CYBERTEC Scalefield Secure

Getting started with Oracle

Table of contents

CYBERTEC Scalefield Secure for Oracle

Thank you for working with **CYBERTEC.** We are pleased to help our customers and bring success to them in the area of database compliance handling.

The purpose of this document is to pave the way for a successful deployment of Scalefield Secure POCs around the world. This document contains:

- Instructions on how to pull Scalefield Secure POC containers
- Installation guidelines
- Information exchange and configuration instructions

At the end of this document you will be able to achieve the following:

- **Download** assessment software
- Run **validation** scripts
  - Cross check your infrastructure for correct deployment
  - Assess accessibility and credentials
  - Remove showstoppers before the deployment
- Ship **information** to CYBERTEC
  - Allows us to pre-configure POC
  - Meet requirements for quick deployment
- Allow for a **successful** POC

Downloading the software

In case CYBERTEC or our business partners do not have access to your infrastructure, we kindly ask you to provide us with one of the two following options:

Option A: Using Docker

In case Docker is an option for you, we can offer to pull docker images from our corporate image registry, or publicly available dockerhub.

CYBERTEC container image registry

If you are able to access our container hub platform, it is available at: **containers.cybertec.at**, we will create a robot account with correct privileges, so you would be able to pull the images.

Once we provide you with the robot account details, including the username and password, you can execute following commands:

```
docker login containers.cybertec.at -u 'robot$scalefield+yourlogin'
```

After a successful login, pull the container using the following command:

```
docker pull containers.cybertec.at/scalefield-secure/secure-oracle-verification:latest
```

It will download the container capable of verifying your Oracle deployment.

Docker hub

Kindly provide the following information:

- **Login** account for **https://hub.docker.com/** so that we can give you access to the containers
- **A Contact person** we can work with and assist

We will provide you with access so that you can download the containers.

Next, follow the steps outlined here:
https://docs.docker.com/reference/cli/docker/login/

To pull the container, consider the following command:

```
docker pull cybertecpostgresql/secure-oracle-verification:latest
```

It will download the container capable of verifying your Oracle deployment.

Option B: Using SSH to copy containers

In case you are not able to use Docker, we can provide a virtual machine that allows you to download your dedicated containers. For this, we kindly request the following information:

- **A Contact person** we can work with and assist
- Your SSH key **(public key)** so that we can provide you access

In case those requirements are fulfilled, you will be provided with the hostnames / Docker repo by our engineers. **Our staff will guide you through the process** (screensharing to make it easy for you).

Scalefield Secure: Getting started with Oracle

Once you have downloaded the "Scalefield Secure Validation" containers, the goal is to verify the following components of your infrastructure:

- Check your container
- Is Docker working successfully?
- Is Oracle ready to be monitored?
- Can all relevant information be extracted from Oracle?

Verifying your Docker installation

Once we have verified your download, we can launch the container and see if Docker is working. **Follow the instructions** in the listing and ensure that you are indeed allowed to run the container. Otherwise, consult your system administrator to ensure that Docker has been set up properly on your side.

Here is how it works (on RedHat based systems):

```
[root@hostname ~]# systemctl status docker
● docker.service – Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service;
             enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-02 16:36:12 CEST;
             6 days ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 1212 (dockerd)
      Tasks: 269
     Memory: 687.0M
        CPU: 48min 30.547s
      CGroup: /system.slice/docker.service
```

As you can see the Docker daemon is running. In case it is not, refer to the official documentation.

Congratulations, you have successfully…

- Downloaded the package
- Validated Docker
- Verified that you can run the validation tool

Verify Oracle connectivity and permissions

Finally, it is time to make sure that Scalefield Secure for Oracle can actually connect to Oracle and extract audit information.

What does Scalefield Secure for Oracle do?
Here is the secret …

- **Establish a connection** to Oracle
- Access the "**UNIFIED_AUDIT_TRAIL**"
  - Extracts and archives the log
  - Purges the log to avoid repeated loading
  - Retry in case of error
- Read "**dba_registry_history**" to determine the patch level
  - Copy patch information on a regular basis
  - Determine if patching information can be extracted

Please run the validation program against EVERY Oracle installation you are planning to use. This will ensure that we have a clear picture of your configuration (missing permissions, firewall rules, etc.) which in turn, allows us to easily pre-configure the real POC deployment.

Running this in advance will save you a lot of trouble and avoids time consuming roundtrips suffering from latency and process overhead.

For EACH Oracle deployment in your POC, please run (with your Oracle connect string, user and passwords):

```
$ docker run --rm cybertecpostgresql/secure-oracle-verification \
    --v-server=//10.0.0.79:1521/cytecdb1 \
    --v-ora-user=SYSTEM \
    --v-ora-pass=system \
    --ora-char=AMERICAN_AMERICA.AL32UTF8
```

In case the CYBERTEC container hub was used:

```
$ docker run --rm containers.cybertec.at/scalefield-secure/secure-oracle-verification \
    --v-server=//10.0.0.79:1521/cytecdb1 \
    --v-ora-user=SYSTEM \
    --v-ora-pass=system \
    --ora-char=AMERICAN_AMERICA.AL32UTF8
```

Then send the FULL call + the output to CYBERTEC so that we can verify your installation and in case of error assist to fix. Here successful sample output:

```
Initializing verification database...
Verification database is ready.
12:04:55.514 INFO  secure_oracle_verification.c:482:
      Using Oracle server "//10.0.0.79:1521/cytecdb1"
12:04:55.514 INFO  secure_oracle_verification.c:483: Using Oracle user "SYSTEM"
12:04:55.725 INFO  secure_oracle_verification.c:281:
      Oracle foreign data wrapper set up: oracle_fdw 2.8.0,
      PostgreSQL 17.5 (Debian 17.5-1.pgdg120+1),
      Oracle client 23.8.0.25.4, Oracle server 23.0.0.0.0
12:04:57.776 INFO  secure_oracle_verification.c:342: Oracle setup completed
12:04:57.901 INFO  secure_oracle_verification.c:93: Fetching audit data successful
12:04:57.944 INFO  secure_oracle_verification.c:47:
      found 5 Oracle patch level entries
12:04:57.944 INFO  secure_oracle_verification.c:63:
      Oracle patch level check successful
12:04:57.944 INFO  secure_oracle_verification.c:517: All tests successful!
```

Check for "All tests successful" at the end. In case this shows up, all is good. Otherwise your Oracle system is not accessible the way it should be.

Running the tooling will avoid issues such as:

- firewall issues
- login problems
- permissions settings
- otherwise potential problems

Once all your Oracle deployments provide proper output that includes:

- Your version of Oracle
- Successful login attempt
- Successful access to audit data

Share the results with us.

Congratulations! You have **successfully extracted** all important information for the Proof-of-concept) which can now begin quickly.

In case you have not been able to fetch data from Oracle, reach out to us or to our business partner for hands-on assistance.

Typical error output

In case something is not set up correctly, the output might look like this.
Here are some typical use cases:

- Missing command line parameters
- Oracle is not reachable

Missing command line parameters

Here is what happens when the script is called with missing parameters.
It will show which values have to be set and provides some examples:

```
$ docker run --rm cybertecpostgresql/secure-oracle-verification
```

Or

```
$ docker run --rm
  containers.cybertec.at/scalefield-secure/secure-oracle-verification:latest
Initializing verification database...
Verification database is ready.
Usage:
        ./secure_oracle_verification
Required options:
    --db-conn='dbname=... host=... port=...'
    --v-server=url                # e.g. //localhost:1523/cytecdb3
    --v-ora-user=user             # e.g. system
    --v-ora-pass=pass             # e.g. system
    --ora-char=character_set      # e.g. AMERICAN_AMERICA.AL32UTF8
    --echo-oracle-password        # ATTENTION: prints password into output

Optional options:
    --debug=1
```

Oracle is not reachable

Sometimes, Oracle is not reachable for whatever reason. Maybe the host is not reachable, or maybe the credentials are wrong. Here is what a wrong host might look like:

```
$ docker run --rm
containers.cybertec.at/scalefield-secure/secure-oracle-verification:latest \
      --v-server=//10.0.0.79:1526/cytecdb6 \
      --v-ora-user=SYSTEM \
      --v-ora-pass=system \
      --ora-char=AMERICAN_AMERICA.AL32UTF8
```

… or …

```
$ docker run --rm cybertecpostgresql/secure-oracle-verification \
      --v-server=//10.0.0.79:1526/cytecdb6 \
      --v-ora-user=SYSTEM \
      --v-ora-pass=system \
      --ora-char=AMERICAN_AMERICA.AL32UTF8
```

```
Initializing verification database...
Verification database is ready.
12:07:42.515 INFO  secure_oracle_verification.c:482:
      Using Oracle server "//10.0.0.79:1526/cytecdb6"
12:07:42.515 INFO  secure_oracle_verification.c:483:
      Using Oracle user "SYSTEM"
12:07:45.184 FATAL pg_tools.c:35: Fetching single values failed (SELECT
oracle_diag('secure_oracle_verification')): ERROR:  cannot connect to
foreign Oracle server\nDETAIL:  ORA-12541: Cannot connect. No listener at
host 10.0.0.79 port 1526.\nHelp:
https://docs.oracle.com/error-help/db/ora-12541/\n
```
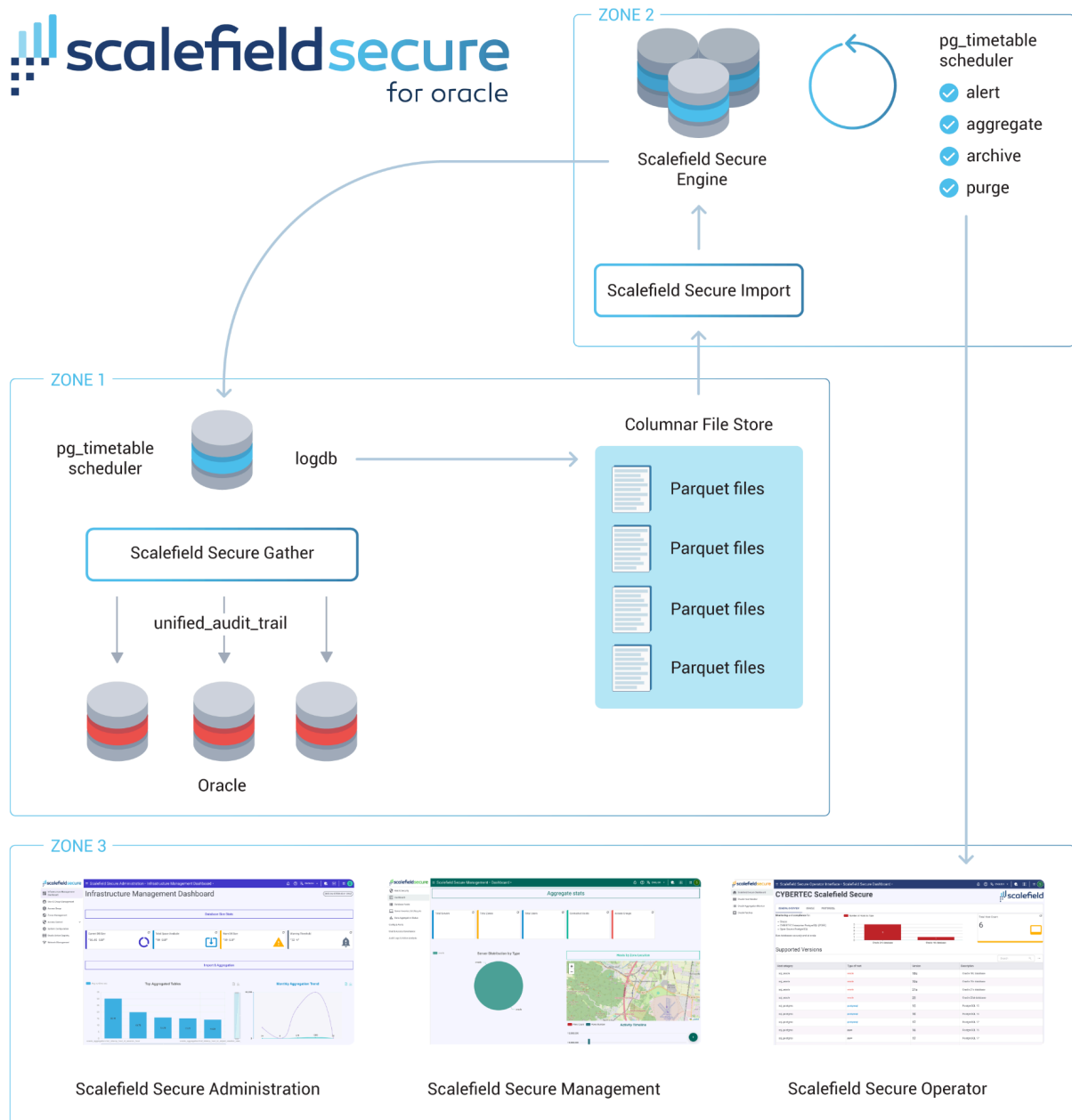
Scalefield Secure: The big picture

Scalefield Secure features a modern system architecture.
The following image shows the general architecture:

Thank you for the POC. To give you some background on what you have just achieved we want to elaborate a bit on the overall architecture. You have successfully verified that you can load data from Oracle. This step is essential for all further processing, as shown in the image. Without a reliable flow of data, it is impossible to understand what is going on inside your database infrastructure.

All the audit data which can now be gathered will be stored in an efficient way and handed over to our scalable processing and analytics engine, which can even span multiple data centers across the globe.

CYBERTEC
POSTGRESQL SERVICES & SUPPORT

AUSTRIA (HQ)
CYBERTEC POSTGRESQL
INTERNATIONAL (HQ)

SWITZERLAND
CYBERTEC POSTGRESQL
SWITZERLAND

URUGUAY
CYBERTEC POSTGRESQL
SOUTH AMERICA

ESTONIA
CYBERTEC POSTGRESQL
NORDIC

POLAND
CYBERTEC POSTGRESQL
POLAND

INDIA
CYBERTEC POSTGRESQL
INDIA PRIVATE LIMITED

SOUTH AFRICA
CYBERTEC POSTGRESQL
SOUTH AFRICA

CYBERTEC PostgreSQL International (HQ)
Römerstraße 19
2752 Wöllersdorf
Austria
Phone: +43 (0)2622 93022-0
E-Mail: office@cybertec.at

CYBERTEC PostgreSQL Switzerland
Bahnhofstraße 10
8001 Zürich
Switzerland
Phone: +41 43 456 2684
E-Mail:
swiss@cybertec-postgresql.com

CYBERTEC PostgreSQL Nordic
Fahle Office
Tartu mnt 84a-M302
10112 Tallinn
Estonia
Phone: +372 712 3013
E-Mail:
nordic@cybertec-postgresql.com

CYBERTEC PostgreSQL Poland
Pl. Inwalidów 10
01-552 Warsaw
Poland
E-Mail:
poland@cybertec-postgresql.com

CYBERTEC PostgreSQL India Private Limited
Booth No. 6,Sector 46,
HSVP Market, Faridabad,
Faridabad- 121010, Haryana
E-Mail:
office@cybertec-postgresql.com

CYBERTEC PG Database Services South America S.A.
Misiones 1486, Piso 3
11000 Montevideo
Uruguay
E-Mail:
latam@cybertec-postgresql.com

CYBERTEC PostgreSQL South Africa
No. 26, Cambridge Office Park
5 Bauhinia Street, Highveld Techno
Park
0046 Centurion
South Africa
Phone: +27(0)012 881 1911
E-Mail:
africa@cybertec-postgresql.com

If you need further information

For more information, or if you have any questions about our range of products, tools and services, contact us. There's no obligation—send us an inquiry via email or give us a call.

ISO 27001 CERTIFIED

Contact

📍 **CYBERTEC PostgreSQL International GmbH**
Römerstraße 19
2752 Wöllersdorf
AUSTRIA

📞 + 43 (0) 2622 93022-0
✉ sales@cybertec-postgresql.com

Version history

Version	Effective Date	Description	Author	Reviewed By	Approved By
1.0	2025-01-12	Secure tutorial	Armin Nesiren, Hans-Jürgen Schönig	Susanne Gruber	Hans-Jürgen Schönig
1.1	2025-03-02	Various updates	Hans-Jürgen Schönig	Scarlett Riggs	Hans-Jürgen Schönig
1.2	2025-06-27	Proofread and Design Review	Scarlett Riggs	Stephanie Chalupa	Scarlett Riggs