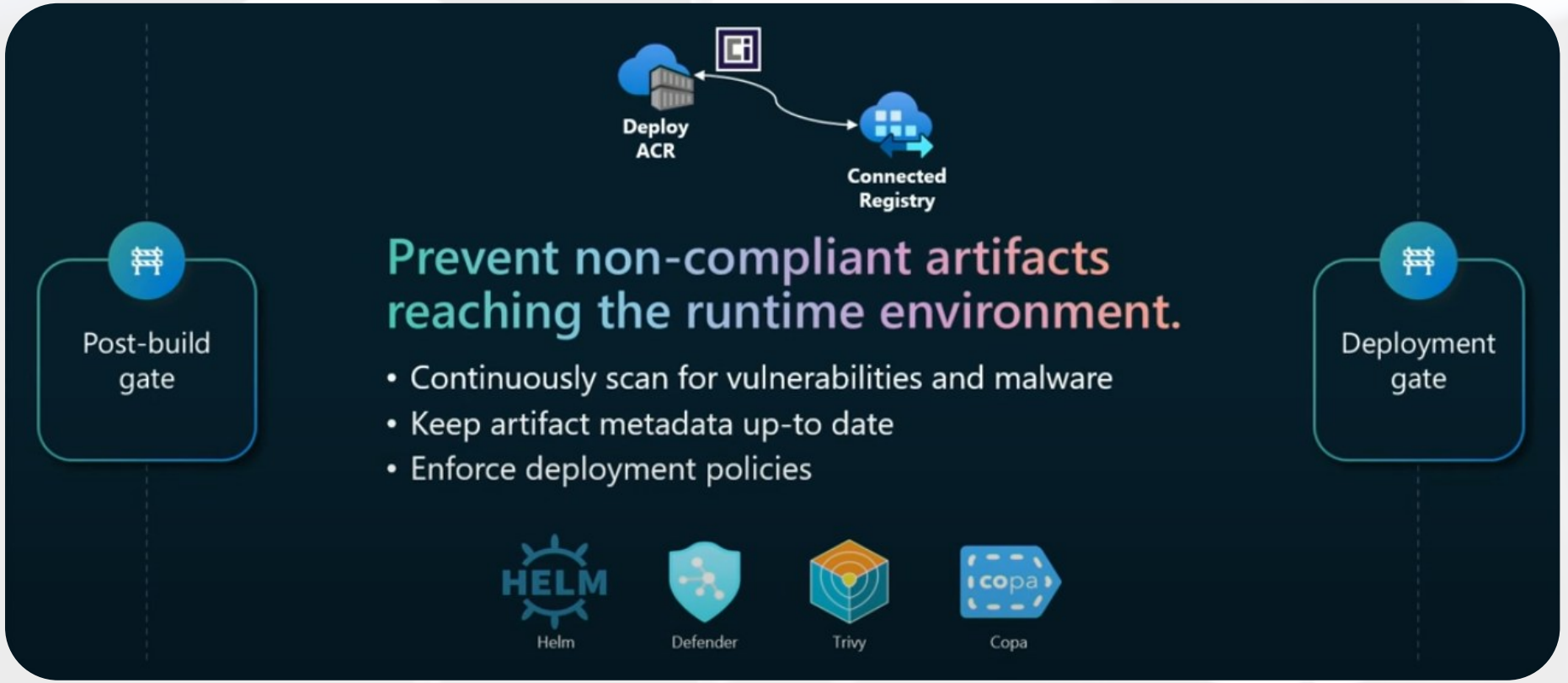
CSSC Stages: Build

Build



CSSC Stages: Deploy

Deploy



CSSC Stages: Run

Demo

1. Build and push to pipeline
2. Scan vulnerabilty and create SBOM
3. Attach artifacts with container image
4. Sign image
5. Push to ACR
6. Pull from ACR

Demo

1. Container Security Scanning
2. Software Bill of Materials (SBOM) Generation
3. Artifact Signing & Verification

4. Automated Policy Enforcement
5. Supply Chain Governance
6. Shift-Left Security

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

- Build & scan the c... 1m 18s
  - Initialize job 2s
  - Checkout DevSecOps... 1s
  - Build order-api cont... 20s
  - Download Trivy v0.61... 3s
  - Scan the order-api co... 9s
  - Scan the order-api ... <1s
  - Push order-api contai... 4s
  - Attach the scan res... 16s
  - List attached artifacts... 6s
  - Create a SBOM doc... <1s
  - Attach the SBOM do... 5s
  - List attached artifacts... 6s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

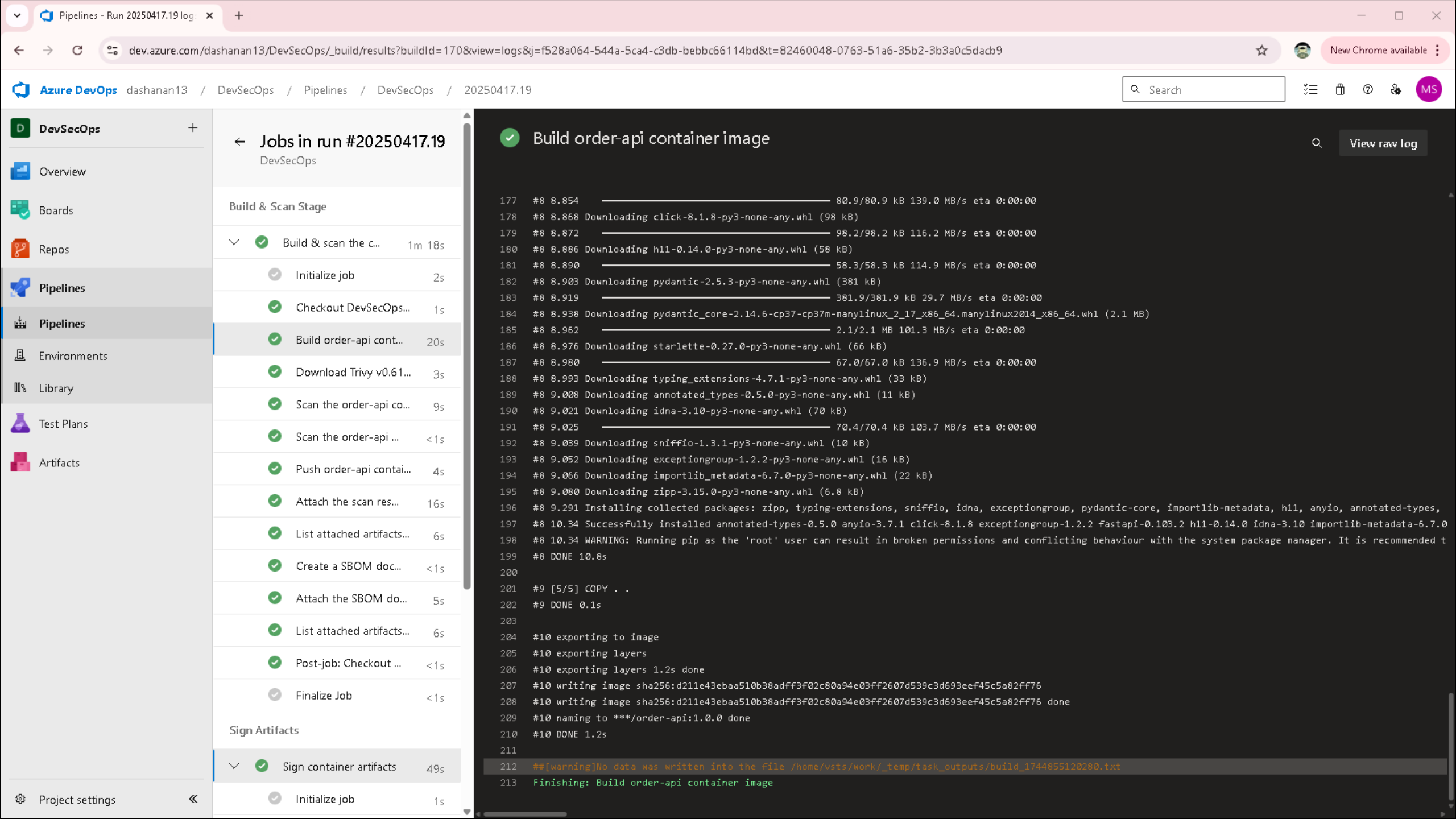
Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s

Build & scan the container image

View raw log

```
1  ##[warning]See https://aka.ms/azdo-ubuntu-24.04 for changes to the ubuntu-24.04 image. Some tools (e.g. Mono, NuGet, Terraform) are not available on the image. The
2  Pool: Azure Pipelines
3  Image: ubuntu-latest
4  Agent: Hosted Agent
5  Started: Today at 3:58 AM
6  Duration: 1m 18s
7
8  ▸ Job preparation parameters
43 Job live console data:
44 Finishing: Build & scan the container image
```


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=f528a064-544a-5ca4-c3db-bebbc66114bd&t=82460048-0763-51a6-35b2-3b3a0c5dacb9
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
DevSecOps
Build & Scan Stage
Build & scan the c... 1m 18s
Initialize job 2s
Checkout DevSecOps... 1s
Build order-api cont... 20s
Download Trivy v0.61... 3s
Scan the order-api co... 9s
Scan the order-api ... <1s
Push order-api contai... 4s
Attach the scan res... 16s
List attached artifacts... 6s
Create a SBOM doc... <1s
Attach the SBOM do... 5s
List attached artifacts... 6s
Post-job: Checkout ... <1s
Finalize Job <1s
Sign Artifacts
Sign container artifacts 49s
Initialize job 1s
Build order-api container image
View raw log
177 #8 8.854 ━━ 80.9/80.9 kB 139.0 MB/s eta 0:00:00
178 #8 8.868 Downloading click-8.1.8-py3-none-any.whl (98 kB)
179 #8 8.872 ━━ 98.2/98.2 kB 116.2 MB/s eta 0:00:00
180 #8 8.886 Downloading h11-0.14.0-py3-none-any.whl (58 kB)
181 #8 8.890 ━━ 58.3/58.3 kB 114.9 MB/s eta 0:00:00
182 #8 8.903 Downloading pydantic-2.5.3-py3-none-any.whl (381 kB)
183 #8 8.919 ━━ 381.9/381.9 kB 29.7 MB/s eta 0:00:00
184 #8 8.938 Downloading pydantic_core-2.14.6-cp37-cp37m-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
185 #8 8.962 ━━ 2.1/2.1 MB 101.3 MB/s eta 0:00:00
186 #8 8.976 Downloading starlette-0.27.0-py3-none-any.whl (66 kB)
187 #8 8.980 ━━ 67.0/67.0 kB 136.9 MB/s eta 0:00:00
188 #8 8.993 Downloading typing_extensions-4.7.1-py3-none-any.whl (33 kB)
189 #8 9.008 Downloading annotated_types-0.5.0-py3-none-any.whl (11 kB)
190 #8 9.021 Downloading idna-3.10-py3-none-any.whl (70 kB)
191 #8 9.025 ━━ 70.4/70.4 kB 103.7 MB/s eta 0:00:00
192 #8 9.039 Downloading sniffio-1.3.1-py3-none-any.whl (10 kB)
193 #8 9.052 Downloading exceptiongroup-1.2.2-py3-none-any.whl (16 kB)
194 #8 9.066 Downloading importlib_metadata-6.7.0-py3-none-any.whl (22 kB)
195 #8 9.080 Downloading zipp-3.15.0-py3-none-any.whl (6.8 kB)
196 #8 9.291 Installing collected packages: zipp, typing-extensions, sniffio, idna, exceptiongroup, pydantic-core, importlib-metadata, h11, anyio, annotated-types,
197 #8 10.34 Successfully installed annotated-types-0.5.0 anyio-3.7.1 click-8.1.8 exceptiongroup-1.2.2 fastapi-0.103.2 h11-0.14.0 idna-3.10 importlib-metadata-6.7.0
198 #8 10.34 WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended t
199 #8 DONE 10.8s
200
201 #9 [5/5] COPY . .
202 #9 DONE 0.1s
203
204 #10 exporting to image
205 #10 exporting layers
206 #10 exporting layers 1.2s done
207 #10 writing image sha256:d211e43ebaa510b38adff3f02c80a94e03ff2607d539c3d693eef45c5a82ff76
208 #10 writing image sha256:d211e43ebaa510b38adff3f02c80a94e03ff2607d539c3d693eef45c5a82ff76 done
209 #10 naming to ***/order-api:1.0.0 done
210 #10 DONE 1.2s
211
212 ##[warning]No data was written into the file /home/vsts/work/_temp/task_outputs/build_1744855120280.txt
213 Finishing: Build order-api container image

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

- Build & scan the c... 1m 18s
  - Initialize job 2s
  - Checkout DevSecOps... 1s
  - Build order-api cont... 20s
  - Download Trivy v0.61... 3s
  - Scan the order-api co... 9s
  - Scan the order-api ... <1s
  - Push order-api contai... 4s
  - Attach the scan res... 16s
  - List attached artifacts... 6s
  - Create a SBOM doc... <1s
  - Attach the SBOM do... 5s
  - List attached artifacts... 6s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

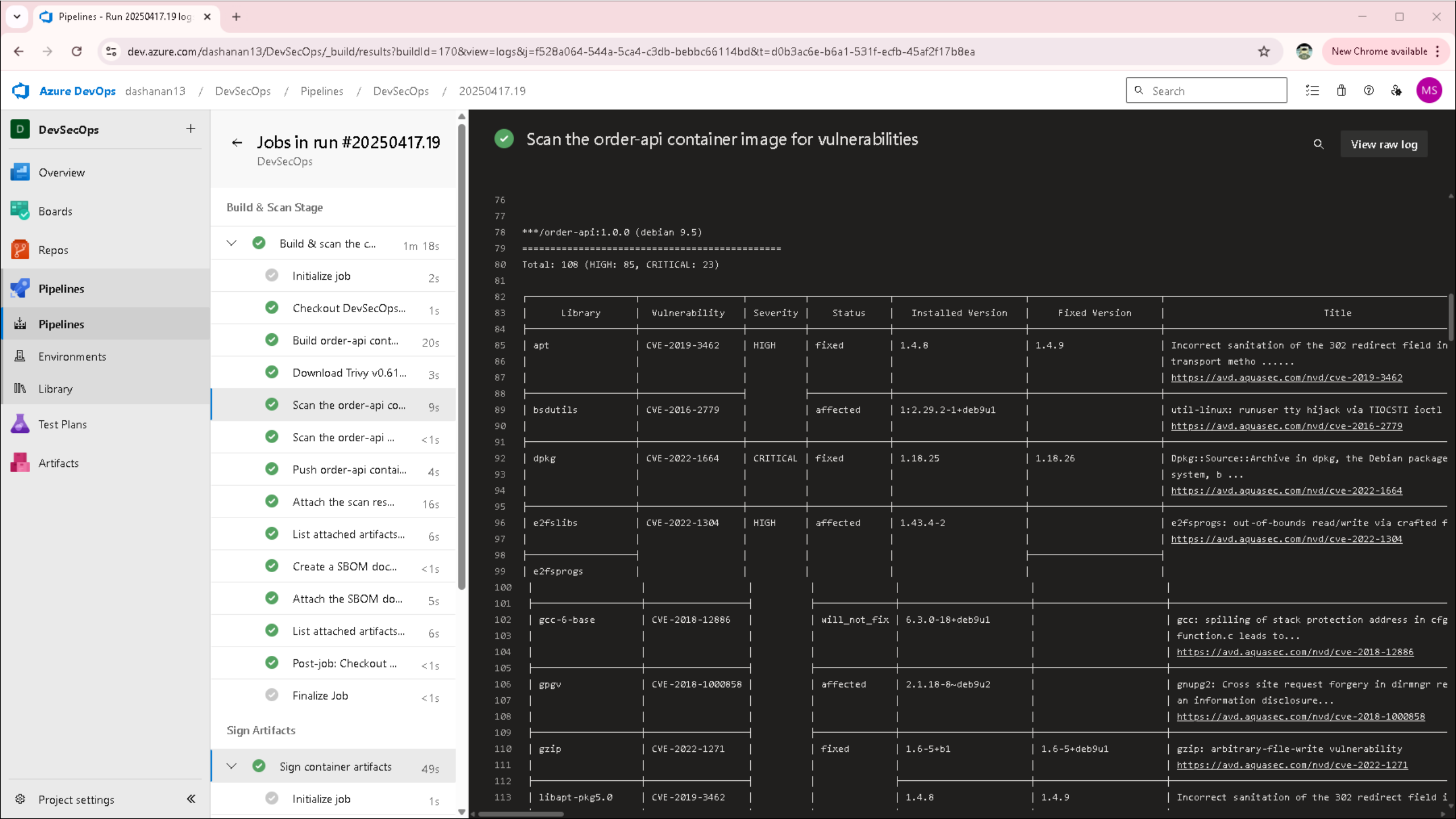
Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s

Scan the order-api container image for vulnerabilities

View raw log

```
Starting: Scan the order-api container image for vulnerabilities
==============================================================================
Task         : Bash
Description  : Run a Bash script on macOS, Linux, or Windows
Version      : 3.250.1
Author       : Microsoft Corporation
Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/bash
==============================================================================
Generating script.
Script contents:
trivy image --exit-code 0 --severity HIGH,CRITICAL --scanners vuln ***/order-api:1.0.0
========================== Starting Command Output ===========================
/usr/bin/bash /home/vsts/work/_temp/7f95442e-cb57-4d1a-9db8-9aa9ef0baaa8.sh
2025-04-17T01:58:44Z    INFO    [vulndb] Need to update DB
2025-04-17T01:58:44Z    INFO    [vulndb] Downloading vulnerability DB...
2025-04-17T01:58:44Z    INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
23.28 MiB / 62.34 MiB [---------------------->_____________________________________] 37.35% ? p/s ?54.09 MiB / 62.34 MiB [-----------------------------------
2025-04-17T01:58:47Z    INFO    [vuln] Vulnerability scanning is enabled
2025-04-17T01:58:53Z    INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all affe
2025-04-17T01:58:53Z    INFO    Detected OS     family="debian" version="9.5"
2025-04-17T01:58:53Z    INFO    [debian] Detecting vulnerabilities...   os_version="9" pkg_num=86
2025-04-17T01:58:53Z    INFO    Number of language-specific files       num=1
2025-04-17T01:58:53Z    INFO    [python-pkg] Detecting vulnerabilities...
2025-04-17T01:58:53Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.61/docs/scanner/vulnerability#severity-se
2025-04-17T01:58:53Z    WARN    This OS version is no longer supported by the distribution      family="debian" version="9.5"
2025-04-17T01:58:53Z    WARN    The vulnerability detection may be insufficient because security updates are not provided
2025-04-17T01:58:53Z    INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

Report Summary

┌──────────────────────────────────────────────────────────────────────┬────────────┬─────────────────┐
│                                Target                                │    Type    │ Vulnerabilities │
├──────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┤
│ ***/order-api:1.0.0 (debian 9.5)                                     │   debian   │       108       │
├──────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┤
│ usr/local/lib/python3.7/site-packages/annotated_types-0.5.0.dist-info/METADATA   │ python-pkg │        0        │
├──────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┤
│ usr/local/lib/python3.7/site-packages/anyio-3.7.1.dist-info/METADATA             │ python-pkg │        0        │
```




```
***/order-api:1.0.0 (debian 9.5)
==========================================
Total: 108 (HIGH: 85, CRITICAL: 23)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2019-3462	HIGH	fixed	1.4.8	1.4.9	Incorrect sanitation of the 302 redirect field in transport metho https://avd.aquasec.com/nvd/cve-2019-3462
bsdutils	CVE-2016-2779		affected	1:2.29.2-1+deb9u1		util-linux: runuser tty hijack via TIOCSTI ioctl https://avd.aquasec.com/nvd/cve-2016-2779
dpkg	CVE-2022-1664	CRITICAL	fixed	1.18.25	1.18.26	Dpkg::Source::Archive in dpkg, the Debian package system, b ... https://avd.aquasec.com/nvd/cve-2022-1664
e2fslibs	CVE-2022-1304	HIGH	affected	1.43.4-2		e2fsprogs: out-of-bounds read/write via crafted f https://avd.aquasec.com/nvd/cve-2022-1304
e2fsprogs						
gcc-6-base	CVE-2018-12886		will_not_fix	6.3.0-18+deb9u1		gcc: spilling of stack protection address in cfg function.c leads to... https://avd.aquasec.com/nvd/cve-2018-12886
gpgv	CVE-2018-1000858		affected	2.1.18-8~deb9u2		gnupg2: Cross site request forgery in dirmngr re an information disclosure... https://avd.aquasec.com/nvd/cve-2018-1000858
gzip	CVE-2022-1271		fixed	1.6-5+b1	1.6-5+deb9u1	gzip: arbitrary-file-write vulnerability https://avd.aquasec.com/nvd/cve-2022-1271
libapt-pkg5.0	CVE-2019-3462			1.4.8	1.4.9	Incorrect sanitation of the 302 redirect field i

Pipelines - Run 20250417.19 log

dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=f528a064-544a-5ca4-c3db-bebbc66114bd&t=9373f12f-98b4-5ed6-8c34-c08256cd4401

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

- Build & scan the c... 1m 18s
  - Initialize job 2s
  - Checkout DevSecOps... 1s
  - Build order-api cont... 20s
  - Download Trivy v0.61... 3s
  - Scan the order-api co... 9s
  - Scan the order-api ... <1s
  - Push order-api contai... 4s
  - Attach the scan res... 16s
  - List attached artifacts... 6s
  - Create a SBOM doc... <1s
  - Attach the SBOM do... 5s
  - List attached artifacts... 6s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s

Scan the order-api container image for vulnerabilities

View raw log

```
1  Starting: Scan the order-api container image for vulnerabilities
2  ==============================================================================
3  Task         : Bash
4  Description  : Run a Bash script on macOS, Linux, or Windows
5  Version      : 3.250.1
6  Author       : Microsoft Corporation
7  Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/bash
8  ==============================================================================
9  Generating script.
10 Script contents:
11 trivy image --exit-code 0 --severity HIGH,CRITICAL --security-checks vuln --format sarif --output ./trivy-sarif.json ***/order-api:1.0.0
12 ========================== Starting Command Output ===========================
13 /usr/bin/bash /home/vsts/work/_temp/20ee3dc8-6e13-47a7-9895-a55d1bcc701c.sh
14 2025-04-17T01:58:54Z    WARN    '--security-checks' is deprecated. Use '--scanners' instead.
15 2025-04-17T01:58:54Z    INFO    [vuln] Vulnerability scanning is enabled
16 2025-04-17T01:58:54Z    INFO    Detected OS     family="debian" version="9.5"
17 2025-04-17T01:58:54Z    INFO    [debian] Detecting vulnerabilities...   os_version="9" pkg_num=86
18 2025-04-17T01:58:54Z    INFO    Number of language-specific files       num=1
19 2025-04-17T01:58:54Z    INFO    [python-pkg] Detecting vulnerabilities...
20 2025-04-17T01:58:54Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.61/docs/scanner/vulnerability#severity-select
21 2025-04-17T01:58:54Z    WARN    This OS version is no longer supported by the distribution      family="debian" version="9.5"
22 2025-04-17T01:58:54Z    WARN    The vulnerability detection may be insufficient because security updates are not provided
23
24 Finishing: Scan the order-api container image for vulnerabilities
```

Pipelines - Run 20250417.19 log

dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=f528a064-544a-5ca4-c3db-bebbc66114bd&t=6ff500d3-3fc5-54ed-71bb-26614be3e02f

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

Build & scan the c...	1m 18s
Initialize job	2s
Checkout DevSecOps...	1s
Build order-api cont...	20s
Download Trivy v0.61...	3s
Scan the order-api co...	9s
Scan the order-api ...	<1s
Push order-api contai...	4s
Attach the scan res...	16s
List attached artifacts...	6s
Create a SBOM doc...	<1s
Attach the SBOM do...	5s
List attached artifacts...	6s
Post-job: Checkout ...	<1s
Finalize Job	<1s

Sign Artifacts

Sign container artifacts	49s
Initialize job	1s

Attach the scan result to the order-api container image

View raw log

```
26  Python (Linux) 3.12.8 (main, Mar 25 2025, 10:54:53) [GCC 11.4.0]
27
28  Legal docs and information: aka.ms/AzureCliLegal
29
30
31  Your CLI is up-to-date.
32  Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
33  Setting active cloud to: AzureCloud
34  /usr/bin/az cloud set -n AzureCloud
35  /usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
36  [
37    {
38      "cloudName": "AzureCloud",
39      "homeTenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
40      "id": "2638031b-e819-4081-bacf-43f23a07121c",
41      "isDefault": true,
42      "managedByTenants": [],
43      "name": "Visual Studio Enterprise Subscription",
44      "state": "Enabled",
45      "tenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
46      "user": {
47        "name": "***",
48        "type": "servicePrincipal"
49      }
50    }
51  ]
52  /usr/bin/az account set --subscription 2638031b-e819-4081-bacf-43f23a07121c
53  /usr/bin/bash /home/vsts/work/_temp/azureclitaskscript1744855139265.sh
54  WARNING: The output will be changed in next breaking change release(2.73.0) scheduled for May 2025. Exit code will be 1 if command fails for docker login.
55  Login Succeeded
56  Uploading cf5175f6e00a trivy-sarif.json
57  Uploaded  cf5175f6e00a trivy-sarif.json
58  Attached to [registry] ***/order-api@sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
59  Digest: sha256:190552af1511b4ee80a1719dd29a03b7820aba6a892639469fc77f7bc5d37d4f
60
61  /usr/bin/az account clear
62  Finishing: Attach the scan result to the order-api container image
```

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

- Build & scan the c... 1m 18s
  - Initialize job 2s
  - Checkout DevSecOps... 1s
  - Build order-api cont... 20s
  - Download Trivy v0.61... 3s
  - Scan the order-api co... 9s
  - Scan the order-api ... <1s
  - Push order-api contai... 4s
  - Attach the scan res... 16s
  - List attached artifacts... 6s
  - Create a SBOM doc... <1s
  - Attach the SBOM do... 5s
  - List attached artifacts... 6s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s

Create a SBOM document for the order-api container image

View raw log

```
1  Starting: Create a SBOM document for the order-api container image
2  ==============================================================================
3  Task         : Bash
4  Description  : Run a Bash script on macOS, Linux, or Windows
5  Version      : 3.250.1
6  Author       : Microsoft Corporation
7  Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/bash
8  ==============================================================================
9  Generating script.
10 Script contents:
11 trivy image --format spdx --output ./sbom.spdx.json ***/order-api:1.0.0
12 ========================== Starting Command Output ===========================
13 /usr/bin/bash /home/vsts/work/_temp/5977106b-6aaf-43c9-9d30-09c4664c9904.sh
14 2025-04-17T01:59:22Z    INFO    "--format spdx" disables security scanning. Specify "--scanners vuln" explicitly if you want to include vulnerabilities in the "spdx"
15 2025-04-17T01:59:22Z    INFO    Detected OS     family="debian" version="9.5"
16 2025-04-17T01:59:22Z    INFO    Number of language-specific files       num=1
17
18 Finishing: Create a SBOM document for the order-api container image
```

Pipelines - Run 20250417.19 log

dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=f528a064-544a-5ca4-c3db-bebbc66114bd&t=bff80307-5bd6-5560-8f0e-a3a4175bfdf1

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

DevSecOps

Build & Scan Stage

- Build & scan the c... 1m 18s
  - Initialize job 2s
  - Checkout DevSecOps... 1s
  - Build order-api cont... 20s
  - Download Trivy v0.61... 3s
  - Scan the order-api co... 9s
  - Scan the order-api ... <1s
  - Push order-api contai... 4s
  - Attach the scan res... 16s
  - List attached artifacts... 6s
  - Create a SBOM doc... <1s
  - Attach the SBOM do... 5s
  - List attached artifacts... 6s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

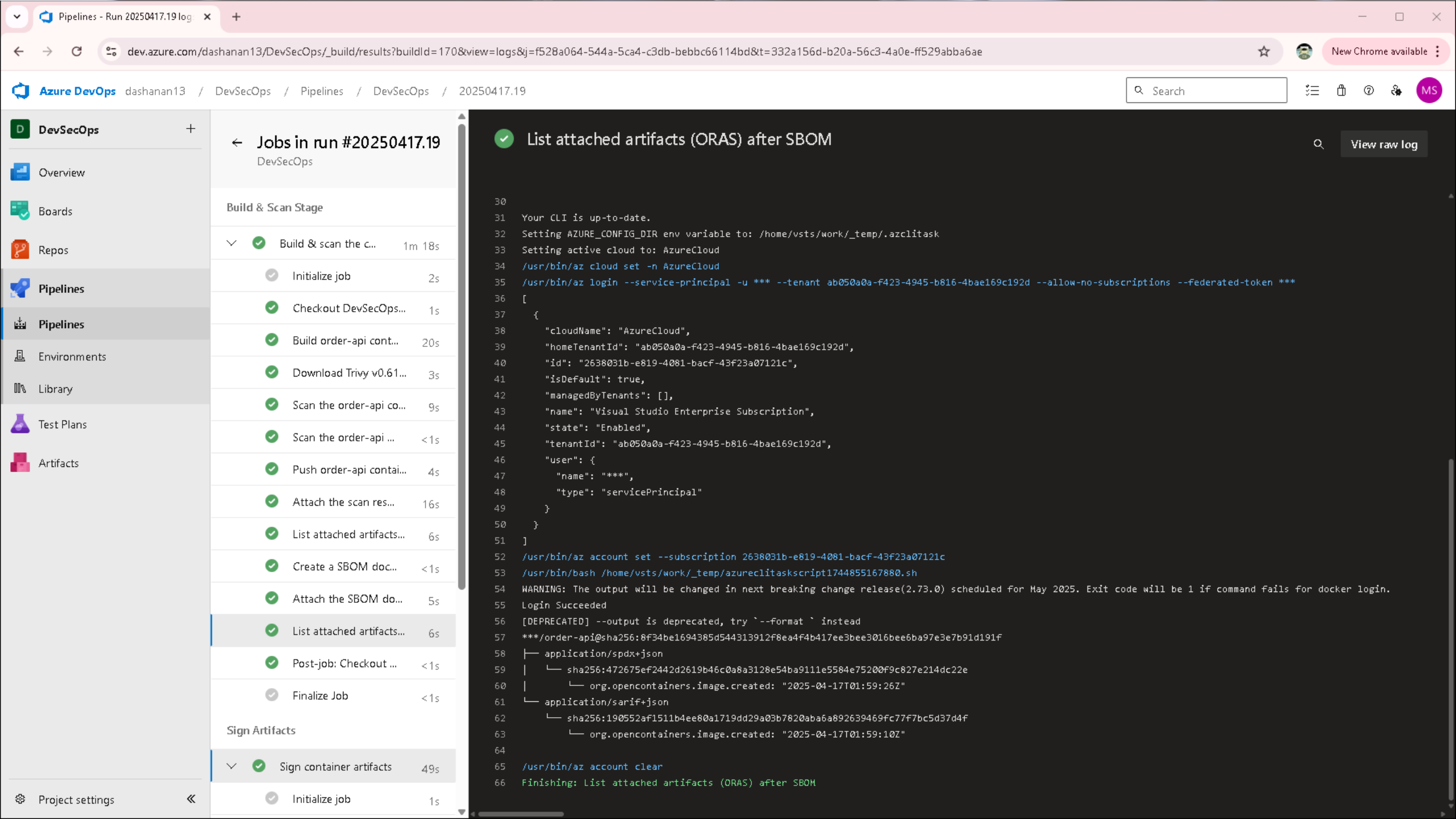
Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s

Attach the SBOM document to the order-api container image

View raw log

```
Extensions directory '/opt/az/azcliextensions'

Python (Linux) 3.12.8 (main, Mar 25 2025, 10:54:53) [GCC 11.4.0]

Legal docs and information: aka.ms/AzureCliLegal


Your CLI is up-to-date.
Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
Setting active cloud to: AzureCloud
/usr/bin/az cloud set -n AzureCloud
/usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
    "id": "2638031b-e819-4081-bacf-43f23a07121c",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Visual Studio Enterprise Subscription",
    "state": "Enabled",
    "tenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
    "user": {
      "name": "***",
      "type": "servicePrincipal"
    }
  }
]
/usr/bin/az account set --subscription 2638031b-e819-4081-bacf-43f23a07121c
/usr/bin/bash /home/vsts/work/_temp/azureclitaskscript1744855162788.sh
Uploading 00e16a7eaf88 sbom.spdx.json
Uploaded  00e16a7eaf88 sbom.spdx.json
Attached to [registry] ***/order-api@sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
Digest: sha256:472675ef2442d2619b46c0a8a3128e54ba9111e5584e75200f9c827e214dc22e

/usr/bin/az account clear
Finishing: Attach the SBOM document to the order-api container image
```


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=f528a064-544a-5ca4-c3db-bebbc66114bd&t=332a156d-b20a-56c3-4a0e-ff529abba6ae
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
DevSecOps
Build & Scan Stage
Build & scan the c... 1m 18s
Initialize job 2s
Checkout DevSecOps... 1s
Build order-api cont... 20s
Download Trivy v0.61... 3s
Scan the order-api co... 9s
Scan the order-api ... <1s
Push order-api contai... 4s
Attach the scan res... 16s
List attached artifacts... 6s
Create a SBOM doc... <1s
Attach the SBOM do... 5s
List attached artifacts... 6s
Post-job: Checkout ... <1s
Finalize Job <1s
Sign Artifacts
Sign container artifacts 49s
Initialize job 1s
List attached artifacts (ORAS) after SBOM
View raw log
30
31 Your CLI is up-to-date.
32 Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
33 Setting active cloud to: AzureCloud
34 /usr/bin/az cloud set -n AzureCloud
35 /usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
36 [
37 {
38 "cloudName": "AzureCloud",
39 "homeTenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
40 "id": "2638031b-e819-4081-bacf-43f23a07121c",
41 "isDefault": true,
42 "managedByTenants": [],
43 "name": "Visual Studio Enterprise Subscription",
44 "state": "Enabled",
45 "tenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
46 "user": {
47 "name": "***",
48 "type": "servicePrincipal"
49 }
50 }
51]
52 /usr/bin/az account set --subscription 2638031b-e819-4081-bacf-43f23a07121c
53 /usr/bin/bash /home/vsts/work/_temp/azureclitaskscript1744855167880.sh
54 WARNING: The output will be changed in next breaking change release(2.73.0) scheduled for May 2025. Exit code will be 1 if command fails for docker login.
55 Login Succeeded
56 [DEPRECATED] --output is deprecated, try `--format ` instead
57 ***/order-api@sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
58 ├── application/spdx+json
59 │ └── sha256:472675ef2442d2619b46c0a8a3128e54ba9111e5584e75200f9c827e214dc22e
60 │ └── org.opencontainers.image.created: "2025-04-17T01:59:26Z"
61 └── application/sarif+json
62 └── sha256:190552af1511b4ee80a1719dd29a03b7820aba6a892639469fc77f7bc5d37d4f
63 └── org.opencontainers.image.created: "2025-04-17T01:59:10Z"
64
65 /usr/bin/az account clear
66 Finishing: List attached artifacts (ORAS) after SBOM

qwerty | Repositories

Container registry

Search

Microsoft Defender for Cloud
Properties
Locks
Services
Repositories
Webhooks
Geo-replications
Tasks
Connected registries (Preview)
Cache
Repository permissions
Policies
Content trust
Retention (Preview)
Monitoring
Automation
Help

Refresh

Search to filter repositories ...

Repositories

order-api

order-api

Repository

Refresh | Start artifact streaming | Manage deleted artifacts | Delete repository

Essentials

Repository
order-api

Tag count
4

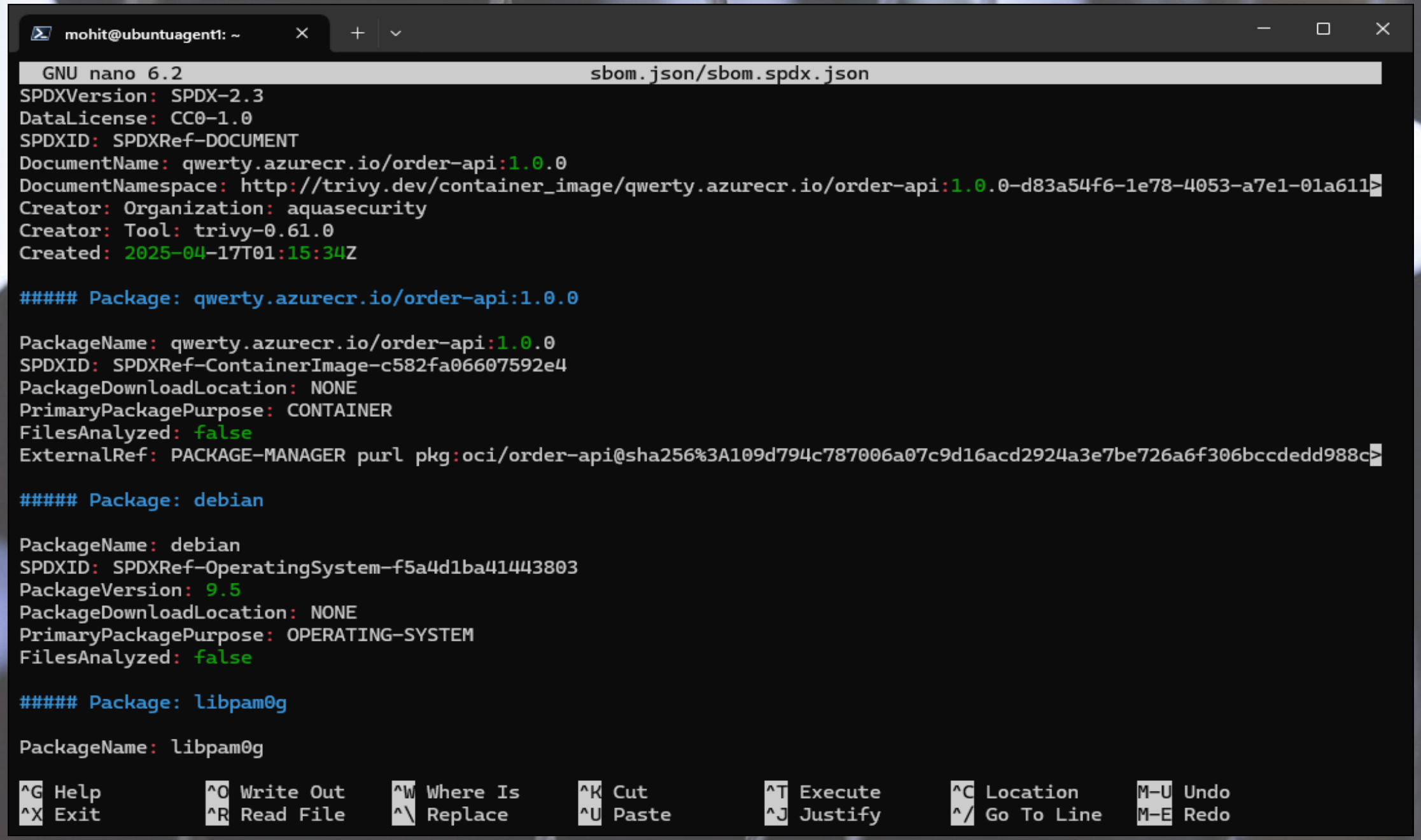
Last updated date
4/17/2025, 4:00 AM GMT+2

Manifest count
12

Search to filter tags ...

Tags	Digest	Last modified
sha256-472675ef2442d2619b46c0a8a...	sha256:e5572c134bb9c563fb7eef55c2...	4/17/2025, 4:00 AM GMT+2
sha256-190552af1511b4ee80a1719dd...	sha256:357affd16d399003d3da21b66...	4/17/2025, 4:00 AM GMT+2
sha256-8f34be1694385d544313912f8...	sha256:fa8831c467a5665e7d5dc7bd5...	4/17/2025, 4:00 AM GMT+2
1.0.0	sha256:8f34be1694385d544313912f8e...	4/17/2025, 3:58 AM GMT+2

```
mohit@ubuntuagent1:~$ ls
CybersecurityPractitionerMeetup  demo-llm-exploit  get-docker.sh  myagent  snap  vsts-agent-linux-x64-3.232.3.tar.gz
mohit@ubuntuagent1:~$ oras login qwerty.azurecr.io -u "qwerty" -p $(az acr credential show --name qwerty --query "passwords[0].value" -o
 tsv)
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
Login Succeeded
mohit@ubuntuagent1:~$ oras pull qwerty.azurecr.io/order-api@$SBOM_DIGEST   --output sbom.json
✓ Pulled      sbom.spdx.json                                                    77.4/77.4 kB 100.00%    3ms
  └─ sha256:fcd268f0aa7a4bbb4753dd31b293b531644dc51709afefbab47608e3fcd70bfc
✓ Pulled      application/vnd.oci.image.manifest.v1+json                          734/734  B 100.00%  197µs
  └─ sha256:4542c38ef5f985610ec8be502643b78619995cf37885221a6b91e4973440ac28
Pulled [registry] qwerty.azurecr.io/order-api@sha256:4542c38ef5f985610ec8be502643b78619995cf37885221a6b91e4973440ac28
Digest: sha256:4542c38ef5f985610ec8be502643b78619995cf37885221a6b91e4973440ac28
mohit@ubuntuagent1:~$ oras pull qwerty.azurecr.io/order-api@$S^C
mohit@ubuntuagent1:~$ ls sbom.json/
sbom.spdx.json
mohit@ubuntuagent1:~$ nano sbom.json/sbom.spdx.json
```


mohit@ubuntuagent1: ~
GNU nano 6.2 sbom.json/sbom.spdx.json
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: qwerty.azurecr.io/order-api:1.0.0
DocumentNamespace: http://trivy.dev/container_image/qwerty.azurecr.io/order-api:1.0.0-d83a54f6-1e78-4053-a7e1-01a611>
Creator: Organization: aquasecurity
Creator: Tool: trivy-0.61.0
Created: 2025-04-17T01:15:34Z
Package: qwerty.azurecr.io/order-api:1.0.0
PackageName: qwerty.azurecr.io/order-api:1.0.0
SPDXID: SPDXRef-ContainerImage-c582fa06607592e4
PackageDownloadLocation: NONE
PrimaryPackagePurpose: CONTAINER
FilesAnalyzed: false
ExternalRef: PACKAGE-MANAGER purl pkg:oci/order-api@sha256%3A109d794c787006a07c9d16acd2924a3e7be726a6f306bccdedd988c>
Package: debian
PackageName: debian
SPDXID: SPDXRef-OperatingSystem-f5a4d1ba41443803
PackageVersion: 9.5
PackageDownloadLocation: NONE
PrimaryPackagePurpose: OPERATING-SYSTEM
FilesAnalyzed: false
Package: libpam0g
PackageName: libpam0g
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

- Attach the scan res... 16s
- List attached artifacts... 6s
- Create a SBOM doc... <1s
- Attach the SBOM do... 5s
- List attached artifacts... 6s
- Post-job: Checkout ... <1s
- Finalize Job <1s

Sign Artifacts

- Sign container artifacts 49s
  - Initialize job 1s
  - Checkout DevSecOps... 2s
  - Download & Prepare ... 2s
  - Sign the order-api c... 27s
  - Sign the order-api co... 6s
  - Sign the order-api co... 5s
  - PublishPipelineArtifact 3s
  - Post-job: Checkout ... <1s
  - Finalize Job <1s

Deploy to Dev

- Verify Artifacts 1m 7s

List attached artifacts (ORAS) after SBOM

View raw log

```
30
31  Your CLI is up-to-date.
32  Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
33  Setting active cloud to: AzureCloud
34  /usr/bin/az cloud set -n AzureCloud
35  /usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
36  [
37    {
38      "cloudName": "AzureCloud",
39      "homeTenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
40      "id": "2638031b-e819-4081-bacf-43f23a07121c",
41      "isDefault": true,
42      "managedByTenants": [],
43      "name": "Visual Studio Enterprise Subscription",
44      "state": "Enabled",
45      "tenantId": "ab050a0a-f423-4945-b816-4bae169c192d",
46      "user": {
47        "name": "***",
48        "type": "servicePrincipal"
49      }
50    }
51  ]
52  /usr/bin/az account set --subscription 2638031b-e819-4081-bacf-43f23a07121c
53  /usr/bin/bash /home/vsts/work/_temp/azureclitaskscript1744855167880.sh
54  WARNING: The output will be changed in next breaking change release(2.73.0) scheduled for May 2025. Exit code will be 1 if command fails for docker login.
55  Login Succeeded
56  [DEPRECATED] --output is deprecated, try `--format ` instead
57  ***/order-api@sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
58  ├── application/spdx+json
59  │   └── sha256:472675ef2442d2619b46c0a8a3128e54ba9111e5584e75200f9c827e214dc22e
60  │       └── org.opencontainers.image.created: "2025-04-17T01:59:26Z"
61  └── application/sarif+json
62      └── sha256:190552af1511b4ee80a1719dd29a03b7820aba6a892639469fc77f7bc5d37d4f
63          └── org.opencontainers.image.created: "2025-04-17T01:59:10Z"
64
65  /usr/bin/az account clear
66  Finishing: List attached artifacts (ORAS) after SBOM
```

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

Attach the scan res... 16s

List attached artifacts... 6s

Create a SBOM doc... <1s

Attach the SBOM do... 5s

List attached artifacts... 6s

Post-job: Checkout ... <1s

Finalize Job <1s

Sign Artifacts

Sign container artifacts 49s

Initialize job 1s

Checkout DevSecOps... 2s

Download & Prepare ... 2s

Sign the order-api c... 27s

Sign the order-api co... 6s

Sign the order-api co... 5s

PublishPipelineArtifact 3s

Post-job: Checkout ... <1s

Finalize Job <1s

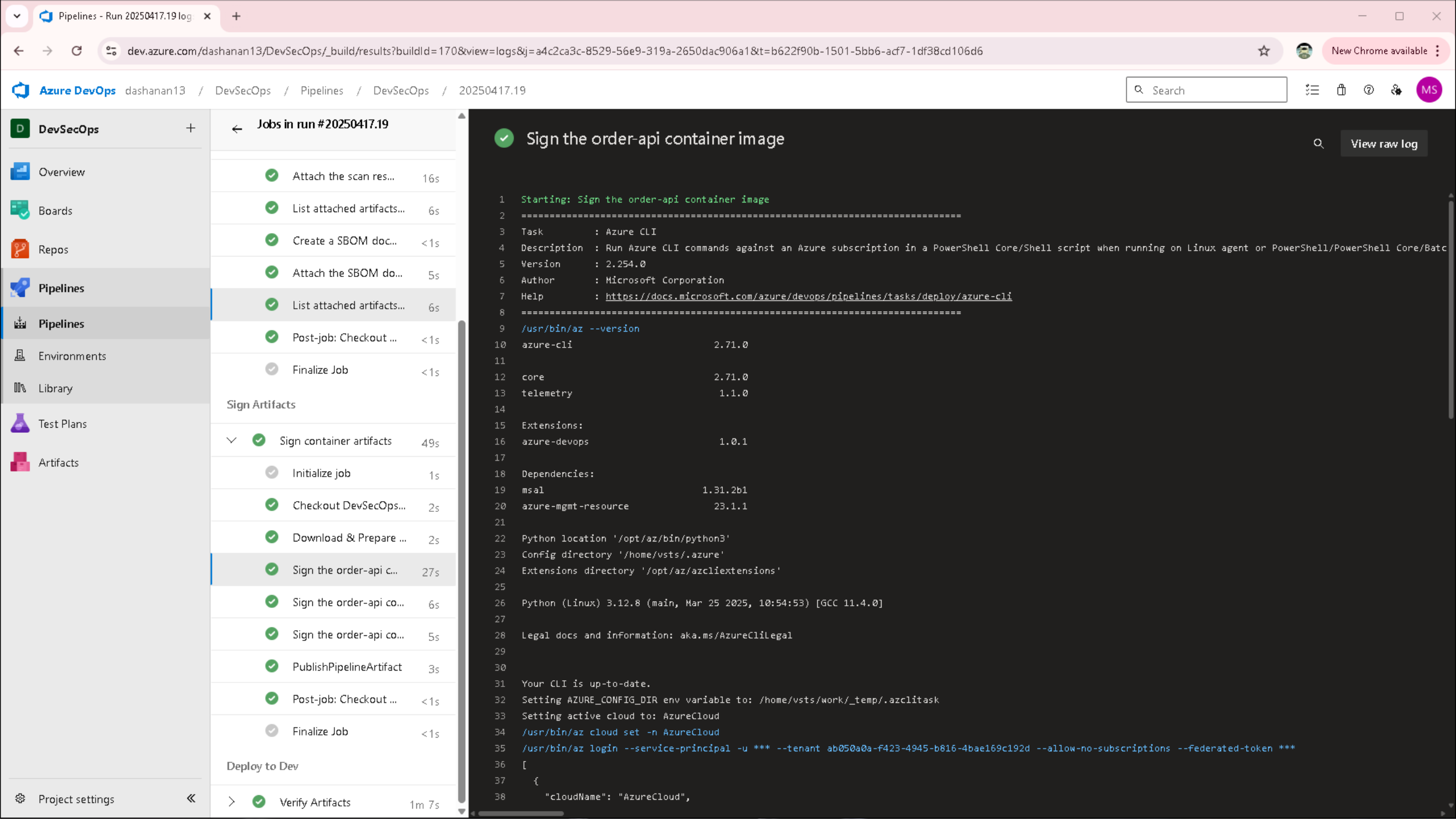
Deploy to Dev

Verify Artifacts 1m 7s

Download & Prepare Notation v1.3.0

View raw log

```
1  Starting: Download & Prepare Notation v1.3.0
2  ==============================================================================
3  Task         : Bash
4  Description  : Run a Bash script on macOS, Linux, or Windows
5  Version      : 3.250.1
6  Author       : Microsoft Corporation
7  Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/bash
8  ==============================================================================
9  Generating script.
10 ========================== Starting Command Output ===========================
11 /usr/bin/bash /home/vsts/work/_temp/6ffba494-d457-46a2-a273-13d4c7a50eda.sh
12 --2025-04-17 01:59:52--  https://github.com/notaryproject/notation/releases/download/v1.3.0/notation_1.3.0_linux_amd64.tar.gz
13 Resolving github.com (github.com)... 4.208.26.197
14 Connecting to github.com (github.com)|4.208.26.197|:443... connected.
15 HTTP request sent, awaiting response... 302 Found
16 Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/257347648/775e0dd6-ce85-4b68-857d-5807ea3e9269?X-Amz-Algorithm=AWS4-HMAC-SHA2
17 --2025-04-17 01:59:52--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/257347648/775e0dd6-ce85-4b68-857d-5807ea3e9269?X-Amz-Algorithm
18 Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.111.133, ...
19 Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connected.
20 HTTP request sent, awaiting response... 200 OK
21 Length: 4145991 (4.0M) [application/octet-stream]
22 Saving to: 'notation_1.3.0_linux_amd64.tar.gz'
23
24      0K .......... .......... .......... .......... ..........  1% 4.56M 1s
25     50K .......... .......... .......... .......... ..........  2% 9.80M 1s
26    100K .......... .......... .......... .......... ..........  3% 8.08M 1s
27    150K .......... .......... .......... .......... ..........  4% 25.2M 0s
28    200K .......... .......... .......... .......... ..........  6% 23.9M 0s
29    250K .......... .......... .......... .......... ..........  7% 9.23M 0s
30    300K .......... .......... .......... .......... ..........  8% 46.1M 0s
31    350K .......... .......... .......... .......... ..........  9% 31.4M 0s
32    400K .......... .......... .......... .......... .......... 11% 98.6M 0s
33    450K .......... .......... .......... .......... .......... 12% 29.9M 0s
34    500K .......... .......... .......... .......... .......... 13% 10.4M 0s
35    550K .......... .......... .......... .......... .......... 14%  146M 0s
36    600K .......... .......... .......... .......... .......... 16% 77.9M 0s
37    650K .......... .......... .......... .......... .......... 17% 42.8M 0s
38    700K .......... .......... .......... .......... .......... 18% 61.4M 0s
```


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=a4c2ca3c-8529-56e9-319a-2650dac906a1&t=b622f90b-1501-5bb6-acf7-1df38cd106d6
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
Attach the scan res... 16s
List attached artifacts... 6s
Create a SBOM doc... <1s
Attach the SBOM do... 5s
List attached artifacts... 6s
Post-job: Checkout ... <1s
Finalize Job <1s
Sign Artifacts
Sign container artifacts 49s
Initialize job 1s
Checkout DevSecOps... 2s
Download & Prepare ... 2s
Sign the order-api c... 27s
Sign the order-api co... 6s
Sign the order-api co... 5s
PublishPipelineArtifact 3s
Post-job: Checkout ... <1s
Finalize Job <1s
Deploy to Dev
Verify Artifacts 1m 7s
Sign the order-api container image
View raw log
1 Starting: Sign the order-api container image
2 ==
3 Task : Azure CLI
4 Description : Run Azure CLI commands against an Azure subscription in a PowerShell Core/Shell script when running on Linux agent or PowerShell/PowerShell Core/Batc
5 Version : 2.254.0
6 Author : Microsoft Corporation
7 Help : https://docs.microsoft.com/azure/devops/pipelines/tasks/deploy/azure-cli
8 ==
9 /usr/bin/az --version
10 azure-cli 2.71.0
11
12 core 2.71.0
13 telemetry 1.1.0
14
15 Extensions:
16 azure-devops 1.0.1
17
18 Dependencies:
19 msal 1.31.2b1
20 azure-mgmt-resource 23.1.1
21
22 Python location '/opt/az/bin/python3'
23 Config directory '/home/vsts/.azure'
24 Extensions directory '/opt/az/azcliextensions'
25
26 Python (Linux) 3.12.8 (main, Mar 25 2025, 10:54:53) [GCC 11.4.0]
27
28 Legal docs and information: aka.ms/AzureCliLegal
29
30
31 Your CLI is up-to-date.
32 Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
33 Setting active cloud to: AzureCloud
34 /usr/bin/az cloud set -n AzureCloud
35 /usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
36 [
37 {
38 "cloudName": "AzureCloud",

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

Jobs in run #20250417.19

Attach the scan res... 16s

List attached artifacts... 6s

Create a SBOM doc... <1s

Attach the SBOM do... 5s

List attached artifacts... 6s

Post-job: Checkout ... <1s

Finalize Job <1s

Sign Artifacts

Sign container artifacts 49s

Initialize job 1s

Checkout DevSecOps... 2s

Download & Prepare ... 2s

Sign the order-api c... 27s

Sign the order-api co... 6s

Sign the order-api co... 5s

PublishPipelineArtifact 3s

Post-job: Checkout ... <1s

Finalize Job <1s

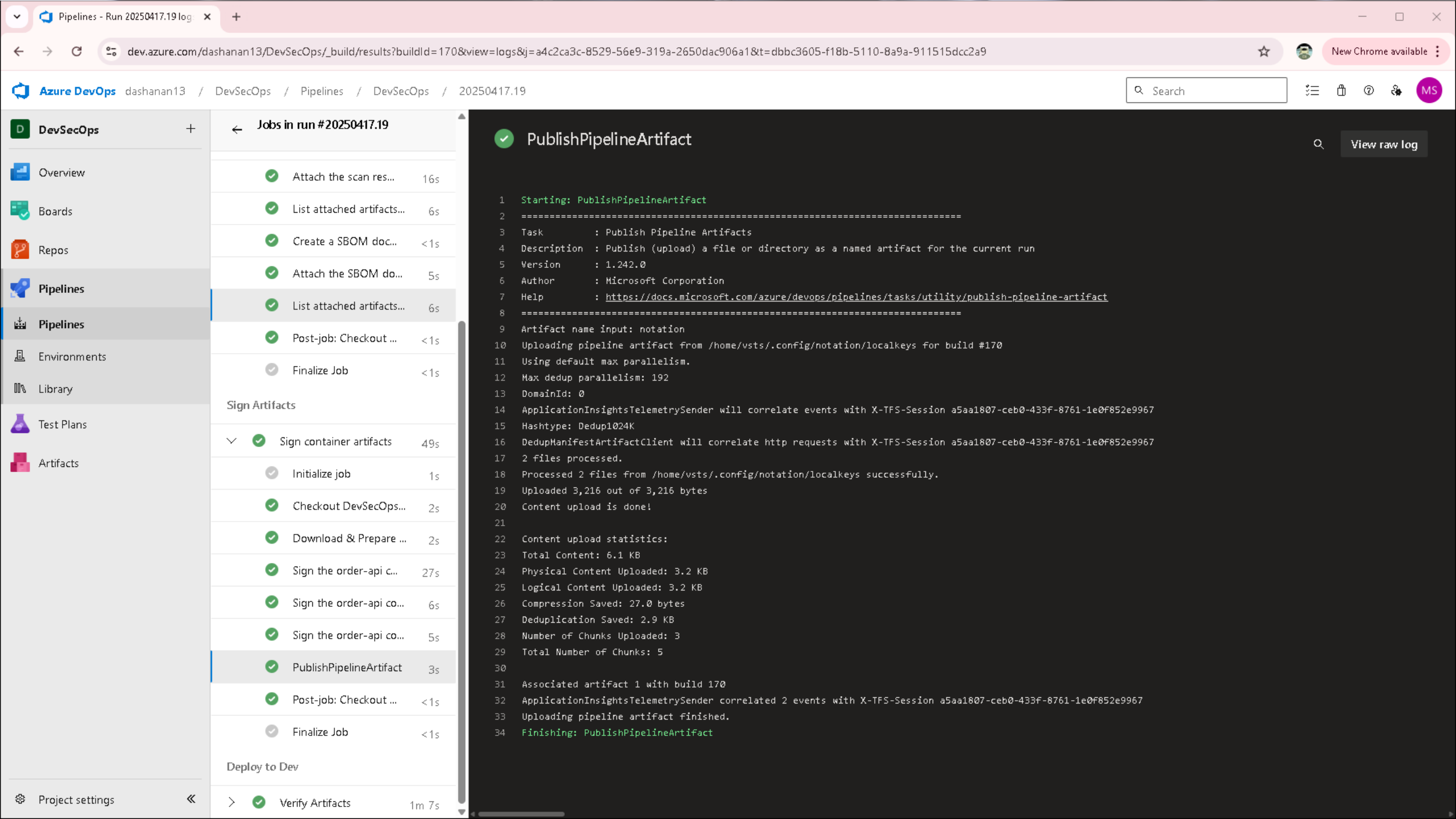
Deploy to Dev

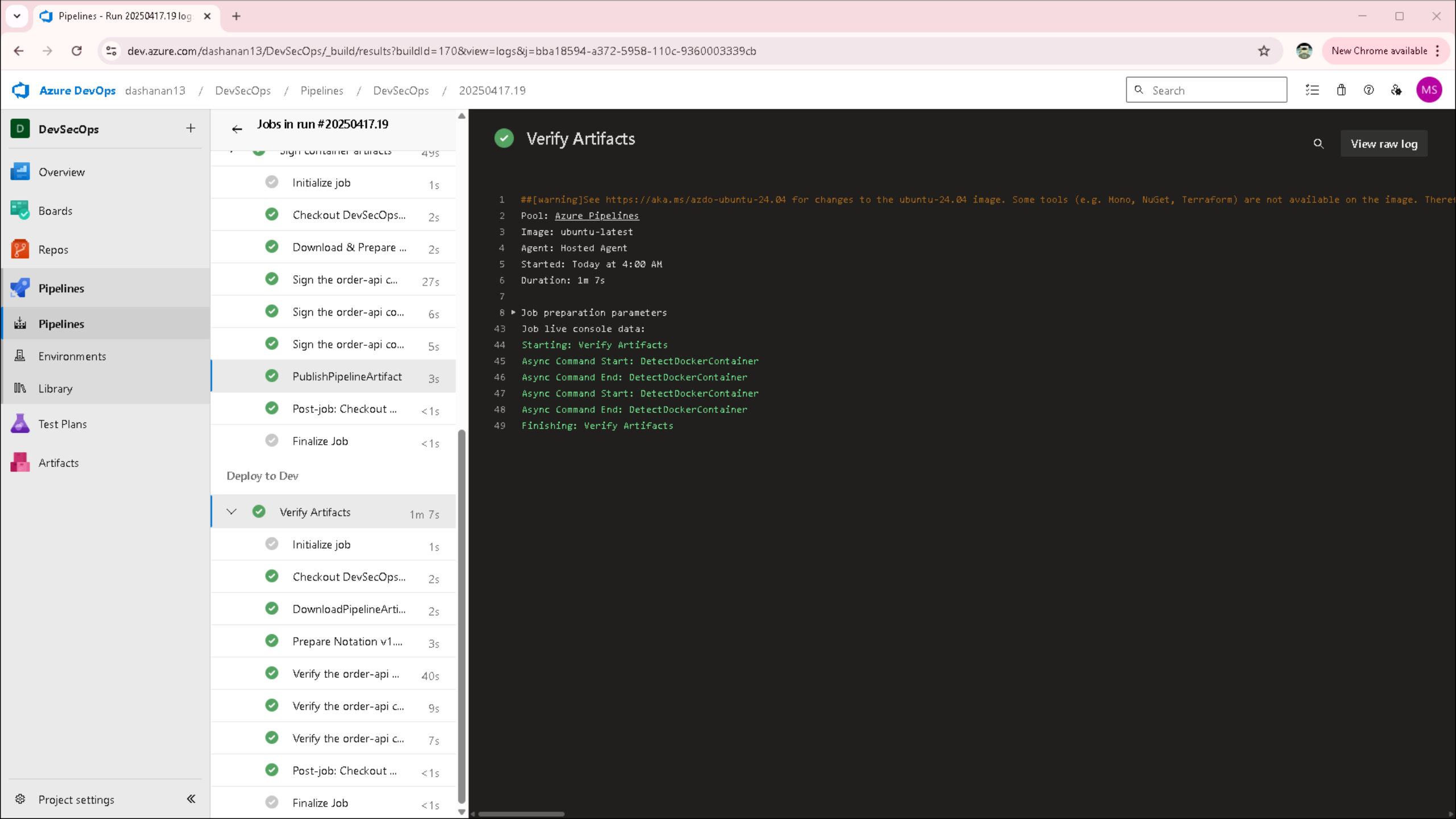
Verify Artifacts 1m 7s

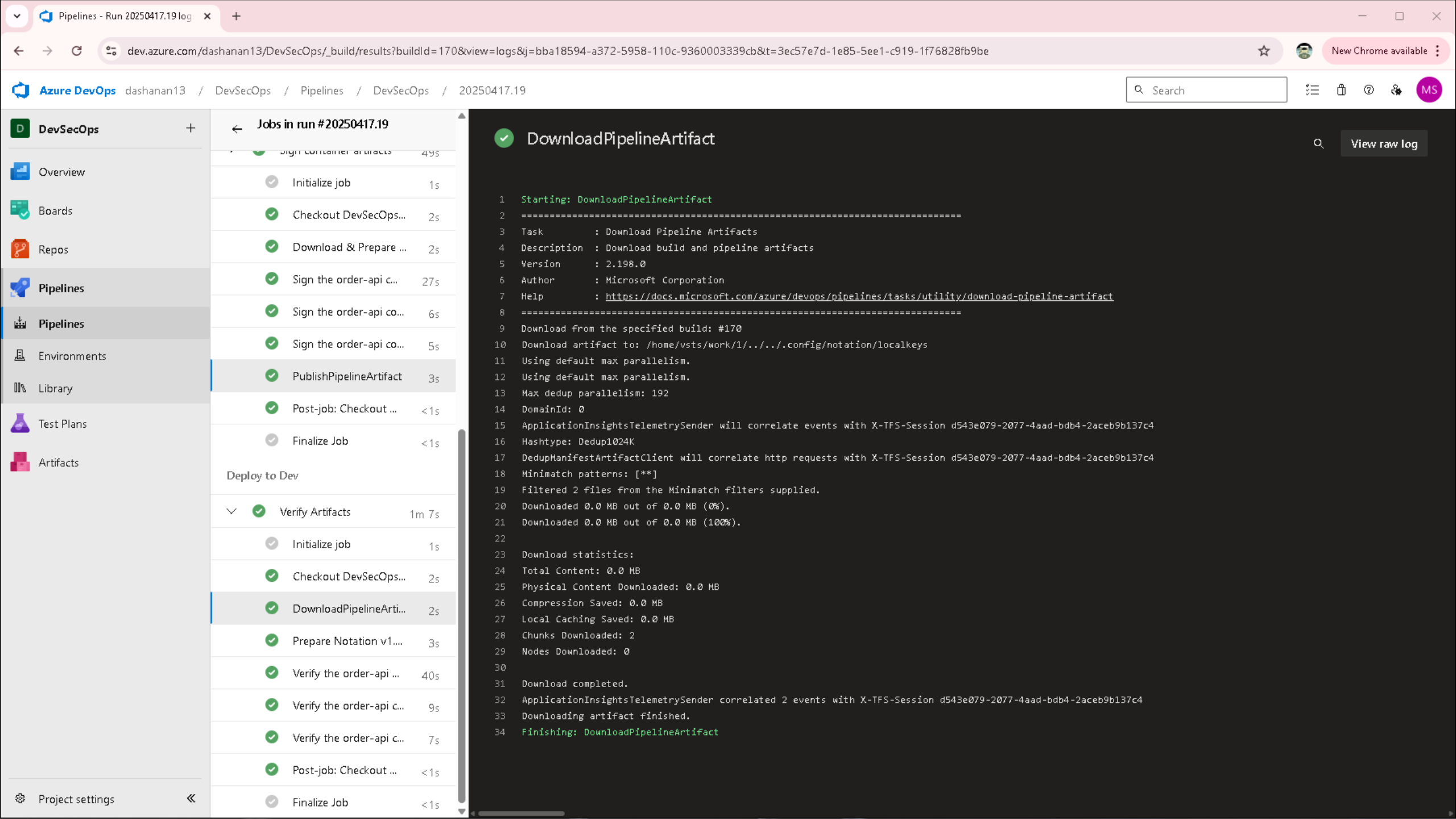
Sign the order-api container SBOM document

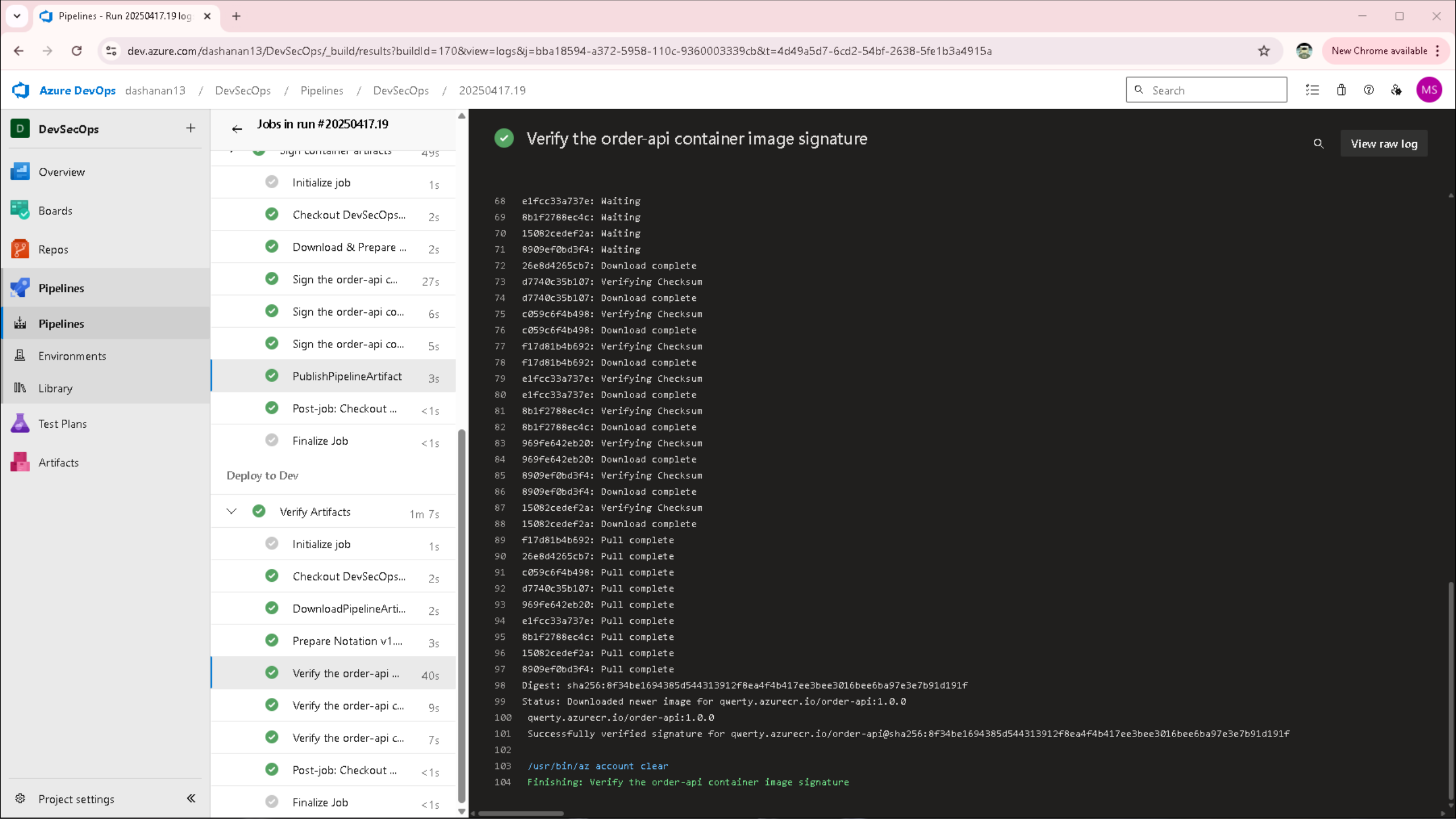
View raw log

```
Starting: Sign the order-api container SBOM document
==============================================================================
Task         : Azure CLI
Description  : Run Azure CLI commands against an Azure subscription in a PowerShell Core/Shell script when running on Linux agent or PowerShell/PowerShell Core/Batc
Version      : 2.254.0
Author       : Microsoft Corporation
Help         : https://docs.microsoft.com/azure/devops/pipelines/tasks/deploy/azure-cli
==============================================================================
/usr/bin/az --version
azure-cli                         2.71.0

core                              2.71.0
telemetry                          1.1.0

Extensions:
azure-devops                       1.0.1

Dependencies:
msal                            1.31.2b1
azure-mgmt-resource               23.1.1

Python location '/opt/az/bin/python3'
Config directory '/home/vsts/.azure'
Extensions directory '/opt/az/azcliextensions'

Python (Linux) 3.12.8 (main, Mar 25 2025, 10:54:53) [GCC 11.4.0]

Legal docs and information: aka.ms/AzureCliLegal


Your CLI is up-to-date.
Setting AZURE_CONFIG_DIR env variable to: /home/vsts/work/_temp/.azclitask
Setting active cloud to: AzureCloud
/usr/bin/az cloud set -n AzureCloud
/usr/bin/az login --service-principal -u *** --tenant ab050a0a-f423-4945-b816-4bae169c192d --allow-no-subscriptions --federated-token ***
[
  {
    "cloudName": "AzureCloud",
```


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=a4c2ca3c-8529-56e9-319a-2650dac906a1&t=dbbc3605-f18b-5110-8a9a-911515dcc2a9
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
Attach the scan res... 16s
List attached artifacts... 6s
Create a SBOM doc... <1s
Attach the SBOM do... 5s
List attached artifacts... 6s
Post-job: Checkout ... <1s
Finalize Job <1s
Sign Artifacts
Sign container artifacts 49s
Initialize job 1s
Checkout DevSecOps... 2s
Download & Prepare ... 2s
Sign the order-api c... 27s
Sign the order-api co... 6s
Sign the order-api co... 5s
PublishPipelineArtifact 3s
Post-job: Checkout ... <1s
Finalize Job <1s
Deploy to Dev
Verify Artifacts 1m 7s
PublishPipelineArtifact
View raw log
1 Starting: PublishPipelineArtifact
2 ==
3 Task : Publish Pipeline Artifacts
4 Description : Publish (upload) a file or directory as a named artifact for the current run
5 Version : 1.242.0
6 Author : Microsoft Corporation
7 Help : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/publish-pipeline-artifact
8 ==
9 Artifact name input: notation
10 Uploading pipeline artifact from /home/vsts/.config/notation/localkeys for build #170
11 Using default max parallelism.
12 Max dedup parallelism: 192
13 DomainId: 0
14 ApplicationInsightsTelemetrySender will correlate events with X-TFS-Session a5aa1807-ceb0-433f-8761-1e0f852e9967
15 Hashtype: Dedup1024K
16 DedupManifestArtifactClient will correlate http requests with X-TFS-Session a5aa1807-ceb0-433f-8761-1e0f852e9967
17 2 files processed.
18 Processed 2 files from /home/vsts/.config/notation/localkeys successfully.
19 Uploaded 3,216 out of 3,216 bytes
20 Content upload is done!
21
22 Content upload statistics:
23 Total Content: 6.1 KB
24 Physical Content Uploaded: 3.2 KB
25 Logical Content Uploaded: 3.2 KB
26 Compression Saved: 27.0 bytes
27 Deduplication Saved: 2.9 KB
28 Number of Chunks Uploaded: 3
29 Total Number of Chunks: 5
30
31 Associated artifact 1 with build 170
32 ApplicationInsightsTelemetrySender correlated 2 events with X-TFS-Session a5aa1807-ceb0-433f-8761-1e0f852e9967
33 Uploading pipeline artifact finished.
34 Finishing: PublishPipelineArtifact


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=bba18594-a372-5958-110c-9360003339cb
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
Initialize job 1s
Checkout DevSecOps... 2s
Download & Prepare ... 2s
Sign the order-api c... 27s
Sign the order-api co... 6s
Sign the order-api co... 5s
PublishPipelineArtifact 3s
Post-job: Checkout ... <1s
Finalize Job <1s
Deploy to Dev
Verify Artifacts 1m 7s
Initialize job 1s
Checkout DevSecOps... 2s
DownloadPipelineArti... 2s
Prepare Notation v1.... 3s
Verify the order-api ... 40s
Verify the order-api c... 9s
Verify the order-api c... 7s
Post-job: Checkout ... <1s
Finalize Job <1s
Verify Artifacts
View raw log
1 ##[warning]See https://aka.ms/azdo-ubuntu-24.04 for changes to the ubuntu-24.04 image. Some tools (e.g. Mono, NuGet, Terraform) are not available on the image. There
2 Pool: Azure Pipelines
3 Image: ubuntu-latest
4 Agent: Hosted Agent
5 Started: Today at 4:00 AM
6 Duration: 1m 7s
7
8 ▸ Job preparation parameters
43 Job live console data:
44 Starting: Verify Artifacts
45 Async Command Start: DetectDockerContainer
46 Async Command End: DetectDockerContainer
47 Async Command Start: DetectDockerContainer
48 Async Command End: DetectDockerContainer
49 Finishing: Verify Artifacts


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=bba18594-a372-5958-110c-9360003339cb&t=3ec57e7d-1e85-5ee1-c919-1f76828fb9be
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
Initialize job 1s
Checkout DevSecOps... 2s
Download & Prepare ... 2s
Sign the order-api c... 27s
Sign the order-api co... 6s
Sign the order-api co... 5s
PublishPipelineArtifact 3s
Post-job: Checkout ... <1s
Finalize Job <1s
Deploy to Dev
Verify Artifacts 1m 7s
Initialize job 1s
Checkout DevSecOps... 2s
DownloadPipelineArti... 2s
Prepare Notation v1.... 3s
Verify the order-api ... 40s
Verify the order-api c... 9s
Verify the order-api c... 7s
Post-job: Checkout ... <1s
Finalize Job <1s
DownloadPipelineArtifact
View raw log
1 Starting: DownloadPipelineArtifact
2 ==
3 Task : Download Pipeline Artifacts
4 Description : Download build and pipeline artifacts
5 Version : 2.198.0
6 Author : Microsoft Corporation
7 Help : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/download-pipeline-artifact
8 ==
9 Download from the specified build: #170
10 Download artifact to: /home/vsts/work/1/../../.config/notation/localkeys
11 Using default max parallelism.
12 Using default max parallelism.
13 Max dedup parallelism: 192
14 DomainId: 0
15 ApplicationInsightsTelemetrySender will correlate events with X-TFS-Session d543e079-2077-4aad-bdb4-2aceb9b137c4
16 Hashtype: Dedup1024K
17 DedupManifestArtifactClient will correlate http requests with X-TFS-Session d543e079-2077-4aad-bdb4-2aceb9b137c4
18 Minimatch patterns: [**]
19 Filtered 2 files from the Minimatch filters supplied.
20 Downloaded 0.0 MB out of 0.0 MB (0%).
21 Downloaded 0.0 MB out of 0.0 MB (100%).
22
23 Download statistics:
24 Total Content: 0.0 MB
25 Physical Content Downloaded: 0.0 MB
26 Compression Saved: 0.0 MB
27 Local Caching Saved: 0.0 MB
28 Chunks Downloaded: 2
29 Nodes Downloaded: 0
30
31 Download completed.
32 ApplicationInsightsTelemetrySender correlated 2 events with X-TFS-Session d543e079-2077-4aad-bdb4-2aceb9b137c4
33 Downloading artifact finished.
34 Finishing: DownloadPipelineArtifact


Pipelines - Run 20250417.19 log
dev.azure.com/dashanan13/DevSecOps/_build/results?buildId=170&view=logs&j=bba18594-a372-5958-110c-9360003339cb&t=4d49a5d7-6cd2-54bf-2638-5fe1b3a4915a
New Chrome available
Azure DevOps dashanan13 / DevSecOps / Pipelines / DevSecOps / 20250417.19
Search
MS
DevSecOps
Overview
Boards
Repos
Pipelines
Pipelines
Environments
Library
Test Plans
Artifacts
Project settings
Jobs in run #20250417.19
Initialize job 1s
Checkout DevSecOps... 2s
Download & Prepare ... 2s
Sign the order-api c... 27s
Sign the order-api co... 6s
Sign the order-api co... 5s
PublishPipelineArtifact 3s
Post-job: Checkout ... <1s
Finalize Job <1s
Deploy to Dev
Verify Artifacts 1m 7s
Initialize job 1s
Checkout DevSecOps... 2s
DownloadPipelineArti... 2s
Prepare Notation v1.... 3s
Verify the order-api ... 40s
Verify the order-api c... 9s
Verify the order-api c... 7s
Post-job: Checkout ... <1s
Finalize Job <1s
Verify the order-api container image signature
View raw log
68 e1fcc33a737e: Waiting
69 8b1f2788ec4c: Waiting
70 15082cedef2a: Waiting
71 8909ef0bd3f4: Waiting
72 26e8d4265cb7: Download complete
73 d7740c35b107: Verifying Checksum
74 d7740c35b107: Download complete
75 c059c6f4b498: Verifying Checksum
76 c059c6f4b498: Download complete
77 f17d81b4b692: Verifying Checksum
78 f17d81b4b692: Download complete
79 e1fcc33a737e: Verifying Checksum
80 e1fcc33a737e: Download complete
81 8b1f2788ec4c: Verifying Checksum
82 8b1f2788ec4c: Download complete
83 969fe642eb20: Verifying Checksum
84 969fe642eb20: Download complete
85 8909ef0bd3f4: Verifying Checksum
86 8909ef0bd3f4: Download complete
87 15082cedef2a: Verifying Checksum
88 15082cedef2a: Download complete
89 f17d81b4b692: Pull complete
90 26e8d4265cb7: Pull complete
91 c059c6f4b498: Pull complete
92 d7740c35b107: Pull complete
93 969fe642eb20: Pull complete
94 e1fcc33a737e: Pull complete
95 8b1f2788ec4c: Pull complete
96 15082cedef2a: Pull complete
97 8909ef0bd3f4: Pull complete
98 Digest: sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
99 Status: Downloaded newer image for qwerty.azurecr.io/order-api:1.0.0
100 qwerty.azurecr.io/order-api:1.0.0
101 Successfully verified signature for qwerty.azurecr.io/order-api@sha256:8f34be1694385d544313912f8ea4f4b417ee3bee3016bee6ba97e3e7b91d191f
102
103 /usr/bin/az account clear
104 Finishing: Verify the order-api container image signature

DevSecOps - Pipelines

dev.azure.com/dashanan13/DevSecOps/_apps/hub/ms.vss-build-web.ci-designer-hub?pipelineId=22&branch=main

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

DevSecOps

Variables | Run

main | DevSecOps / azure-pipelines.yml | Show assistant

```yaml
stages:
# Other stages for SAST, SCA tools...
- stage: BuildAndScanStage
  displayName: 'Build & Scan Stage'
  jobs:
  - job: BuildAndScanContainerImage
    displayName: 'Build & scan the container image'
    steps:
    Settings
    - task: Docker@2
      displayName: 'Build $(orderAPIImageName) container image'
      inputs:
        containerRegistry: '$(acrServiceConnectionName)'
        repository: '$(orderAPIImageName)'
        command: 'build'
        Dockerfile: './OrderAPI/Dockerfile'
        buildContext: '.'
        tags: '1.0.0'

    Settings
    - task: Bash@3
      displayName: 'Download Trivy v$(trivyVersion)'
      inputs:
        targetType: 'inline'
        script: |
          wget https://github.com/aquasecurity/trivy/releases/download/v$(trivyVersion)/trivy_$(trivyVersion)_Linux-64bit.deb
          sudo dpkg -i trivy_$(trivyVersion)_Linux-64bit.deb
          trivy -v
    Settings
    - task: Bash@3
      displayName: 'Scan the $(orderAPIImageName) container image for vulnerabilities'
      inputs:
        targetType: 'inline'
        script: |
          trivy image --exit-code 0 --severity HIGH,CRITICAL --scanners vuln $(acrName).azurecr.io/$(orderAPIImageName):1.0.0
```

DevSecOps - Pipelines

dev.azure.com/dashanan13/DevSecOps/_apps/hub/ms.vss-build-web.ci-designer-hub?pipelineId=22&branch=main

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

DevSecOps

Variables | Run

main | DevSecOps / azure-pipelines.yml | Show assistant

```yaml
- task: Bash@3
  displayName: 'Scan the $(orderAPIImageName) container image for vulnerabilities'
  inputs:
    targetType: 'inline'
    script: |
      trivy image --exit-code 0 --severity HIGH,CRITICAL --security-checks vuln --format sarif --output ./trivy-sarif.json $(acrName).azurecr.io/$(orderAPIImageN
```

Settings

```yaml
- task: Docker@2
  displayName: 'Push $(orderAPIImageName) container image'
  inputs:
    containerRegistry: '$(acrServiceConnectionName)'
    repository: '$(orderAPIImageName)'
    command: 'push'
    tags: '1.0.0'
```

Settings

```yaml
- task: AzureCLI@2
  displayName: 'Attach the scan result to the $(orderAPIImageName) container image'
  inputs:
    azureSubscription: 'DevOpsPoC'
    scriptType: 'bash'
    scriptLocation: 'inlineScript'
    inlineScript: |
      az acr login --name $(acrName)
      oras attach --artifact-type application/sarif+json $(acrName).azurecr.io/$(orderAPIImageName):1.0.0 ./trivy-sarif.json:application/json
```

Settings

```yaml
- task: AzureCLI@2
  displayName: 'List attached artifacts (ORAS) after scan'
  inputs:
    azureSubscription: 'DevOpsPoC'
    scriptType: 'bash'
    scriptLocation: 'inlineScript'
    inlineScript: |
      az acr login --name $(acrName)
      oras discover $(acrName).azurecr.io/$(orderAPIImageName):1.0.0 -v -o tree
```

DevSecOps - Pipelines

dev.azure.com/dashanan13/DevSecOps/_apps/hub/ms.vss-build-web.ci-designer-hub?pipelineId=22&branch=main

New Chrome available

Azure DevOps dashanan13 / DevSecOps / Pipelines

Search

MS

DevSecOps

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Library

Test Plans

Artifacts

Project settings

DevSecOps

Variables | Run

main | DevSecOps / azure-pipelines.yml | Show assistant

```
Settings
89    - task: Bash@3
90      displayName: 'Create a SBOM document for the $(orderAPIImageName) container image'
91      inputs:
92        targetType: 'inline'
93        script: |
94          trivy image --format spdx --output ./sbom.spdx.json $(acrName).azurecr.io/$(orderAPIImageName):1.0.0
    Settings
95    - task: AzureCLI@2
96      displayName: 'Attach the SBOM document to the $(orderAPIImageName) container image'
97      inputs:
98        azureSubscription: 'DevOpsPoC'
99        scriptType: 'bash'
100       scriptLocation: 'inlineScript'
101       inlineScript: |
102         oras attach --artifact-type application/spdx+json $(acrName).azurecr.io/$(orderAPIImageName):1.0.0 ./sbom.spdx.json:application/json
103
104
    Settings
105   - task: AzureCLI@2
106     displayName: 'List attached artifacts (ORAS) after SBOM'
107     inputs:
108       azureSubscription: 'DevOpsPoC'
109       scriptType: 'bash'
110       scriptLocation: 'inlineScript'
111       inlineScript: |
112         az acr login --name $(acrName)
113         oras discover $(acrName).azurecr.io/$(orderAPIImageName):1.0.0 -v -o tree
114
115
116 - stage: SigningStage
117   displayName: 'Sign Artifacts'
118   dependsOn: BuildAndScanStage
119   jobs:
120   - job: SignContainerArtifacts
121     displayName: 'Sign container artifacts'
122     steps:
    Settings
```

Summary

Work in Stages

Different Stages
Different Toolset
Different Processes

Authenticity and Integrity across supply chain

End to end observability

Links to checkout

- Containers Secure Supply Chain Framework documentation
- bureado/awesome-software-supply-chain-security
- https://azure-samples.github.io/aks-labs/docs/security/acr-patching
- Microsoft Developer Youtube: Securing the Containers' Supply Chain for Azure Kubernetes Service
- Level-up Container Security: 4 Open-Source Tools for Secure Software Supply Chain
- Zero Trust Architecture
- Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines

Quiz

Why is signing container images important in DevSecOps?

To reduce the image storage size	To automatically scale the container in production	To verify the image hasn't been tampered with since creation	To make the image download faster

Quiz

What is the primary purpose of generating an SBOM (Software Bill of Materials) in DevSecOps?			
automate container scaling in Kubernetes	list all software components and dependencies	encrypt container images before deployment	monitor real-time traffic to containers


THANK YOU
THANK YOU
MERCI
OBRIGADO
GRAZIE
ASANTE
どうも
WELALIN
GRAZIE
CHOKRANE
MULTUMESC
VINAKA
ZIKOMO
NIRRINGRAZZJAK
TERMA KASIH
MAAKE
SPASIBO
MATONDO
SUWUN
EIO