EDB GlobalConnect Technology
Partner Implementation Guide

Thales CipherTrust Transparent Encryption

Contents

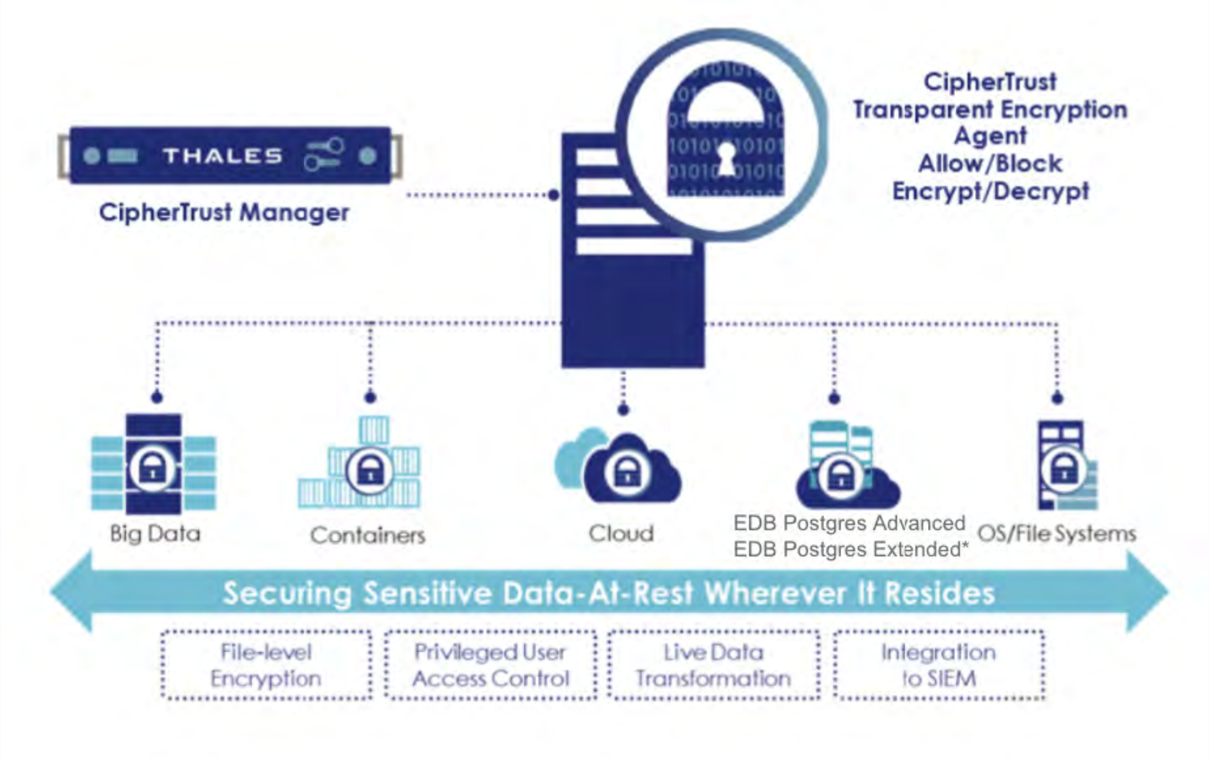
1 Partner information

Partner Name	Thales
Partner Product	CipherTrust Transparent Encryption
Web Site	**https://cpl.thalesgroup.com/encryption**
Version & Platform	**7.1.0, Available platforms: Windows , Linux**
Product Description	CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments.

EDB Certified Partner GlobalConnect Technology

2 Solution summary

Thales' CipherTrust Transparent Encryption secures data at-rest for EDB Postgres databases and backups with file system-level encryption backed by centralized key management, privileged user access controls and detailed data access audit logging. CipherTrust Transparent Encryption allows customers to adopt EDB Postgres for highly-sensitive and regulated data both on-premises and in the cloud while also meeting their compliance obligations. CipherTrust Transparent Encryption has been certified with EDB Postgres Advanced standalone, and with EDB Postgres Extended as part of a BDR (bi-directional replication) cluster, and with barman.



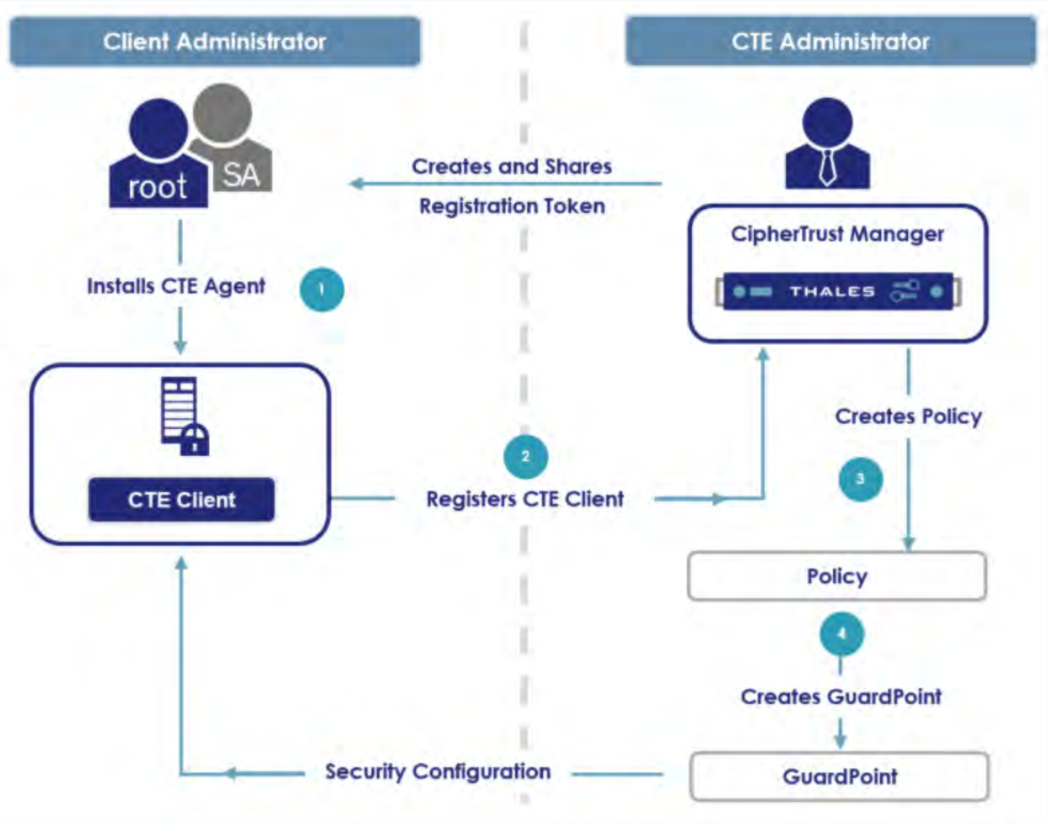
* Note: EDB Postgres Extended represents EDB Postgres Extended with BDR (Bi-Directional Replication) and barman.

3 Implementing CTE

Implementing the CipherTrust Transparent Encryption (CTE) solution requires the following components:

1. Postgres Server installed and in operation.
2. CipherTrust Manager installed and operational.
3. A CTE agent installed on the Postgres host registered to the CipherTrust Manager.

The following diagram shows the basic flow of the CTE solution:



3.1 Prerequisites

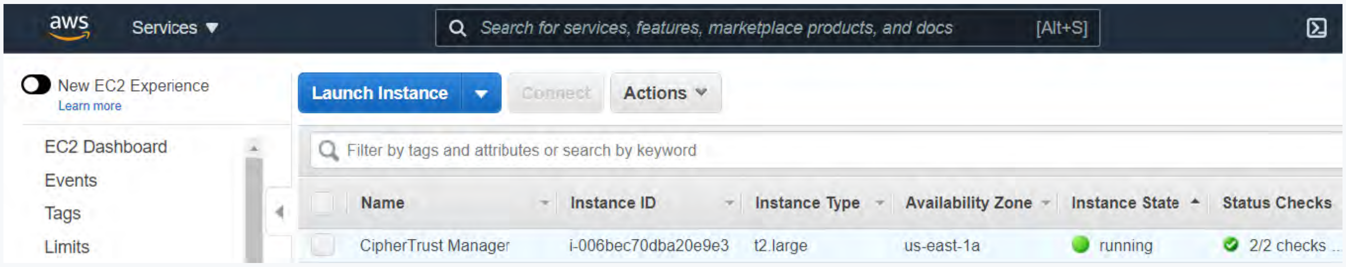
Postgres Host

1. Ensure that the Postgres Server is installed and running.
2. For CentOS 7, you need to install the following repository:

```
sudo yum install -y lsof
```

CipherTrust Manager

1. Ensure CipherTrust Manager is installed and running.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
New EC2 Experience
Learn more
EC2 Dashboard
Events
Tags
Limits
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
CipherTrust Manager	i-006bec70dba20e9e3	t2.large	us-east-1a	● running	✓ 2/2 checks ...

3.2 Configuring CipherTrust Manager

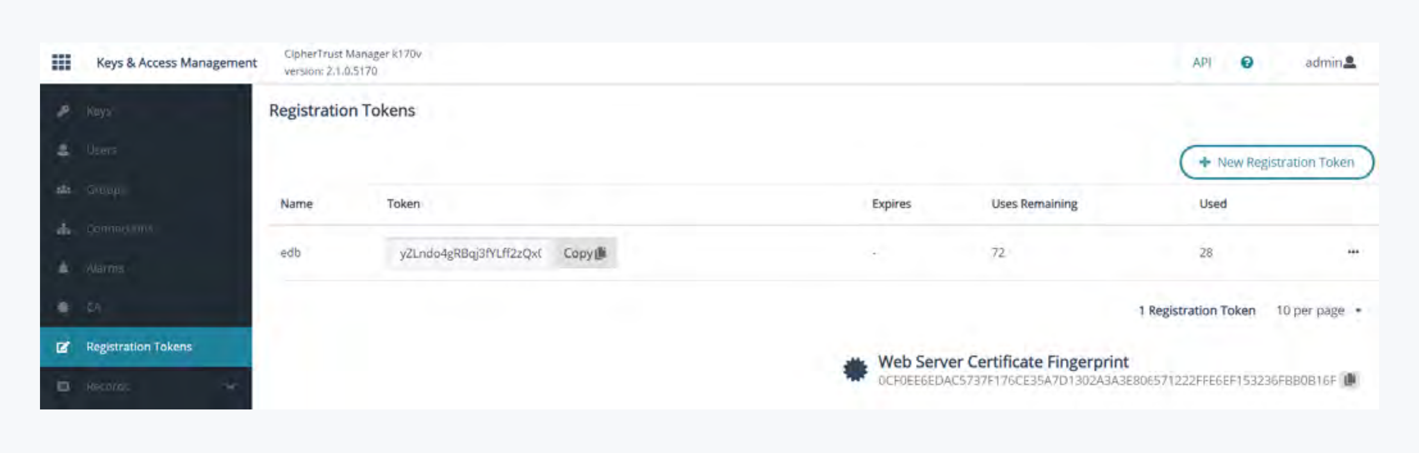
Logon to the CipherTrust Manager (CM) Web GUI and perform the following steps:

1. **Create Registration Token**

    a. Navigate to Key and Access Management and select Registration Tokens. This token will be used for the CTE agent enrollment to CM.

    b. Select New Registration Token to create a new Registration Token.

The following screenshot shows a Registration Token created with the name edb.



CipherTrust Manager k170v
version: 2.1.0.5170

Registration Tokens

Name	Token	Expires	Uses Remaining	Used
edb	yZLndo4gRBqj3fYLff2zQx(	-	72	28

1 Registration Token

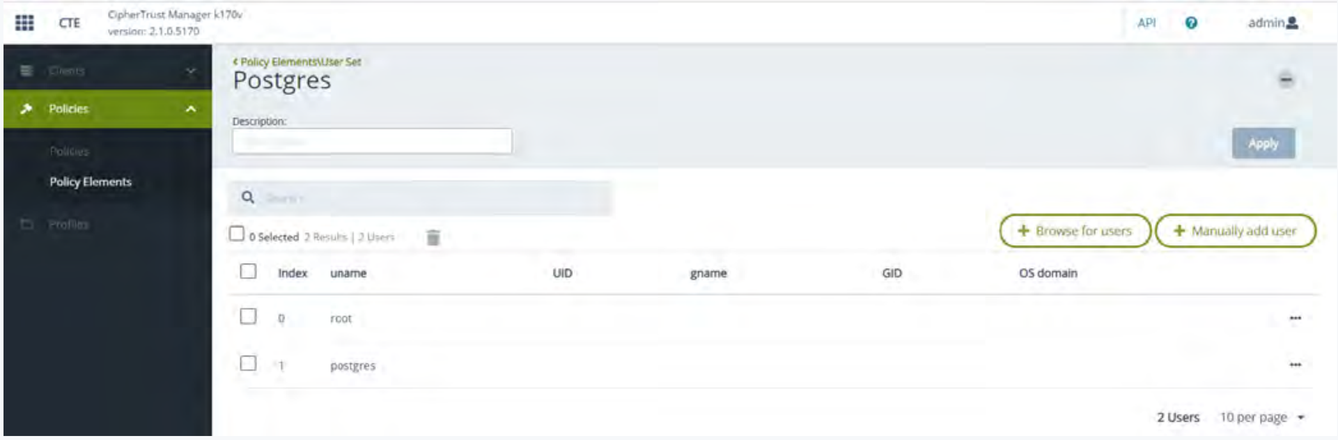
Web Server Certificate Fingerprint
0CF0EE6EDAC5737F176CE35A7D1302A3A3E806571222FFE6EF153236FBB0B16F

2. Create User Sets

a. Navigate to CTE and select Policies, Policy Elements and then User Sets.

b. Select Create User Set to create a new User Set.

The following screenshots show the User Sets created, Postgres, EnterpriseDB and Barman.



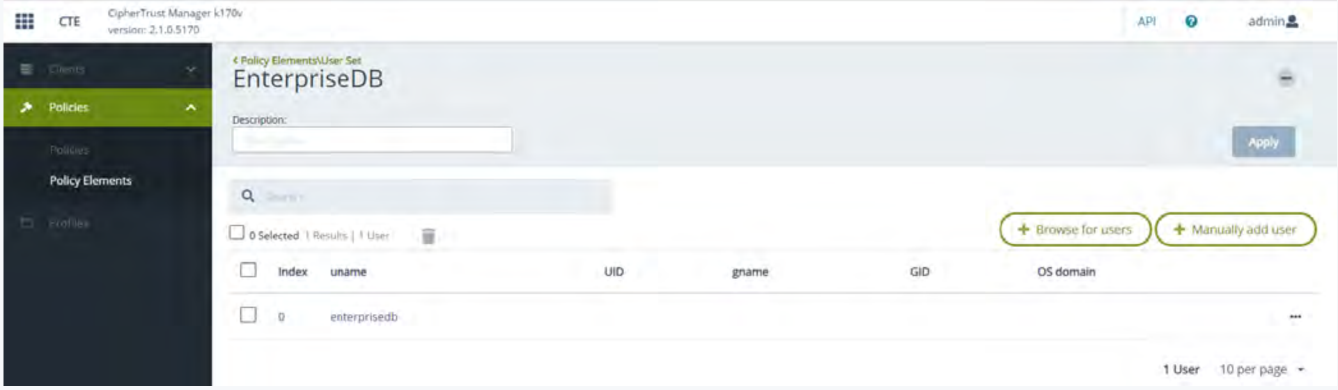
Postgres

Description:

□ 0 Selected 2 Results | 2 Users

□	Index	uname	UID	gname	GID	OS domain
□	0	root				
□	1	postgres				

2 Users 10 per page



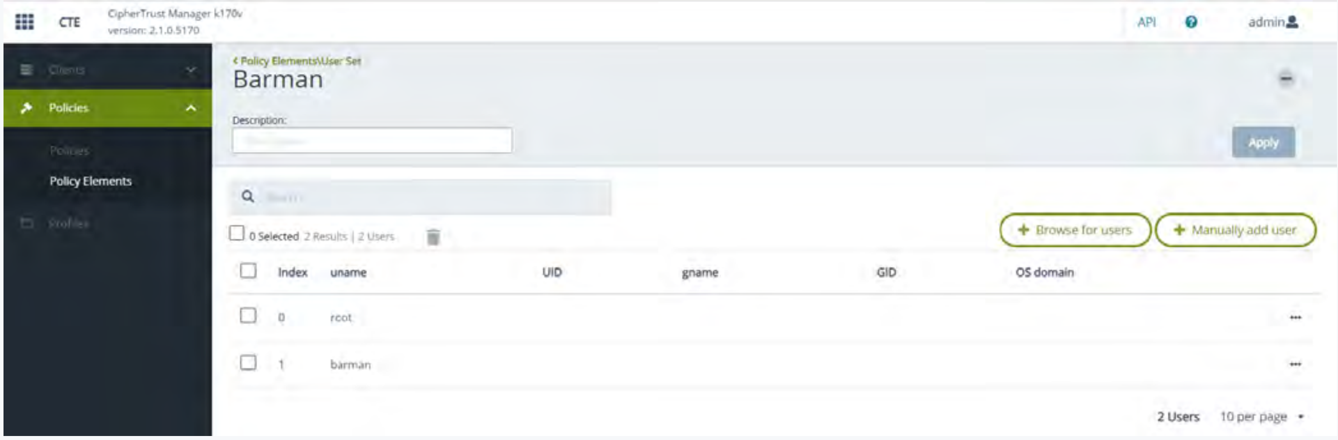
EnterpriseDB

Description:

□ 0 Selected 1 Results | 1 User

□	Index	uname	UID	gname	GID	OS domain
□	0	enterprisedb				

1 User 10 per page



Barman

Description:

□ 0 Selected 2 Results | 2 Users

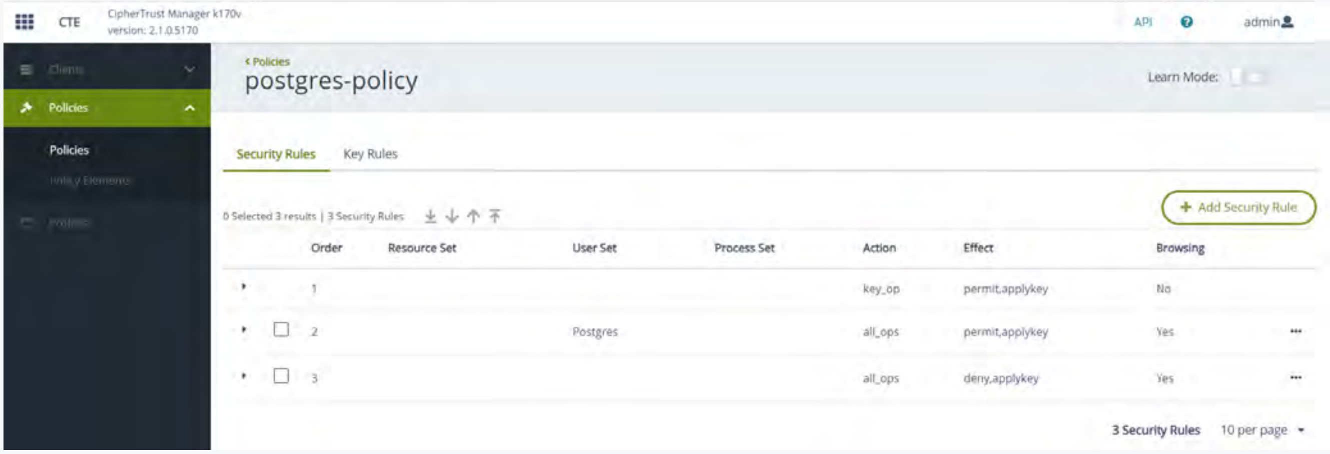
□	Index	uname	UID	gname	GID	OS domain
□	0	root				
□	1	barman				

2 Users 10 per page

2. Create Policies

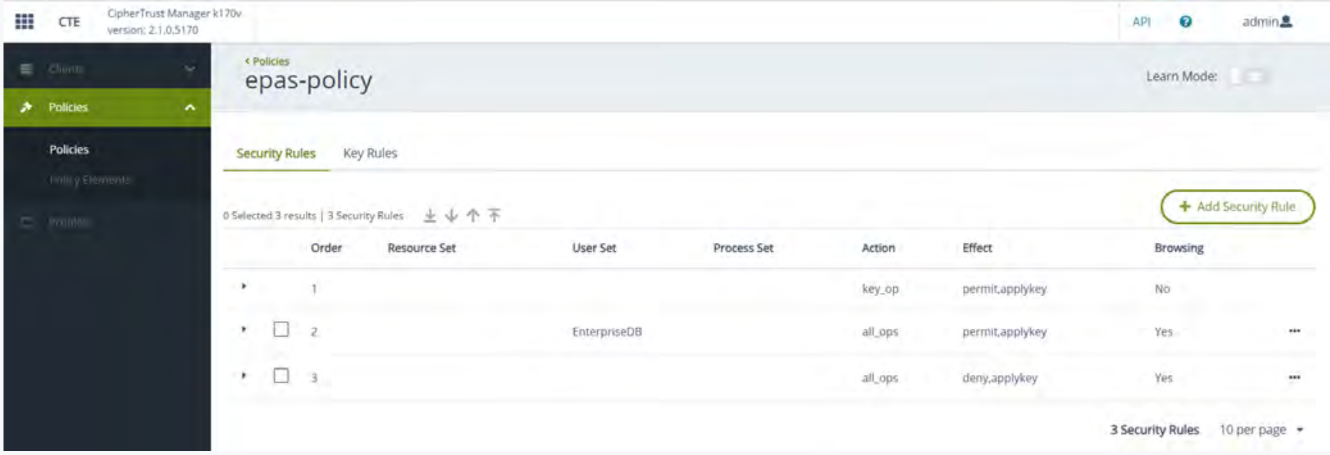
a. Navigate back to Policies and select Create Policy.

The following screenshots show Live Data Transformation (LDT) policies postgres-policy, epas-policy and barman-policy.



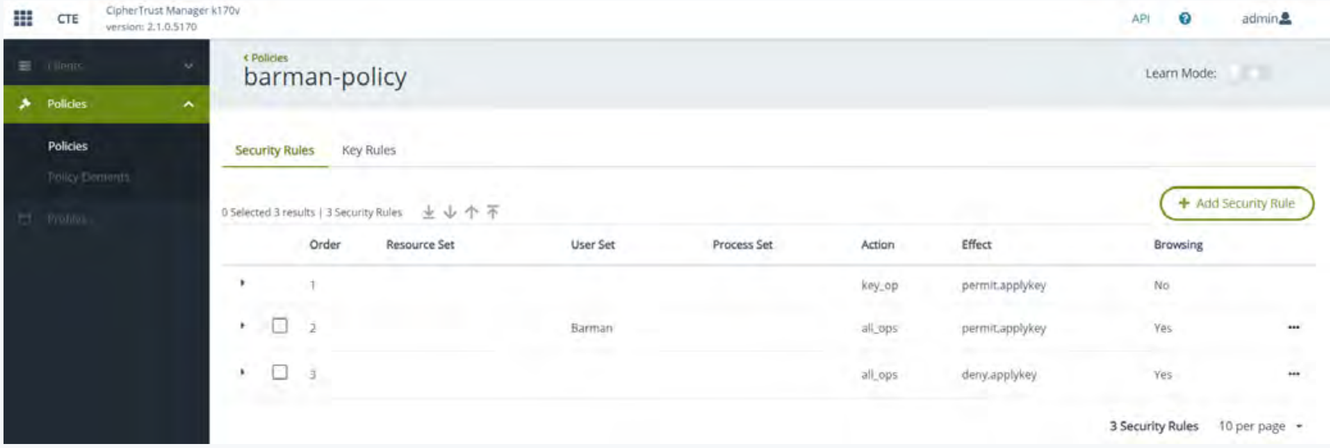
postgres-policy

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing
1				key_op	permit,applykey	No
2		Postgres		all_ops	permit,applykey	Yes
3				all_ops	deny,applykey	Yes



epas-policy

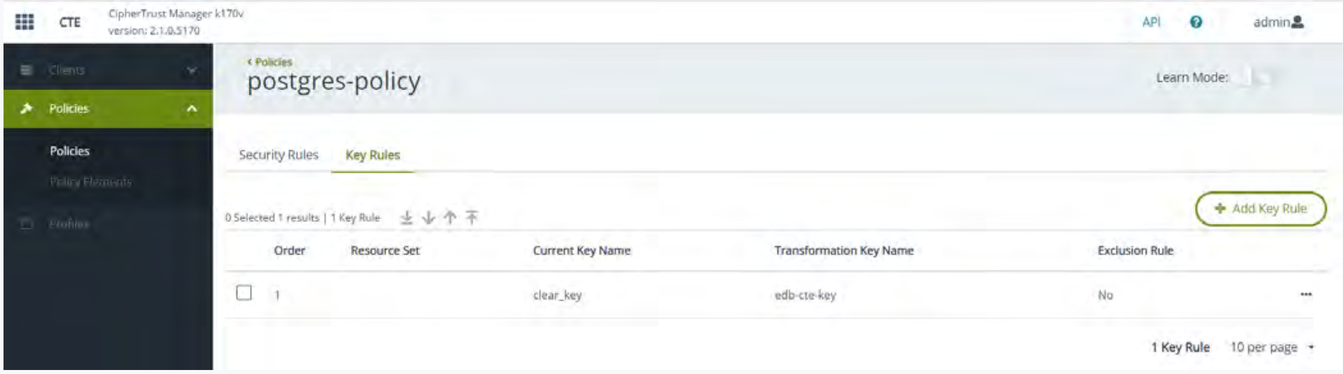
Order	Resource Set	User Set	Process Set	Action	Effect	Browsing
1				key_op	permit,applykey	No
2		EnterpriseDB		all_ops	permit,applykey	Yes
3				all_ops	deny,applykey	Yes



barman-policy

Order	Resource Set	User Set	Process Set	Action	Effect	Browsing
1				key_op	permit,applykey	No
2		Barman		all_ops	permit,applykey	Yes
3				all_ops	deny,applykey	Yes

NOTE: The policies include the User Sets Postgres and EnterpriseDB respectively created in Step 2 and the same Key Rule for the policies:



postgres-policy

0 Selected 1 results | 1 Key Rule

	Order	Resource Set	Current Key Name	Transformation Key Name	Exclusion Rule	
□	1		clear_key	edb-cte-key	No	•••

1 Key Rule   10 per page

3.3 Installing CTE Agent

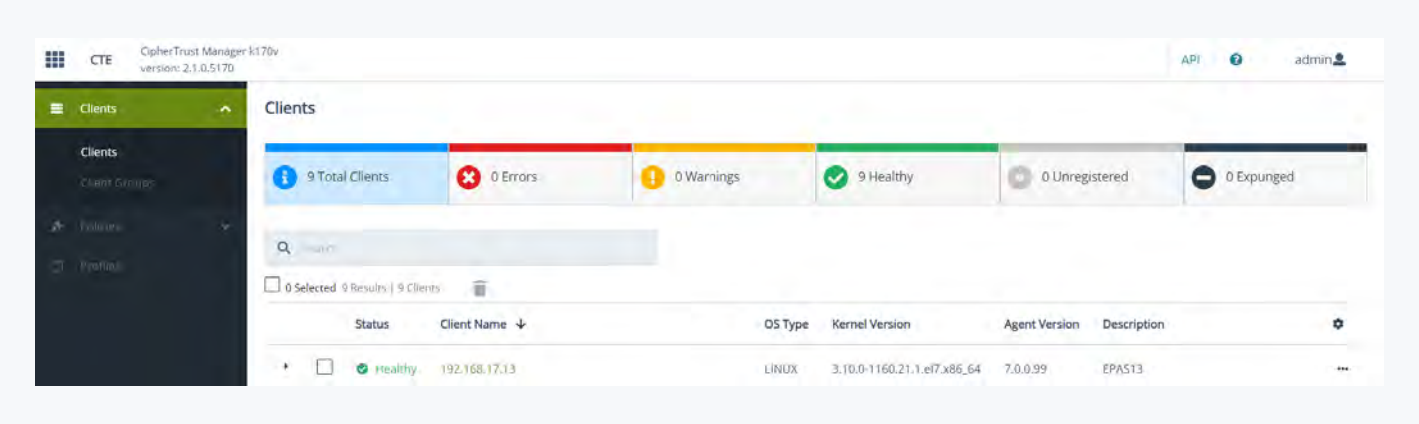
Refer to the following guides from Thales for installing the CTE agent on the Postgres host:

CTE Agent Quick Start Guide
CTE Agent Advanced Installation Guide

NOTE: You will need the Registration Token and host address of the CipherTrust Manager during the installation.

After the CTE agent is successfully installed, verify the Postgres host is registered with CM.

1. Log on to the CM Web GUI and navigate to CTE.
2. Select Clients. The client status should appear as Healthy as shown below (you may have to wait a few seconds for the status to get updated).

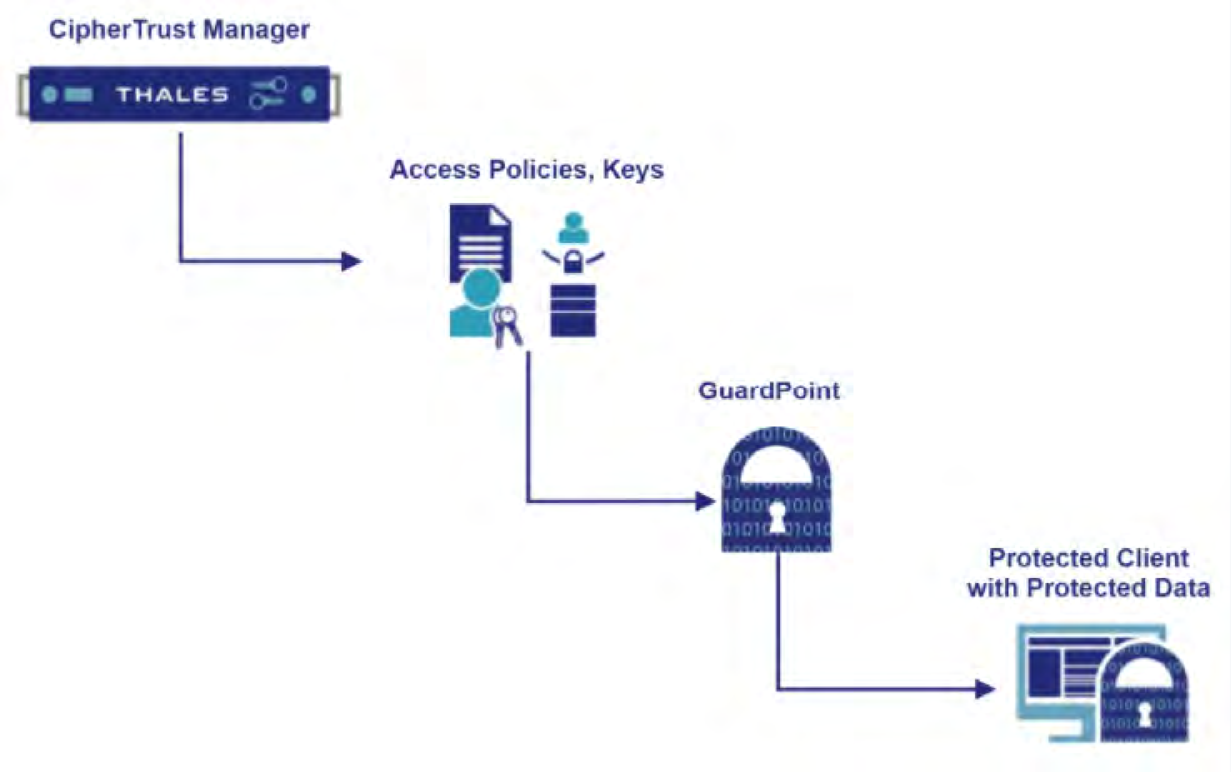


□ 0 Selected 9 Results | 9 Clients

		Status	Client Name ↓	OS Type	Kernel Version	Agent Version	Description	
▸	□	✓ Healthy	192.168.17.13	LINUX	3.10.0-1160.21.1.el7.x86_64	7.0.0.99	EPAS13	•••

4 Using CTE

CTE protects data either at the file level or at the storage device level. A CTE Agent running on the (Postgres) host manages the files behind a GuardPoint by enforcing the policy associated with it, and communicates data access events to the CipherTrust Manager for logging. A GuardPoint is usually associated with a Linux mount point or a Windows volume, but may also be associated with a directory subtree.



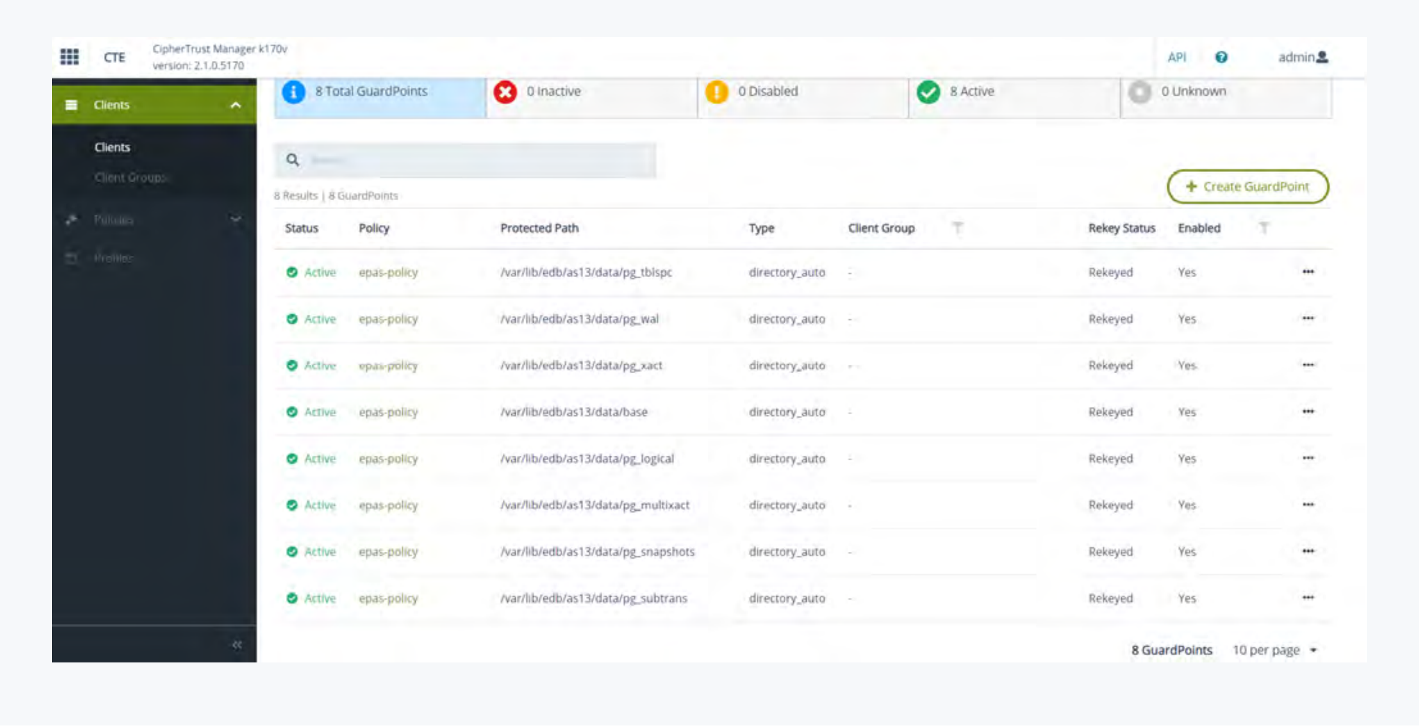
4.1 Sample User Scenarios

This section describes sample user scenarios of deploying CTE solutions on Postgres hosts such as

- **EDB Postgres Advanced Server**
- **EDB Postgres Extended with BDR**

EDB Postgres Advanced Server (Single Instance)

1. Install CTE agent on the Postgres host.
2. Login to the Postgres host and stop the postgres server.
3. Create the GuardPoints via the CM Web GUI using the epas-policy Policy on the postgres host. Set the following directories as the Protected Path on the EDB Postgres Advanced Server host (assuming PGDATA is set /var/lib/edb/as13/data on the host):



Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled
Active	epas-policy	/var/lib/edb/as13/data/pg_tblspc	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_wal	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_xact	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/base	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_logical	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_multixact	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_snapshots	directory_auto	-	Rekeyed	Yes
Active	epas-policy	/var/lib/edb/as13/data/pg_subtrans	directory_auto	-	Rekeyed	Yes

4. Restart the Postgres server on the Postgres host as the user enterprisedb.

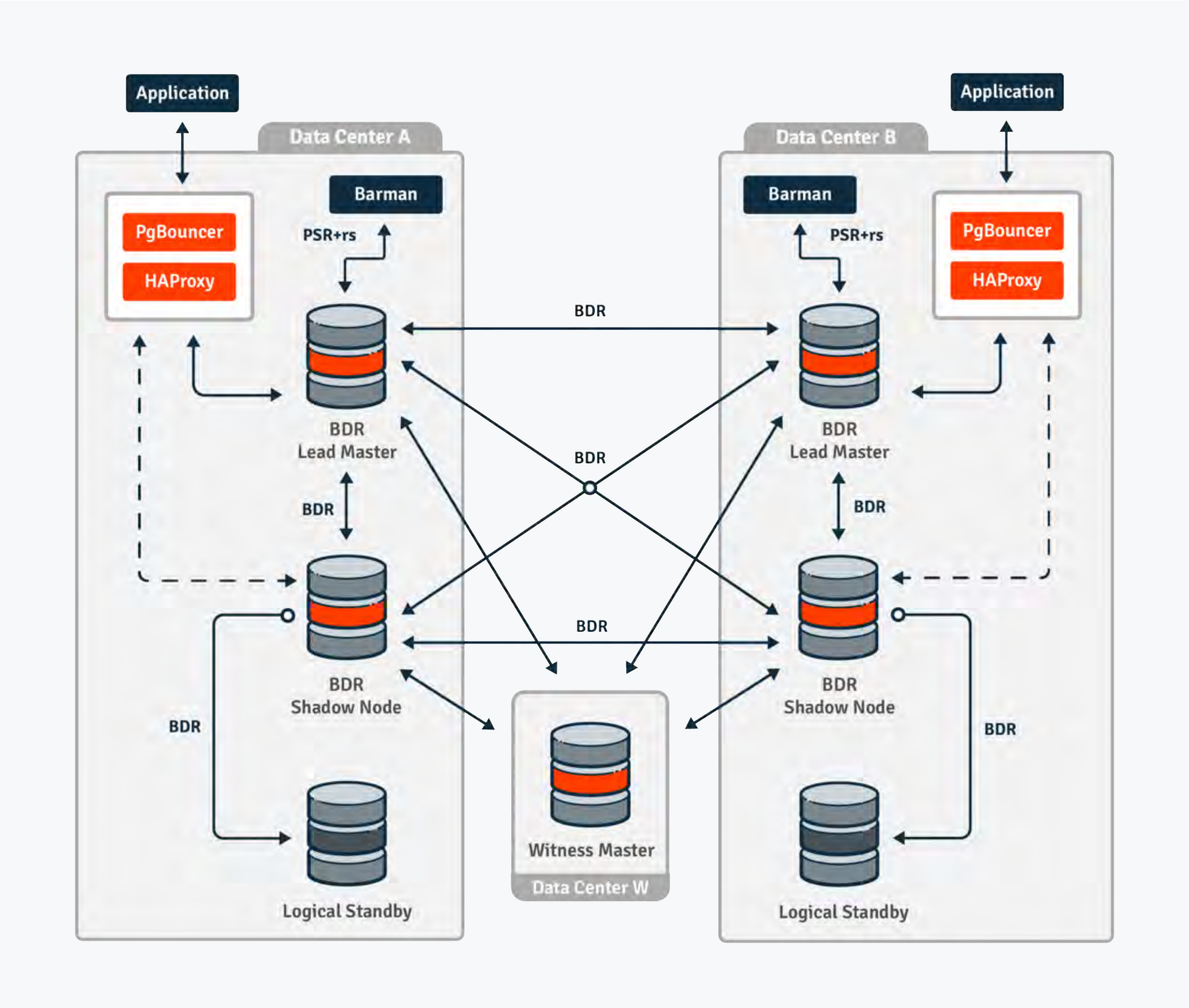
   Make sure you are logged in using ssh (not sudo).

EDB Certified Partner GlobalConnect Technology

EDB Postgres Extended with BDR-Always-ON

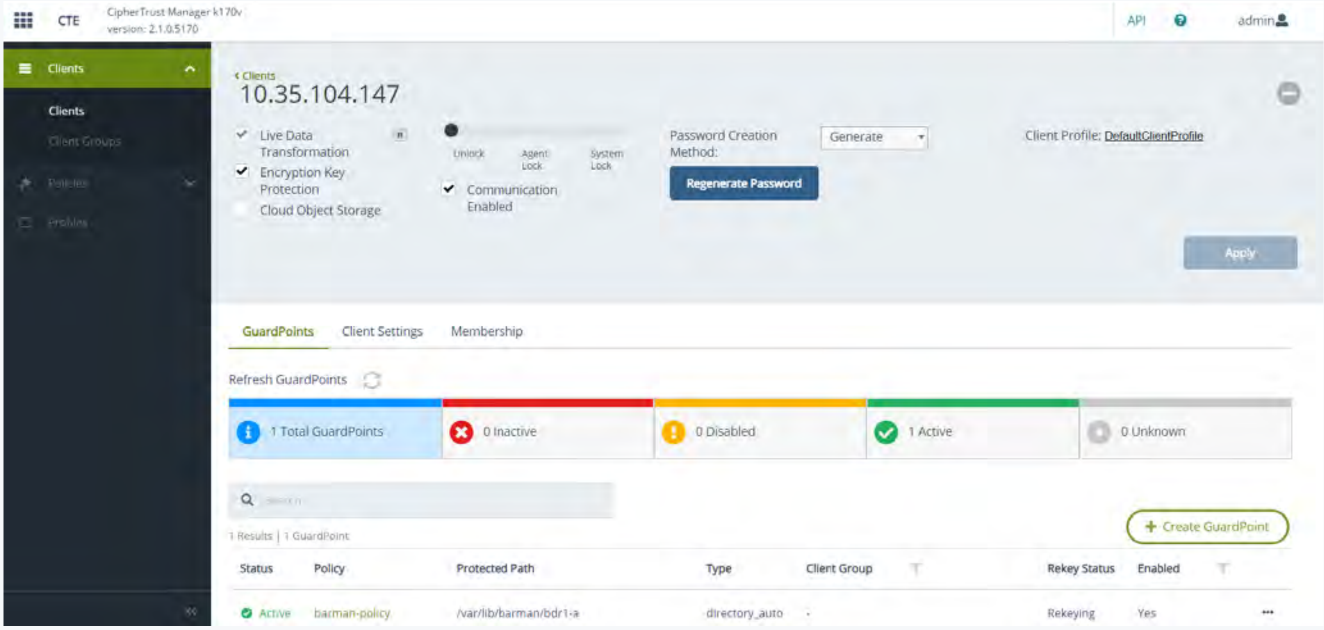
The following diagram shows the BDR-Always-ON architecture. For more details, refer to the **BDR-Always-ON Architecture documentation.**

NOTE: The documentation requires EDB access credentials.



1. Install CTE agents on all the Postgres and barman nodes.

2. Create a GuardPoint via the CM Web GUI using the barman-policy Policy on the directory /var/lib/barman/<server-name> on the barman node in data center A (DC A). The following screenshot shows a GuardPoint created for the barman node.



10.35.104.147

✓ Live Data Transformation

☑ Encryption Key Protection

□ Cloud Object Storage

☑ Communication Enabled

Password Creation Method: Generate

Client Profile: DefaultClientProfile

1 Total GuardPoints | 0 Inactive | 0 Disabled | 1 Active | 0 Unknown

1 Results | 1 GuardPoint

Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled	
✓ Active	barman-policy	/var/lib/barman/bdr1-a	directory_auto	-	Rekeying	Yes	•••

3. Login to the Standby node in data center A and stop the postgres server.

4. Create a GuardPoint on the Standby node via the CM Web GUI using the postgres-policy Policy on the PGDATA directory /opt/postgres/data.

5. Restart the Postgres server on the Standby node as the user postgres. Make sure you are logged in using ssh (not sudo).

6. Login to the Shadow Master node in data center A and stop the postgres server.

7. Create a GuardPoint on the Shadow Master node via the CM Web GUI using the postgres-policy Policy on the PGDATA directory /opt/postgres/data.

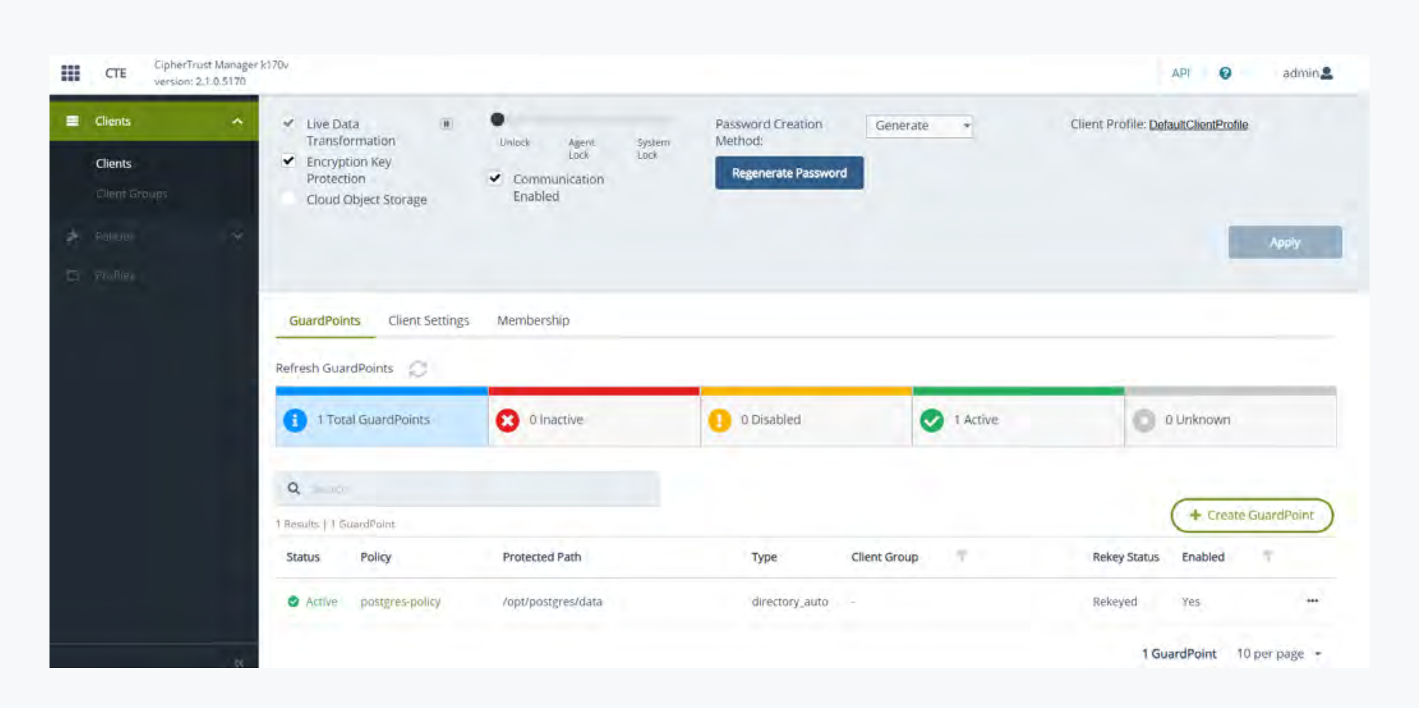
8. Restart the Postgres server on the Shadow Master node as the user postgres. Make sure you are logged in using ssh (not sudo).

9. Login to the Lead Master node in data center A and stop the postgres server.

10. Create a GuardPoint on the Lead Master node via the CM Web GUI using the postgres-policy Policy on the PGDATA directory /opt/postgres/data.

11. Restart the Postgres server on the Lead Master node as the user postgres. Make sure you are logged in using ssh (not sudo).

The following screenshot shows a GuardPoint created for Lead Master in data center A.



✓ Live Data Transformation

☑ Encryption Key Protection

○ Cloud Object Storage

● Unlock — Agent Lock — System Lock

☑ Communication Enabled

Password Creation Method: Generate

Client Profile: DefaultClientProfile

1 Total GuardPoints | 0 Inactive | 0 Disabled | 1 Active | 0 Unknown

1 Results | 1 GuardPoint

Status	Policy	Protected Path	Type	Client Group	Rekey Status	Enabled
✓ Active	postgres-policy	/opt/postgres/data	directory_auto	-	Rekeyed	Yes

1 GuardPoint 10 per page

12. Repeat steps 2 through 11 for postgres and barman nodes in data center B (DC B).

5 Certification environment

Certification Test Date:	May 19 2021
EDB Postgres Advanced Server	13.2.5
OS	CentOS Linux 7 (Core)
Memory	2G
Processor	Intel® Xeon® Processor SP Family (“Skylake”)
Cloud Platform	OpenStack (Kilo)
CPU(s)	1
Core(s) per socket	1
Socket(s)	1
Storage	80 GB
CipherTrust Transparent Encryption	7.0.0.99

Certification Test Date:	May 19 2021
EDB Postgres Extended with BDR	3.6.1
OS	CentOS Linux 7
Cloud Platform	AWS
Deployment Tool	tpaexec v20.11

NOTE: Refer to the sample config.yml for deployment details.

EDB

Partner Program

GlobalConnect
Technology

EDB GlobalConnect Technology Partner Implementation Guide

EDB GlobalConnect Technology Partner Implementation Guide

EnterpriseDB Corporation
34 Crosby Drive
Suite 201
Bedford, MA 01730

EDB™
POWER TO POSTGRES