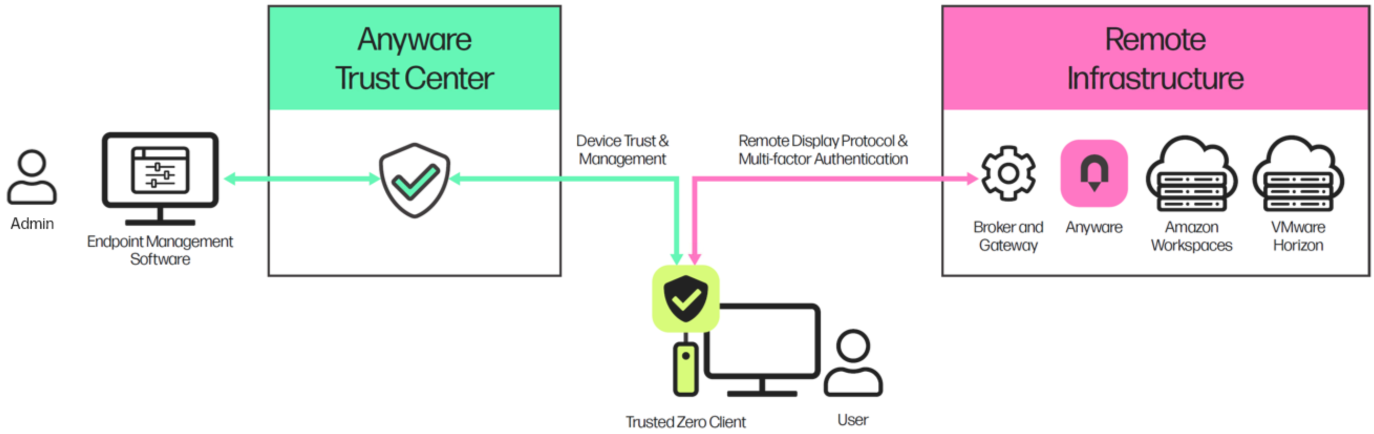
Anyware Trust Center Administrators' Guide

25.03

Table of Contents

Anyware Trust Center Administrators' Guide

The Anyware Trust Center provides a management and security plane for a Trusted Zero Client deployment. Using the Anyware Trust Center, administrators can register Trusted Zero Clients, manage their capabilities and features, enable and disable connections, and monitor access behavior.



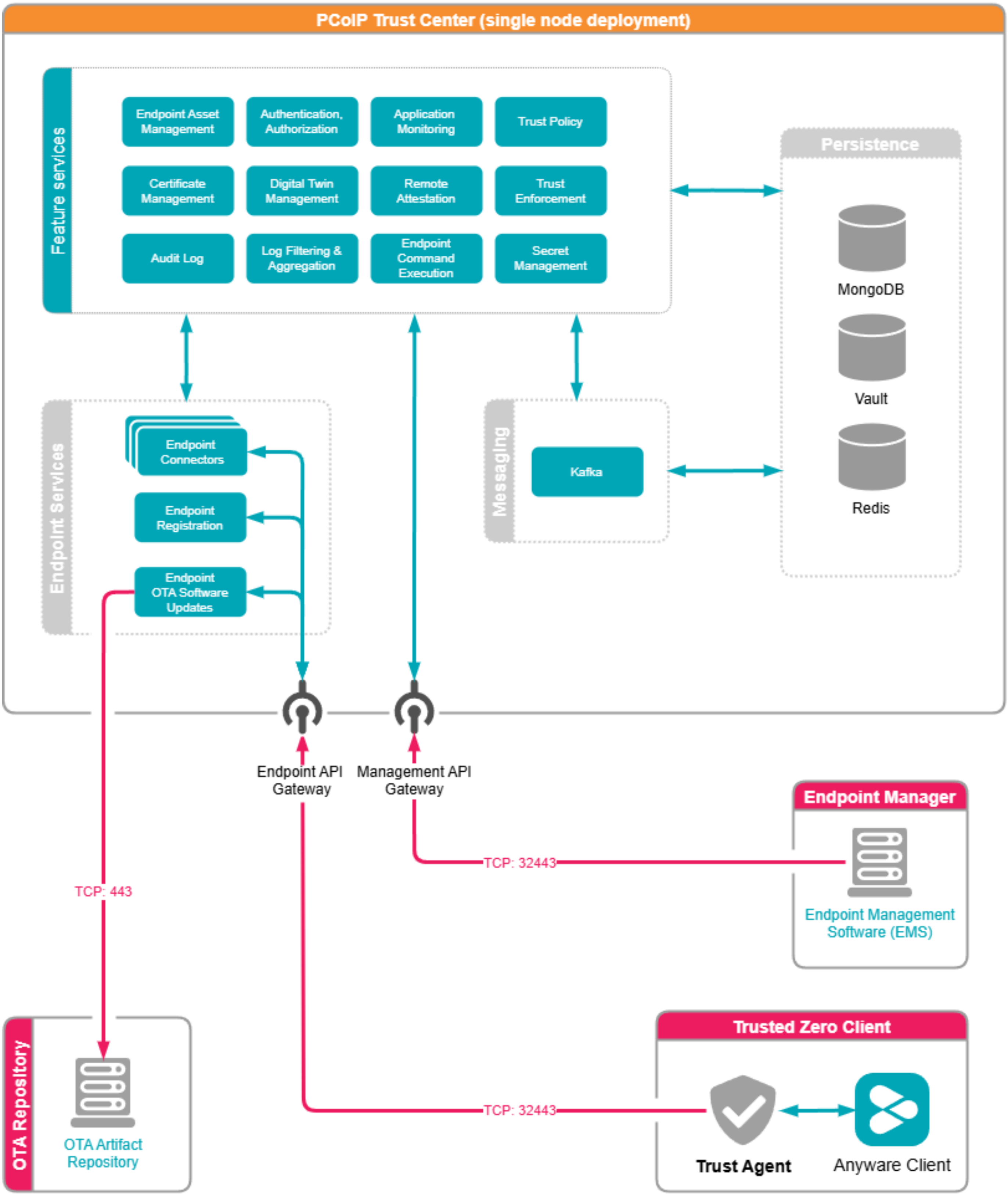
The Anyware Trust Center is an application composed of multiple services on a single VM. It connects to Trusted Zero Client endpoints and your Endpoint Manager.

Important: About Endpoint Managers

The Anyware Trust Center is an API service, and has no user interface. All user interaction and interfaces are provided by an *Endpoint Manager*, also called *Endpoint Management Software (EMS)*. Endpoint Management Software is available from the hardware manufacturer of your Trusted Zero Client. Ensure that the **EMS is compatible** with the Trust Center version you intend to use.

Anyware Trust Center Architecture

The Anyware Trust Center is composed of multiple feature services which communicate internally within the cluster, and also securely communicate with the distributed Trusted Zero Clients and the Endpoint Manager.


PCoIP Trust Center (single node deployment)
Feature services
Endpoint Asset Management
Authentication, Authorization
Application Monitoring
Trust Policy
Certificate Management
Digital Twin Management
Remote Attestation
Trust Enforcement
Audit Log
Log Filtering & Aggregation
Endpoint Command Execution
Secret Management
Persistence
MongoDB
Vault
Redis
Endpoint Services
Endpoint Connectors
Endpoint Registration
Endpoint OTA Software Updates
Messaging
Kafka
Endpoint API Gateway
Management API Gateway
TCP: 443
TCP: 32443
Endpoint Manager
Endpoint Management Software (EMS)
TCP: 32443
OTA Repository
OTA Artifact Repository
Trusted Zero Client
Trust Agent
Anyware Client

About Anyware Trust Center Persistence

The Anyware Trust Center uses multiple services for data persistence. The following table lists these services and briefly describes how each is used.

Service	Description
MongoDB	MongoDB maintains management data, including endpoint configuration, digital twins, and system configuration.
MariaDB	Provides OTA update data and metadata.
Vault	Holds auth secrets, Anyware Trust Center user credentials, and endpoint operational PKI.
Redis	Audit logging and general system caching.

Note: About external services

The Anyware Trust Center does not currently support external instances of these services.

We recommend backing up the Anyware Trust Center and all persistent storage volumes.

About the Zero Trust Ecosystem

The Anyware Zero Trust Ecosystem is a robust architecture for Anyware deployments, founded on zero-trust principles and providing extremely secure Anyware deployments. There are two primary components in the Zero Trust ecosystem: **Trusted Zero Clients**, which allow end users to connect to their remote desktops, and the **Anyware Trust Center**, which manages the Trusted Zero Clients and enforces policies and integrity.

Throughout this document, the Trusted Zero Clients may be referred to as *endpoints*. Currently, the Trusted Zero Client is the only endpoint managed by the Anyware Trust Center.

Security Provisions

The Anyware Trust Center establishes trust between a remote Trusted Client device in several key ways:

- **Birth Certificates**: Each factory-provisioned Trusted Client provides a certificate, assigned when provisioned by the vendor, which is used to establish a trust relationship with your Anyware Trust Center. If a device has an unknown birth certificate, or if its certificate is not signed as expected, it cannot connect.
- **Digital Twins**: The Anyware Trust Center maintains a copy of the *expected* state and the *current* (actual) state of each Trusted Zero Client it manages.

  Each time a Trusted Zero Client connects, the Anyware Trust Center reads the endpoint's current state and compares it with the expected state. If the Trusted Zero Client has been tampered with, the two states will not match, and your Endpoint Management Software (EMS) can revoke its trusted status.

  When administrators modify a Trusted Zero Client's settings, the Anyware Trust Center updates its local copy (the *expected* state), and pushes the changes to the physical Trusted Zero Client the next time it connects.
- **Direct Secure Boot**: Users cannot access the firmware, BIOS, or operating system of the Trusted Zero Clients. Each device securely boots directly into the Anyware Client application.
- **OTA Updates**: Firmware updates for Trusted Zero Clients are delivered Over the Air (OTA), so bug fixes and security updates can be provided immediately when available. OTA updates are delivered

using The Update Framework (TUF) and Uptane frameworks, providing an update mechanism capable of resisting even nation-state level actors.

Important Terminology

- **Provisioning**: Provisioning is performed at the factory, when the Trusted Zero Client is prepared for delivery. This process includes creating the device's birth certificate and signing it with an HP certificate authority.
- **Registration**: The initial connection between a Trusted Zero Client and the Anyware Trust Center, when the Trusted Zero Client is added to the Anyware Trust Center's list of managed devices. After registration, the Trust Center can manage the Trusted Zero Client, and users can connect to their authorized desktops.
- **PKI**: PKI stands for *Public Key Infrastructure*, which is a method of distributing and managing security certificates. The Anyware Trust Center supports either an external PKI, which you provide, or an internal service for smaller or less-complex deployments. External PKIs must provide an externally-issued signing CA that the Anyware Trust Center uses to generate operational certificates.
- **Endpoint Management Software (EMS)**: Also called an *Endpoint Manager*, the Endpoint Management Software is a third-party application that provides a user interface for the Anyware Trust Center. The Endpoint Management Software is available from your Trusted Zero Client manufacturer.

What's New in This Release

Release 25.03 of the Anyware Trust Center contains bug fixes and stability enhancements. Additionally, it also includes the following:

Support for Imprivata Authentication

Version 25.03 of the Anyware Trust Center supports Imprivata OneSign for authenticating Trusted Zero Clients connecting to Horizon hosts. Imprivata OneSign enables users to access corporate networks, desktops, and applications with a single sign on. This reduces the need for maintaining separate passwords and prevents unauthorized access.

For more information, see Enabling Imprivata Authentication.

Trust Center Installation with DISA STIGs

In version 25.03, support has been added to enable the installation of the Trust Center on servers and virtual machines that comply with the security policies and configurations recommended by the US DOD Cyber Exchange. For this purpose, a new configuration called `fapolicyd` has been added, which allows the Trust Center components to run on servers that adhere to STIG requirements. For more information see Trust Center Installation with DISA STIGs.

SIPR/NIPR Network Migration

In version 25.03, support has been added for securely migrating Trusted Zero Clients between SIPR, NIPR, and insecure networks. When re-commissioning a Trusted Zero Client for use on a SIPR/NIPR or insecure network, specific steps must be followed to completely erase all local data and configurations. This prevents accidental or malicious access to critical data during network migrations, and ensures compliance with security recommendations.

Support for Darksite Upgrades

Version 25.03 now supports upgrade of Anyware Trust Center that does not have a connection to the public internet. Upgrading a dark site requires a temporary internet-connected machine, which downloads the required packages to create an upgrade bundle. The upgrade bundle is transferred to the dark site machine and used for upgrading Trust Center.

The dark site installer for 25.03 also includes a few changes from how the commands are run, from the original 24.07 release.

For more information, see Darksite Upgrade of Trust Center.

Support for Uploading OTA packages to Darksite Trust Center

As Darksite Trust Center operates without internet connectivity, automatic OTA updates are not possible. Version 25.03 addresses this limitation by introducing a new command for managing firmware within the Trust Center. Administrators can now download as well as upload OTA packages to the Trust Center server without the need for opening an internet connection.

For more information see the following topics:

- Upgrading Trust Center
- Darksite Upgrade

Other Update

To limit the amount of sensitive data saved into Anyware Trust Center support bundles, the auto-generated Trust Center admin password, typically used as the default password, will no longer be saved to the configuration file. This limits the exposure of sensitive data, and prevents its accidental access.

Info

Support for RHEL 8 has been extended until the end of 2025.

System Requirements

The Anyware Trust Center is installed on a machine that meets the following minimum requirements:

Requirement	
Operating System	• RHEL 8 Support for RHEL 8 has been extended until the end of 2025. • RHEL 9 • Rocky Linux 9 • CentOS Stream 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes. The Trust Center does not support installation on **Sparse** (thin) provisioned disks. Please use raw or thick provisioned disks.
Network	• IP network accessible by your endpoints, with configured DNS. The Anyware Trust Center does not support connections via raw IP addresses. • TCP 32443 (Communication with Trusted Zero Clients) • TCP 443 (Communication with OTA update CDN)
Python	The post-installation and initialization scripts require Python 3.8.2+.
Other software	The OS must have cURL available.

Note that the specifications listed here are minimums. Large or complex deployments should expect to use machines with higher specifications.

Important: A management tool is required

The Anyware Trust Center is an API service and has no user interface. The Anyware Trust Center must be able to connect to a compatible Endpoint Management Tool from a supported manufacturer. Make sure that the **Endpoint Management Tool is compatible** with the Trust Center version that you plan to install.

Dark Site System Requirements

The Anyware Trust Center can be installed in dark sites (sites without a connection to the public internet). Installing in a dark site requires two machines: a temporary internet-connected machine to assemble the installer bundle, and the unconnected machine that will host the Anyware Trust Center. For installation instructions, see Dark Site Installation.

Bundler System Requirements:

This machine is only required while downloading packages and creating an installation bundle, and can be deleted when finished.

Requirement	
Operating System	• RHEL 9 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	At least 20GB free space available for the generated dark site bundle.
Network	The machine used to create the bundle must be connected to the public internet.
Software	Docker v25.0.1+, cURL, DNF

Dark Site Machine Requirements

This machine hosts the Anyware Trust Center in the dark site location and is permanent.

Requirement	
Operating System	• RHEL 8, 9 • Rocky Linux 9 • CentOS Stream 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes. On ESXi or similar hypervisors, the Trust Center does not support installation on **Sparse** (thin) provisioned disks. Please use raw or thick provisioned disks.

Requirement	
Network	A default gateway is required, even without an internet connection. If the machine does not have one, a dummy route is required for installation. See Checking for a Default Gateway for instructions.
Software	DNF

Anyware Trust Center Features

The Anyware Trust Center supports a number of endpoint management settings and capabilities, some of which are constrained by your subscription level. The available features and support level are described next.

About Licensing and Subscription Tiers

Most Anyware Trust Center functionality requires a subscription. Basic functionality is available for free for users who have small deployments, or who are testing proof-of-concept scenarios.

Registration is required for both Trust Center and Trusted Zero Client downloads. New Trusted Zero Client devices ship with a 12-month free subscription.

Endpoint Management

Feature	Free tier	Subscriber
Endpoints under management	up to 50	up to 5,000[1]
Endpoint monitoring	Yes	Yes
Device Logging	Yes	Yes
Endpoint power management	Yes	Yes
Endpoint factory reset	Yes	Yes
Over-the-Air (OTA) updates	—	Yes
Set USB usage policies	—	Yes

Endpoint Under Management

The Anyware Trust Center can manage a large number of endpoint devices. The specific number of supported endpoints supported depends on your subscription tier, as noted above. The free tier, which does not require a subscription, is limited to 50 devices.

Endpoint Auto-Discovery and Configuration

When a new Trusted Zero Client connects to the Anyware Trust Center, it will automatically register and configure it according to policies established in your EMS software.

Endpoint Monitoring

The Anyware Trust Center supports status monitoring of all devices in your deployment, which can be used to display dashboards and other relevant management information in your Endpoint Manager.

Device Logging

The Anyware Trust Center can access logs for all of its managed Trusted Zero Clients, allowing administrators to troubleshoot deployment problems and monitor unusual activity.

Endpoint Power Management

The Anyware Trust Center can shut down or restart the endpoint devices it manages.

Endpoint Factory Reset

The Anyware Trust Center can reset any endpoint to factory defaults.

After a factory reset, the endpoint must re-register with the Trust Center. If it is on the same network as the Trust Center, and if the discovery DNS record is created, this will happen automatically when the device boots up. Otherwise, you will be prompted for the FQDN of the Trust Center.

Over-the-Air (OTA) Updates

The Anyware Trust Center can retrieve device software updates and deploy them to its endpoints automatically. Updates can be configured to install immediately, on a schedule, or by prompting the end user.

Set USB Usage Policies

USB policies can be set for each Trusted Zero Client that the Anyware Trust Center manages. Note that USB policies can also be set on remote PCoIP agents; USB devices must be allowed by *both* the Anyware Trust Center and the PCoIP agent. PCoIP agents, by default, permit all supported USB access.

Anyware Trust Center Management

Feature	Free tier	Subscriber
Concurrent Anyware Trust Center user access	—	Yes
PKI Support	—	Yes
Configure trusted connections	—	Yes

Concurrent User Access

Any number of users can access the Anyware Trust Center via your EMS software at once.

PKI Support

The primary PKI is an internal Hashicorp Vault instance in the Anyware Trust Center. You can provide an issuing CA cert and key to the internal Vault, which allows the root of Trust to come from your existing PKI.

Configure Trusted Connections

Trusted connections can be configured on the Anyware Trust Center. When configured this way, the Trusted Zero Client devices registered with the Anyware Trust Center will not be able to set their own connections, and must use the connections configured.

---

1. The initial release of Anyware Trust Center supports up to 5000 devices connected with a paid subscription. This limit will be increased to 10,000 in a future release. ↩

Installing

Trust Center Installation Overview

Deployment Modes

The current release of the Anyware Trust Center uses a **single-node** installation into a K3S cluster using a provided script. The installation script creates and configures the node for you, and does not require manual setup.

Future releases of the Anyware Trust Center will support multi-node environments, installed into a Kubernetes cluster which you create and manage yourself.

When to Use Single-Node Deployments

The single-node instance of the Anyware Trust Center is appropriate for the following use cases:

- You do not require high availability or redundancy; your security policies permit delayed policy enforcement in the event your Anyware Trust Center is down or unavailable for any reason.
- You are deploying a proof-of-concept system for testing purposes.
- You do not have in-house Kubernetes expertise, and are not retaining our Professional Services team.
- You do not expect to grow beyond the initial node.

Note: Migrating from single-node to multi-node deployments

When multi-node deployments are available, a migration procedure will be published to support moving from one model to the other.

FAILURE RAMIFICATIONS IN SINGLE-NODE DEPLOYMENTS

The single-node deployment of the Anyware Trust Center is not a high-availability configuration. If the Anyware Trust Center is unavailable for any reason, including network connectivity issues, the following will occur until service is restored:

- Endpoints cannot be managed and policies cannot be enforced.
- New endpoints cannot be added.
- Monitoring and logging of endpoints will be paused.
- **Users can still connect to remote sessions while the Anyware Trust Center is down**.

Trusted Zero Clients continue to accumulate logging data even if the Anyware Trust Center is offline. When the Anyware Trust Center is reachable again, logging data will catch up automatically, without loss in continuity.

Planning for Future Multi-Node Deployments

Important: This method is not currently available

Multi-node deployments are not supported in this release of the Anyware Trust Center. This information is included here to help you plan for future deployments.

If any of the following describes your use case, you should plan to use the Multi-Node Installation method when it is available:

- You require high-availability SLAs and real-time monitoring of endpoints (in a single-node deployment, if the Anyware Trust Center is unreachable, monitoring is unavailable until the connection is restored).
- You have enterprise requirements such as multiple Trust Centers deployed in different regions, or a mix of cloud and on-premesis deployments.
- You will create or extend your own self-managed Kubernetes cluster, either by yourself or in consultation with our Professional Services team.

Pre-Installation

Before you begin the installation process (Single node and dark site) for the Anyware Trust Center, it's essential to prepare your **DNS records**.

The **Anyware Trust Center** requires you to add **five domain names** to your DNS records.

First, create the base domain for the Anyware Trust Center. This base domain will be used to construct the other four subdomains. **Record this value**, as you will need it in multiple locations during setup.

For this demonstration, we will use `trust-center.example.com`. This value will help you create the required subdomains.

Single-Node Anyware Trust Center Installation

For small deployments, or as a proof-of-concept test, you can deploy the Anyware Trust Center using the included `trust-center-ctl` script. This script will create a single-node Kubernetes cluster and install the Anyware Trust Center and its dependencies.

Deploying the Anyware Trust Center involves the following steps:

1. Create a new VM to host the Anyware Trust Center.
2. Choose a domain name for connections to the Anyware Trust Center.
3. Configure DNS for the new machine.
4. Get the installation script from our website.
5. Run the installation script on the Anyware Trust Center machine.

1. Create a New VM

Deploy a dedicated server to host the Anyware Trust Center. The method used to do this will depend on your environment; if you are unsure how to proceed, ask your system administrators.

The Anyware Trust Center requires a dedicated server with the following specifications:

Requirement	
Operating System	• RHEL 8 • RHEL 9 • Rocky Linux 8 • Rocky Linux 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes. On ESXi or similar hypervisors, the Trust Center does not support installation on **Sparse** (thin) provisioned disks. Please use raw or thick provisioned disks.
Network	• IP network accessible by your endpoints, with configured DNS. The Anyware Trust Center does not support connections via raw IP addresses. • TCP 32443 (Communication with Trusted Zero Clients)

Requirement	
	• TCP 443 (Communication with OTA update CDN)
Python	The post-installation and initialization scripts require Python 3.8.2+.
Other software	The OS must have cURL available.

Test Environment Specifications

The Trust Center has been thoroughly tested on **Amazon EC2 m5a xlarge**, which has the following specifications.

Requirement	
vCPUs	4
Memory	16GB RAM
Memory per vCPU	4GB
Physical Processor	AMD EPYC 7571
Clock Speed	2.5GHz
CPU Architecture	x86_64

Older or **slower VMs** may experience issues during installation, upgrades, or general use of the Trust Center. For optimal performance, we recommend using a **newer instance** or allocating **additional vCPU cores**.

2. Choose a Domain Name

The Anyware Trust Center requires 5 domain names added to your DNS records. In this step, you're creating the *base* domain for the Anyware Trust Center, which will be used to construct the other 4 subdomains. You'll use this value in multiple locations during setup, so record the value and be ready to copy it.

In this procedure, we will use `trust-center.example.com` to demonstrate the domain name, and how it is leveraged to create the other required values.

3. Create DNS Records

Once your new dedicated server has been created, you must set up the following DNS A records that point to it. For each of the following items, replace `<domain-name>` with the domain name you recorded in the previous step.

- `<domain-name>`

  This is the root domain for your Trust Center. This is what is entered on Trusted Zero Clients if `anywaretrustcenter` is not configured on your LAN.

- `api.<domain-name>`

  The api subdomain is used by Endpoint Management Systems to control the Trust Center. Sometimes, the EMS requires the api subdomain to be specified, but often only the { domain-name } is required.

- `endpoint-connector.<domain-name>`

  The endpoint-connector subdomain is used by Trusted Zero Clients to register and communicate with the Trust Center.

- `ota.<domain-name>`

  The ota subdomain is used by Clients to retrieve Over-the-Air updates from the Trust Center.

- `register.<domain-name>`

  The register subdomain is used by Trusted Zero Clients to onboard with the Trust Center.

Info

If you manually enter the Trust Center address, you can either:

- Provide the root domain name like this: `register.<domain-name>`.
- Provide the root domain name without "register". In this scenario, "register" is added to the address as a prefix.

Important: Supporting automatic Anyware Trust Center discovery

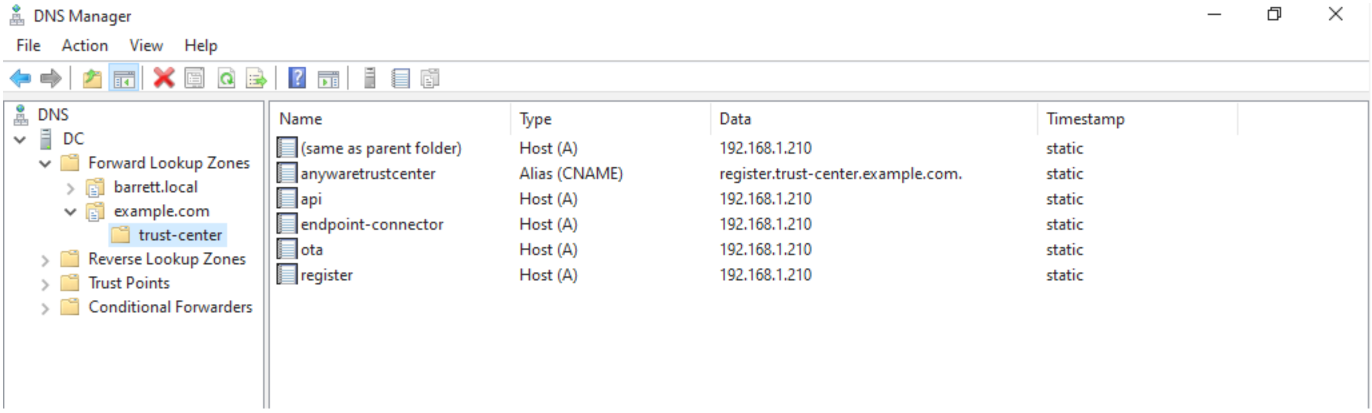
If you plan to support automatic Anyware Trust Center discovery by endpoints, you must also create a CNAME record that redirects `anywaretrustcenter` to `register.<domain-name>`.

Example Illustrating Use of trust-center.example.com

Using `trust-center.example.com` as the base domain, you would create DNS records for the following:

- `trust-center.example.com`
- `api.trust-center.example.com`
- `endpoint-connector.trust-center.example.com`
- `ota.trust-center.example.com`
- `register.trust-center.example.com`

This example shows a different DNS configuration using Windows DNS Manager:



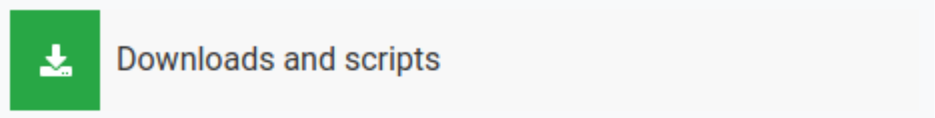
Name	Type	Data	Timestamp
(same as parent folder)	Host (A)	192.168.1.210	static
anywaretrustcenter	Alias (CNAME)	register.trust-center.example.com.	static
api	Host (A)	192.168.1.210	static
endpoint-connector	Host (A)	192.168.1.210	static
ota	Host (A)	192.168.1.210	static
register	Host (A)	192.168.1.210	static

4. Get the Installation Script

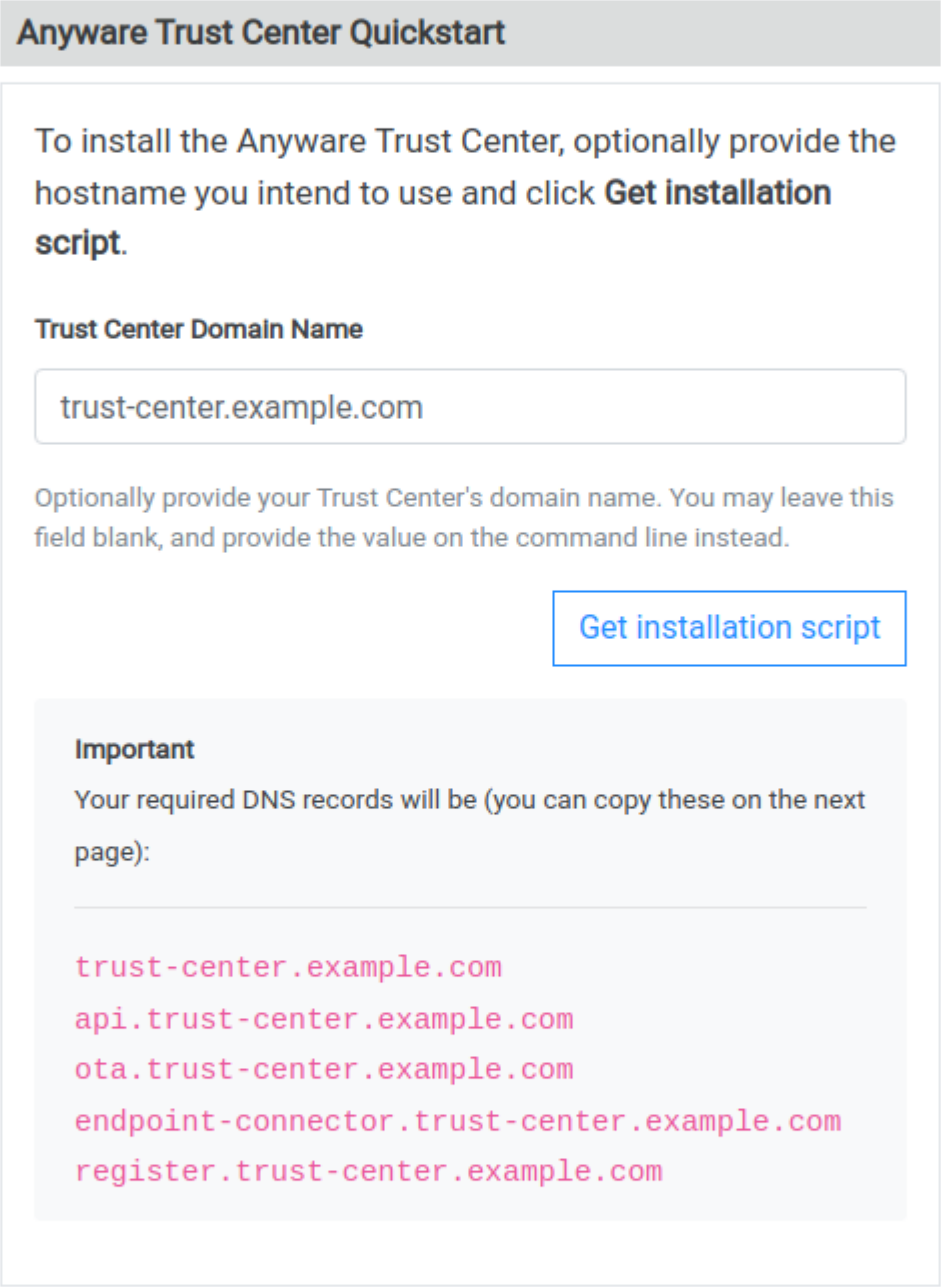
> **Note: Support account is required**
>
> To download the Anyware Trust Center installer, you must have an account on our support site. You can create one from the login screen if you don't already have one.

To download the installer:

1. Go to https://anyware.hp.com/find/product/anyware-trusted-endpoints/current/anyware-trust-center.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**:



4. Read and accept the *End User License Agreement*. Once the agreement has been accepted, the download form is shown:



Anyware Trust Center Quickstart

To install the Anyware Trust Center, optionally provide the hostname you intend to use and click **Get installation script**.

Trust Center Domain Name

trust-center.example.com

Optionally provide your Trust Center's domain name. You may leave this field blank, and provide the value on the command line instead.

Important

Your required DNS records will be (you can copy these on the next page):

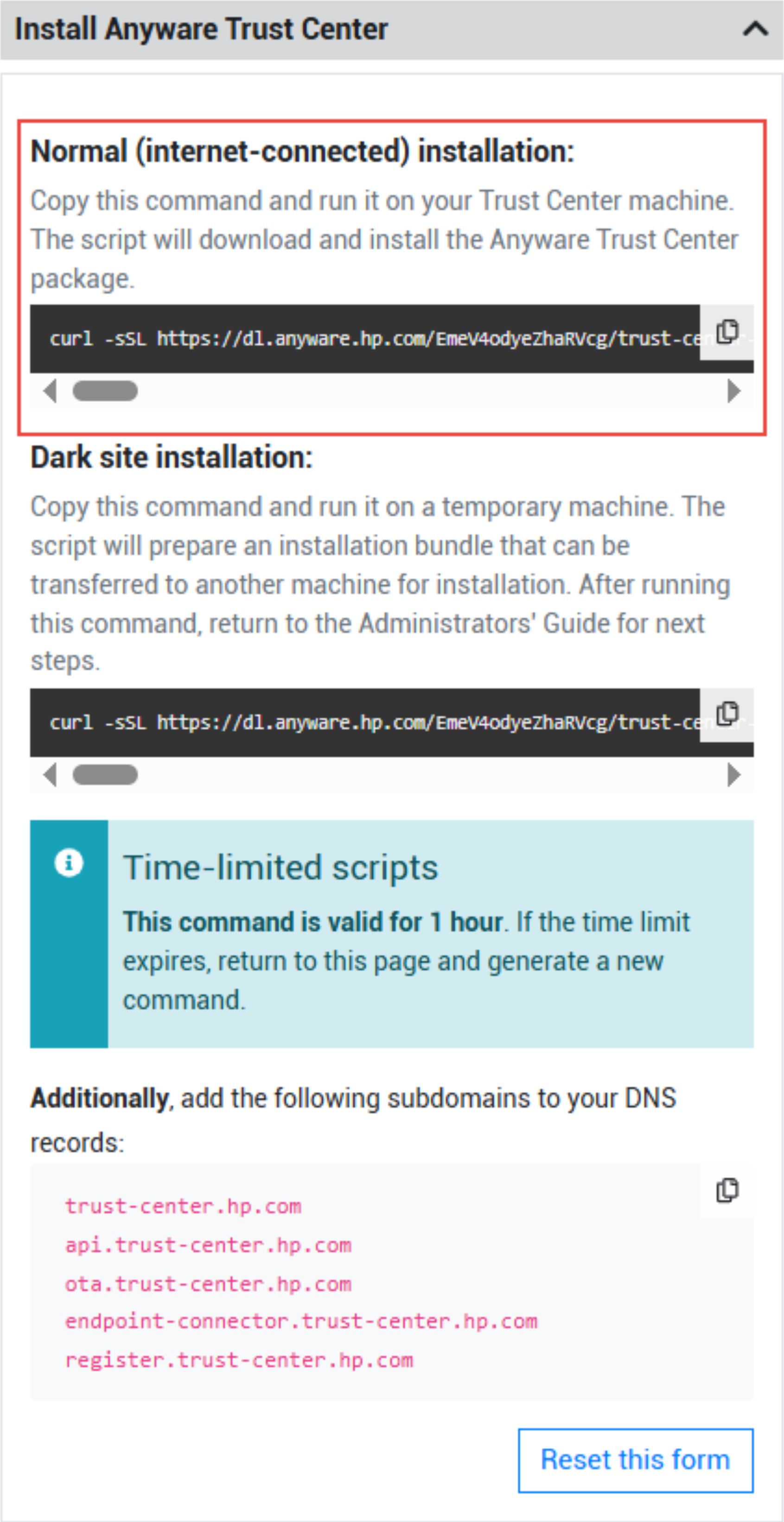
```
trust-center.example.com
api.trust-center.example.com
ota.trust-center.example.com
endpoint-connector.trust-center.example.com
register.trust-center.example.com
```

5. Provide your chosen FQDN—recorded earlier—in the **Trust Center Hostname (FQDN)** field, and click **Get installation script**.

Note: FQDN field is optional

The FQDN value is required to run the installer, but you do not have to supply it here. If you leave this field blank, you must manually add the actual FQDN to the script command before executing it.

The website will generate a download command and display it:



Install Anyware Trust Center

Normal (internet-connected) installation:

Copy this command and run it on your Trust Center machine. The script will download and install the Anyware Trust Center package.

```
curl -sSL https://dl.anyware.hp.com/EmeV4odyeZhaRVcg/trust-ce
```

Dark site installation:

Copy this command and run it on a temporary machine. The script will prepare an installation bundle that can be transferred to another machine for installation. After running this command, return to the Administrators' Guide for next steps.

```
curl -sSL https://dl.anyware.hp.com/EmeV4odyeZhaRVcg/trust-ce
```

Time-limited scripts

This command is valid for 1 hour. If the time limit expires, return to this page and generate a new command.

Additionally, add the following subdomains to your DNS records:

```
trust-center.hp.com
api.trust-center.hp.com
ota.trust-center.hp.com
endpoint-connector.trust-center.hp.com
register.trust-center.hp.com
```

6. Copy the *entire* command displayed under **Normal (internet-connected) installation**. There are two parts, and both are required: a curl command that downloads the installation script, and second command that executes the script.

> **Important: This script is time-limited**
>
> The generated command is valid for 1 hour, after which installation will fail. If that occurs, return to the download page and generate a new command.

The rest of the steps below take place on the Anyware Trust Center VM. If you acquired the script command on a different machine, transfer it to the Anyware Trust Center VM using any acceptable method.

5. Run the Installation Script

1. Create or choose a directory on your newly-created VM, and enter it. The following example will create and enter a new `tc-installation` directory:

   ```
   mkdir tc-installation
   cd tc-installation
   ```

2. In a terminal window, paste the installation script command you copied earlier.

   The installation script will download all required packages and install them on the machine. **The installer takes approximately 15 minutes to complete**. There will be periods of time where the process stops printing messages to the terminal and may appear to hang; this is normal.

   > **Note: Troubleshooting problems**
   >
   > If you encounter breaking issues during installation, see troubleshooting for help.

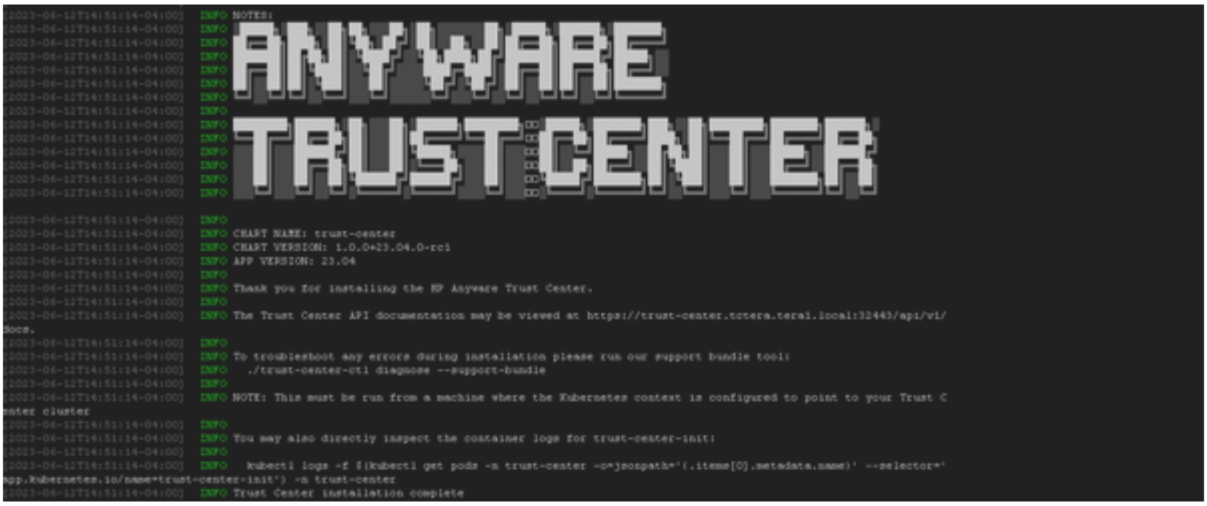
   When executed, the installation command does the following:

   - Downloads the archive for the installer executable
   - Unzips the installer
   - Run the installer as root, passing in two required flags:
   - `fqdn`: The value must be a valid fully-qualified domain name *using only lowercase letters, numbers, and periods*, and should point to the location where the Anyware Trust Center is installed.

- `token`: the JWT token provided by the support site. This value should not be modified, and is valid for one hour after creation.

> **Note: Installation certification errors**
>
> You may see certification errors during installation, which are related to a plugin for Anyware Manager. These errors can be disregarded.

After installation completes, you will see a message similar to this:



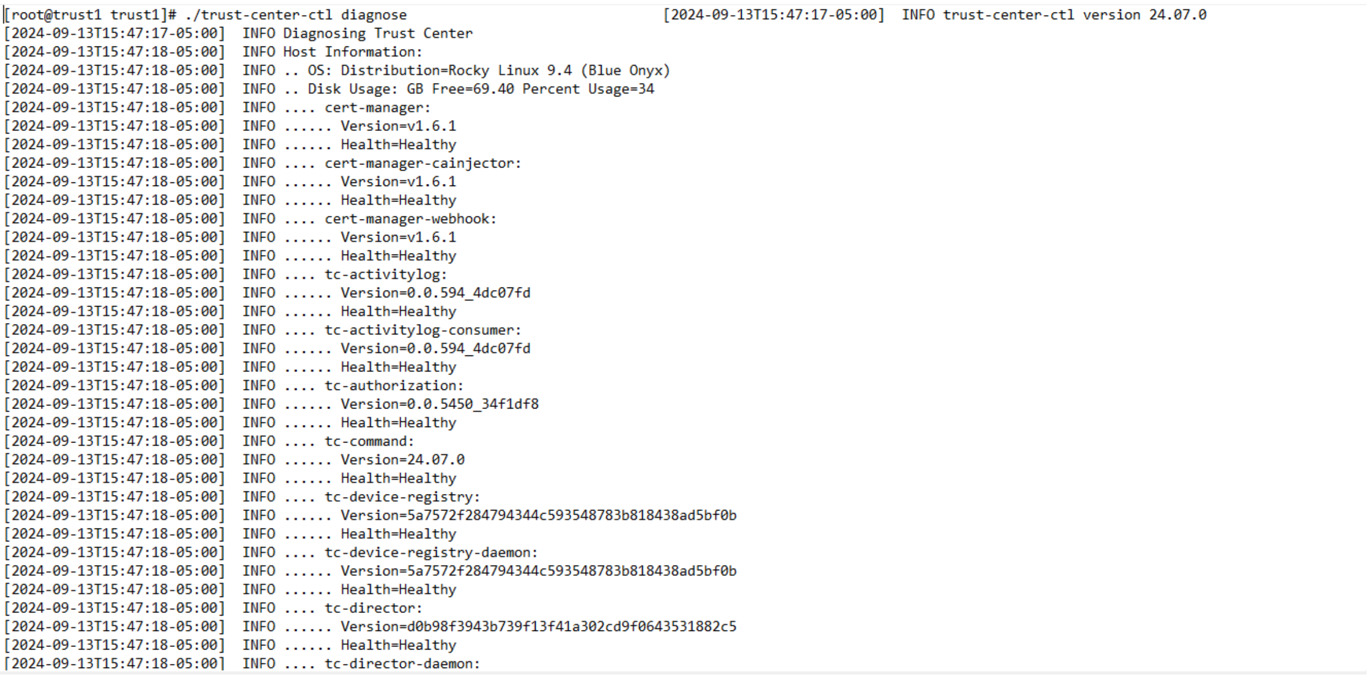
```
[2023-06-12T14:51:14-04:00]  INFO NOTES:
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO

[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO CHART NAME: trust-center
[2023-06-12T14:51:14-04:00]  INFO CHART VERSION: 1.0.0+23.04.0-rc1
[2023-06-12T14:51:14-04:00]  INFO APP VERSION: 23.04
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO Thank you for installing the HP Anyware Trust Center.
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO The Trust Center API documentation may be viewed at https://trust-center.tctera.teral.local:32443/api/v1/
docs.
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO To troubleshoot any errors during installation please run our support bundle tool:
[2023-06-12T14:51:14-04:00]  INFO   ./trust-center-ctl diagnose --support-bundle
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO NOTE: This must be run from a machine where the Kubernetes context is configured to point to your Trust C
enter cluster
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO You may also directly inspect the container logs for trust-center-init:
[2023-06-12T14:51:14-04:00]  INFO
[2023-06-12T14:51:14-04:00]  INFO   kubectl logs -f $(kubectl get pods -n trust-center -o=jsonpath='{.items[0].metadata.name}' --selector='
app.kubernetes.io/name=trust-center-init') -n trust-center
[2023-06-12T14:51:14-04:00]  INFO Trust Center installation complete
```

3. To validate the installation, run the following command:

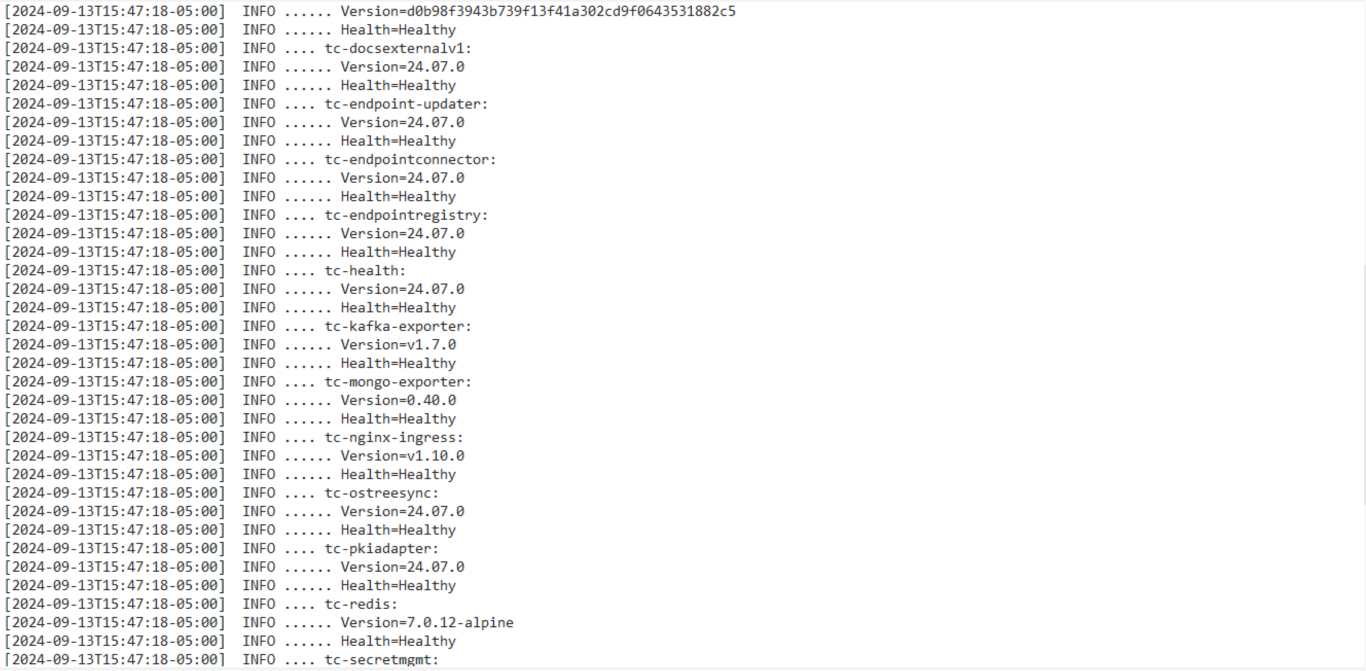
```
sudo ./trust-center-ctl diagnose
```

All services should report healthy.

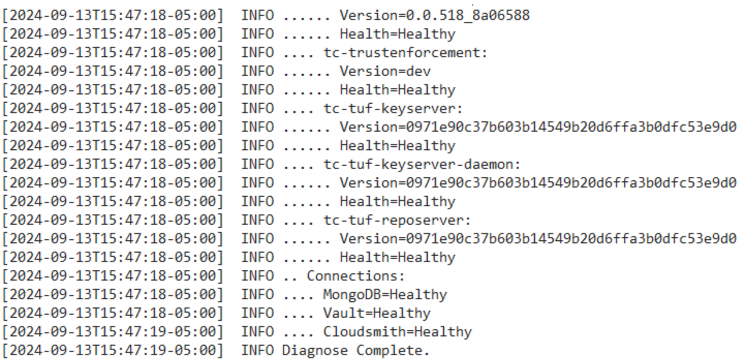
If the diagnostic process finds that the installation completed successfully, you will see log output as shown below, where all service information is indicated as "**Health=Healthy**". You will not see any "**error**" in the log.



```
[root@trust1 trust1]# ./trust-center-ctl diagnose                          [2024-09-13T15:47:17-05:00]  INFO trust-center-ctl version 24.07.0
[2024-09-13T15:47:17-05:00]  INFO Diagnosing Trust Center
[2024-09-13T15:47:18-05:00]  INFO Host Information:
[2024-09-13T15:47:18-05:00]  INFO .. OS: Distribution=Rocky Linux 9.4 (Blue Onyx)
[2024-09-13T15:47:18-05:00]  INFO .. Disk Usage: GB Free=69.40 Percent Usage=34
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager-cainjector:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager-webhook:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-activitylog:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-activitylog-consumer:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-authorization:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.5450_34f1df8
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-command:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-device-registry:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-device-registry-daemon:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-director:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-director-daemon:
```



```
[2024-09-13T15:47:18-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-docsexternalv1:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpoint-updater:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpointconnector:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpointregistry:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-health:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-kafka-exporter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.7.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-mongo-exporter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.40.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-nginx-ingress:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.10.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-ostreesync:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-pkiadapter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-redis:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=7.0.12-alpine
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-secretmgmt:
```

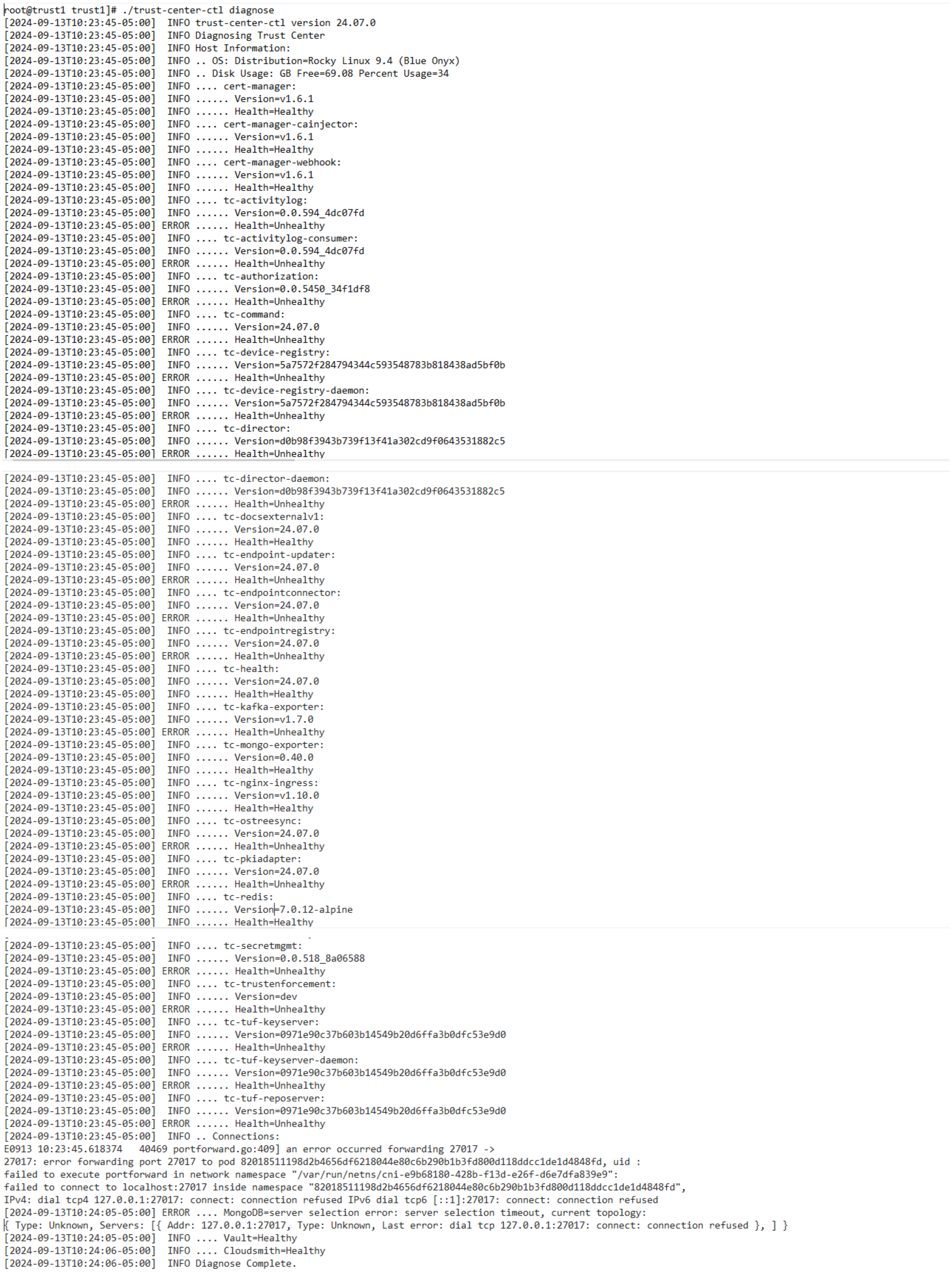


```
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.518_8a06588
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-trustenforcement:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=dev
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-keyserver:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-keyserver-daemon:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-reposerver:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .. Connections:
[2024-09-13T15:47:18-05:00]  INFO .... MongoDB=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... Vault=Healthy
[2024-09-13T15:47:19-05:00]  INFO .... Cloudsmith=Healthy
[2024-09-13T15:47:19-05:00]  INFO Diagnose Complete.
```

If the diagnostic process finds that the installation did not complete successfully, you will see log output as shown below, where **one or more** services indicate an error with "**ERROR ...... Health=Unhealthy**".

The Trust Center may be unhealthy for the following reasons:

- Some databases used in the Trust Center are not compatible with **Sparse (thin) Virtual Disks**. This incompatibility can lead to installation failures without clear error messages. If you encounter an installation failure and are using Sparse Disk Images, switch to **Thick Disk Provisioning**.
- The firewall may be **blocking k3s functionality**. If this is the case, **disable any firewall rules** that could be obstructing k3s local network communications.



```
root@trust1 trust1]# ./trust-center-ctl diagnose
[2024-09-13T10:23:45-05:00]  INFO trust-center-ctl version 24.07.0
[2024-09-13T10:23:45-05:00]  INFO Diagnosing Trust Center
[2024-09-13T10:23:45-05:00]  INFO Host Information:
[2024-09-13T10:23:45-05:00]  INFO .. OS: Distribution=Rocky Linux 9.4 (Blue Onyx)
[2024-09-13T10:23:45-05:00]  INFO .. Disk Usage: GB Free=69.08 Percent Usage=34
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager-cainjector:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager-webhook:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-activitylog:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-activitylog-consumer:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-authorization:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.5450_34f1df8
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-command:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-device-registry:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-device-registry-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-director:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy

[2024-09-13T10:23:45-05:00]  INFO .... tc-director-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-docsexternalv1:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpoint-updater:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpointconnector:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpointregistry:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-health:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-kafka-exporter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.7.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-mongo-exporter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.40.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-nginx-ingress:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.10.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-ostreesync:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-pkiadapter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-redis:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=7.0.12-alpine
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy

[2024-09-13T10:23:45-05:00]  INFO .... tc-secretmgmt:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.518_8a06588
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-trustenforcement:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=dev
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-keyserver:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-keyserver-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-reposerver:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .. Connections:
E0913 10:23:45.618374   40469 portforward.go:409] an error occurred forwarding 27017 ->
27017: error forwarding port 27017 to pod 82018511198d2b4656df6218044e80c6b290b1b3fd800d118ddcc1de1d4848fd, uid :
failed to execute portforward in network namespace "/var/run/netns/cni-e9b68180-428b-f13d-e26f-d6e7dfa839e9":
failed to connect to localhost:27017 inside namespace "82018511198d2b4656df6218044e80c6b290b1b3fd800d118ddcc1de1d4848fd",
IPv4: dial tcp4 127.0.0.1:27017: connect: connection refused IPv6 dial tcp6 [::1]:27017: connect: connection refused
[2024-09-13T10:24:05-05:00] ERROR .... MongoDB=server selection error: server selection timeout, current topology:
{ Type: Unknown, Servers: [{ Addr: 127.0.0.1:27017, Type: Unknown, Last error: dial tcp 127.0.0.1:27017: connect: connection refused }, ] }
[2024-09-13T10:24:05-05:00]  INFO .... Vault=Healthy
[2024-09-13T10:24:06-05:00]  INFO .... Cloudsmith=Healthy
[2024-09-13T10:24:06-05:00]  INFO Diagnose Complete.
```

After Installing

After installation completes, you can set up your management tool to interact and manage Trusted Zero Clients via the Anyware Trust Center.

Refer to the API documentation installed with the Anyware Trust Center for complete details.

Note: The administrator password is automatically generated

The administrator password is automatically generated by the Anyware Trust Center installer, and has the ability to create service account keys. The generated password is placed in the `config.yaml` file in your installation directory.

`<installation_folder>/config.yaml`:

```
global:
images:
    registry: "docker.cloudsmith.io/teradici/trust-center"
    username: "teradici/trust-center"
    password: <repository password>
tc:
    domain: <your domain>
    password: <this is the auto-generated password>
    endpointUpdate:
      accessKey: <repository password>
      repository: "teradici/trusted-zero-client"
```

Troubleshooting

Installation failures

Installation can fail on some distributions or environments unless additional configuration is done. Check the additional configuration requirements listed above. If any steps were missed:

1. Uninstall the Anyware Trust Center
2. Perform the relevant configuration steps
3. Install the Anyware Trust Center again. You will likely need to return to the download site and generate a new download command.

Creating a Support Bundle

Support bundles are archives that capture the current state of the Anyware Trust Center, and are used by our support team to diagnose and troubleshoot issues you may experience.

> **Support Bundle Recommendation**
>
> It is strongly recommended for users to generate a support bundle, before contacting support using the procedure detailed in Creating a Support Bundle.

Checking for a Default Gateway

The Anyware Trust Center requires a default gateway to be set on the dark site machine, even without an internet connection.

To check whether a default gateway exists:

1. Open a console window, and run:

   ```
   ip route | grep default
   ```

   If the response looks similar to this example, then a default route already exists, and you can continue with installation:

   ```
   default via 10.X.X.X dev ens5 proto dhcp src 10.X.X.X metric 100
   ```

2. If the response indicates that no default gateway is present, run the following commands to create a dummy route:

   ```
   ip link add dummy0 type dummy
   ip link set dummy0 up
   ip addr add 203.0.113.254/31 dev dummy0
   ip route add default via 203.0.113.255 dev dummy0 metric 1000
   ```

Troubleshooting Hostname Changes

If the hostname of the machine on which the Anyware Trust Center is installed changes after installation, the Trust Center will not start properly.

To resolve this issue, please follow the troubleshooting steps in troubleshooting.

DarkSite Installation

Overview

The Anyware Trust Center can be installed in darksites, without a connection to the public internet.

Requirements

Existing Requirements for Preparing Trust Center

The requirements to install a Trust Center listed here, are identical to the requirements for running the command to prepare a Trust Center Darksite bundle, with a few additional pre-requisites:

- DNF software package manager is installed
- Docker CE 25.0.1 or greater is required (v25.0.0 had a bug with the "docker save" command)
- Internet connection is required

Info

For darksite installation, the host preparing the bundler must have the following software:

- Docker v25.0.1+
  The Trust Center installer automatically installs Docker if it is not available on the machine.
- cURL
- DNF

High-level Overview of Darksite Installation

Darksite installation involves these general steps:

1. Create a new VM to host the Anyware Trust Center.
2. Choose a domain name for connections to the Anyware Trust Center.

3. Configure DNS for the new machine.
4. Allowlist IP addresses that Cloudsmith uses for their content delivery network.
5. Create dummy gateway, if the machine does not already have a default gateway.
6. Create a temporary VM that will download the required files.
7. Get the installation script from our website.
8. Prepare Trust Center
9. Transfer the files to the production VM.
10. Run the installation script on the Anyware Trust Center machine.

> **Info**
>
> - Ensure that there is no default route before running the commands.
> - The FQDN entered as part of running the prepare command must be accessible within a local network.

1. Create the Darksite Machine

Deploy a dedicated server to host the Anyware Trust Center. You must be able to transfer files to this machine, using USB drives, SSH, or another acceptable method.

The Anyware Trust Center requires a dedicated server with the following specifications (note that the *network* and *software* requirements are different from standard installations):

Requirement	
Operating System	• RHEL 8, 9 • Rocky Linux 9 • CentOS Stream 9
CPUs	4 vCPUs
Memory	16GB RAM
Disk	120GB+, including 80GB+ disk space on `/var` for persistent volumes. On ESXi or similar hypervisors, the Trust Center does not support installation on **Sparse** (thin) provisioned disks. Please use raw or thick provisioned disks.
Network	A default gateway is required, even without an internet connection. If the machine does not have one, a dummy route is required for installation. See Checking for a Default Gateway for instructions.

Requirement	
Software	DNF

TEST ENVIRONMENT SPECIFICATIONS

The above minimum requirements were tested with the following specifications and hardware.

Requirement	
vCPUs	4
Memory	16GB RAM
Memory per vCPU	4GB
Physical Processor	AMD EPYC 7571
Clock Speed	2.5GHz
CPU Architecture	x86_64

Older or **slower servers** may experience issues during installation, upgrades, or general use of the Trust Center. For optimal performance, we recommend using a **modern CPU** or allocating **additional vCPU cores**.

2. Choose a Domain Name

The Anyware Trust Center requires 5 domain names added to your DNS records. In this step, you're creating the *base* domain for the Anyware Trust Center, which will be used to construct the other 4 subdomains. You'll use this value in multiple locations during setup, so record the value and be ready to copy it.

In this procedure, we will use `trust-center.example.com` to demonstrate the domain name, and how it is leveraged to create the other required values.

3. Create DNS Records

Once your new dedicated server has been created, you must set up the following DNS A records that point to it. For each of the following items, replace `<domain-name>` with the domain name you recorded in the previous step.

- `<domain-name>`

This is the root domain for your Trust Center. This is what is entered on Trusted Zero Clients if `anywaretrustcenter` is not configured on your LAN.

- `api.<domain-name>`

  The api subdomain is used by Endpoint Management Systems to control the Trust Center. Sometimes, the EMS requires the api subdomain to be specified, but often only the { domain-name } is required.

- `endpoint-connector.<domain-name>`

  The endpoint-connector subdomain is used by Trusted Zero Clients to register and communicate with the Trust Center.

- `ota.<domain-name>`

  The ota subdomain is used by Clients to retrieve Over-the-Air updates from the Trust Center.

- `register.<domain-name>`

  The register subdomain is used by Trusted Zero Clients to onboard with the Trust Center.

Info

If you manually enter the Trust Center address, you can either:

- Provide the root domain name like this: `register.<domain-name>`.
- Provide the root domain name without "register". In this scenario, "register" is added to the address as a prefix.

Important: Supporting automatic Anyware Trust Center discovery

If you plan to support automatic Anyware Trust Center discovery by endpoints, you must also create a CNAME record that redirects `anywaretrustcenter` to `register.<domain-name>`.

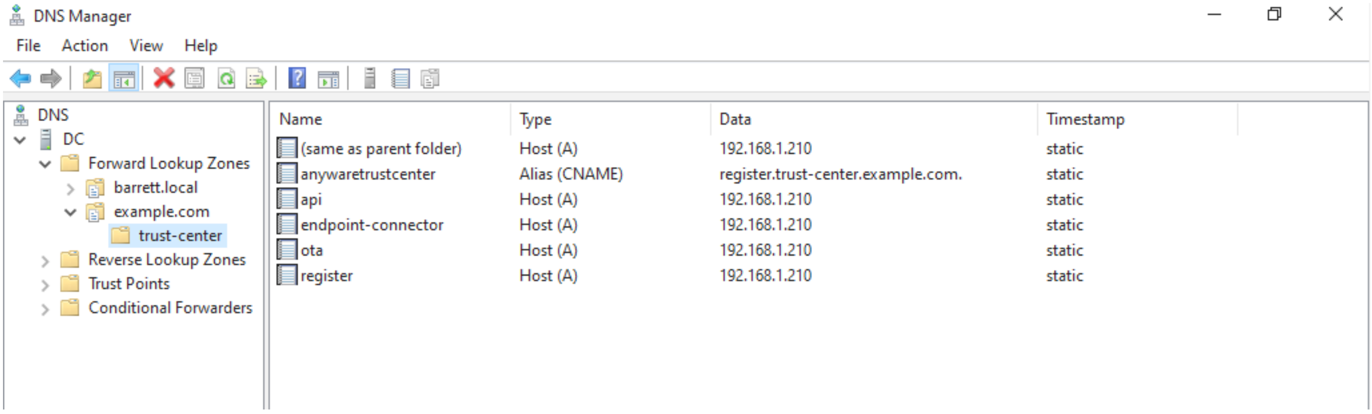
Example Illustrating Use of trust-center.example.com

Using `trust-center.example.com` as the base domain, you would create DNS records for the following:

- `trust-center.example.com`
- `api.trust-center.example.com`

- `endpoint-connector.trust-center.example.com`
- `ota.trust-center.example.com`
- `register.trust-center.example.com`

This example shows a different DNS configuration using Windows DNS Manager:



Name	Type	Data	Timestamp
(same as parent folder)	Host (A)	192.168.1.210	static
anywaretrustcenter	Alias (CNAME)	register.trust-center.example.com.	static
api	Host (A)	192.168.1.210	static
endpoint-connector	Host (A)	192.168.1.210	static
ota	Host (A)	192.168.1.210	static
register	Host (A)	192.168.1.210	static

4. Allowlist Cloudsmith IP Addresses

If you use an IP-based allowlist, we recommend your IT team add the following IP addresses to your allowlist:

- 34.252.163.216
- 52.208.86.0
- 108.129.59.129
- 18.224.75.239
- 18.216.17.80
- 3.135.162.154
- 35.163.82.210
- 52.24.213.62
- 54.203.138.156
- 3.104.99.235
- 52.62.115.207
- 13.55.231.43

These IP addresses are required by Cloudsmith for its content delivery network, and if they are not allowed, the Trust Center installation script cannot be downloaded from our website.

5. Verify or create a default gateway on the darksite machine

The Anyware Trust Center requires a default gateway even when an internet connection is not present. If you are not sure whether your machine already has one, see Checking For a Default Gateway. below, for steps to check and to create one if necessary.

If the machine already has a default gateway, this step is not required.

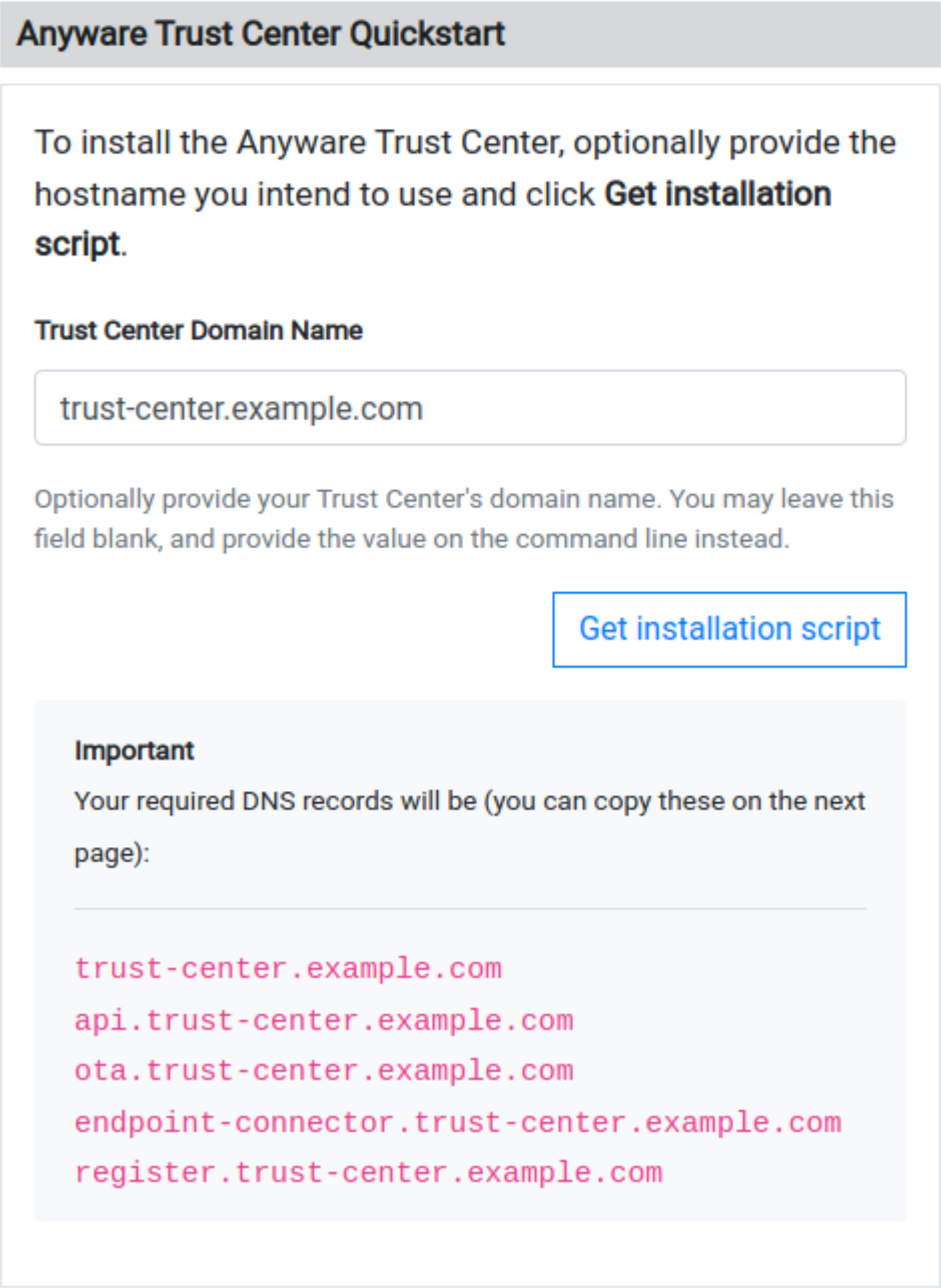
6. Create a temporary internet-connected machine

This machine will be used to download files and create an installer. The bundler machine must meet minimum requirements.

7. Download the installation package and scripts

This procedure is completed from the temporary internet-connected machine:

1. Go to the download website.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**.
4. Read and accept the *End-User License Agreement*. Once the agreement has been accepted, the download form is shown:



Anyware Trust Center Quickstart

To install the Anyware Trust Center, optionally provide the hostname you intend to use and click **Get installation script**.

Trust Center Domain Name

trust-center.example.com

Optionally provide your Trust Center's domain name. You may leave this field blank, and provide the value on the command line instead.

Important

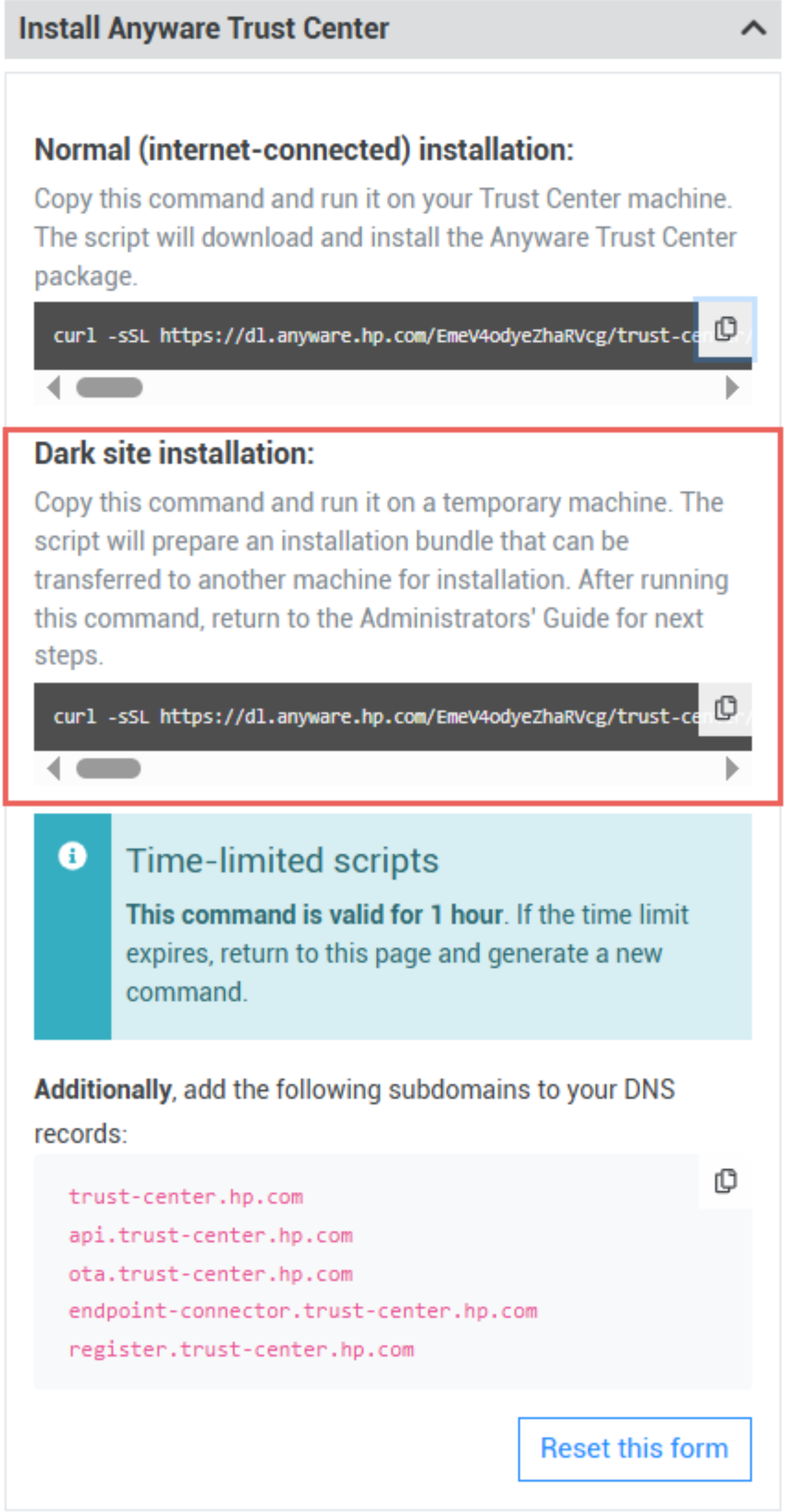
Your required DNS records will be (you can copy these on the next page):

```
trust-center.example.com
api.trust-center.example.com
ota.trust-center.example.com
endpoint-connector.trust-center.example.com
register.trust-center.example.com
```

5. Provide your chosen FQDN—recorded earlier—in the **Trust Center Hostname (FQDN)** field, and click **Get installation script**.

> **Note: FQDN field is optional**
>
> The FQDN value is required to run the installer, but you do not have to supply it here. If you leave this field blank, you must manually add the actual FQDN to the script command before executing it.

6. Under **Dark site installation**, copy the *entire* command displayed. There are two parts, and both are required: a curl command that downloads the installation script, and second command that executes the script.



Install Anyware Trust Center

Normal (internet-connected) installation:

Copy this command and run it on your Trust Center machine. The script will download and install the Anyware Trust Center package.

```
curl -sSL https://dl.anyware.hp.com/EmeV4odyeZhaRVcg/trust-ce
```

Dark site installation:

Copy this command and run it on a temporary machine. The script will prepare an installation bundle that can be transferred to another machine for installation. After running this command, return to the Administrators' Guide for next steps.

```
curl -sSL https://dl.anyware.hp.com/EmeV4odyeZhaRVcg/trust-ce
```

Time-limited scripts

This command is valid for 1 hour. If the time limit expires, return to this page and generate a new command.

Additionally, add the following subdomains to your DNS records:

```
trust-center.hp.com
api.trust-center.hp.com
ota.trust-center.hp.com
endpoint-connector.trust-center.hp.com
register.trust-center.hp.com
```

The following command prepares a Trust Center darksite bundle for installation:

```
sudo ./trust-center-ctl prepare install --fqdn {trust-center-FQDN} --token {jwt token}
```

8. Running the Trust Center Prepare Command

1. Obtain a JWT token from https://docs.teradici.com/find/product/anyware-trusted-endpoints/2023.12/anyware-trust-center.
2. Provision a VM for running the TC prepare command.
3. Use SCP to copy trust-center-ctl binary into VM, and then SSH into VM.
4. Run the following command:

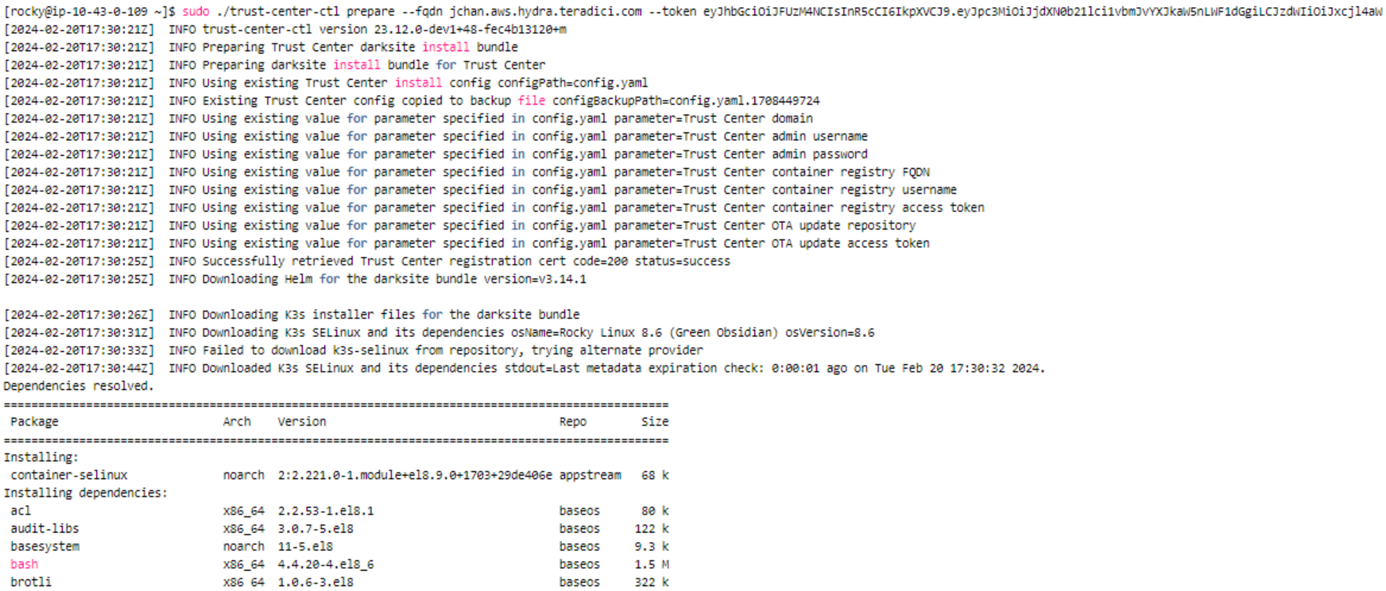
   ```
   sudo ./trust-center-ctl prepare install --fqdn <an fqdn> --token <JWT token from Step 1> --save-path <path to save the darksite bundle>
   ```

   The `--save-path` flag is optional.
5. Once the operation completes, you should see 2 files in the current directory (or in the path specified by `--save-path`):
   - `anyware-trust-center-bundle.tar`
   - `anyware-trust-center-bundle.sha`

> **Important: This script is time-limited**
>
> The generated command is valid for 1 hour. If the token expires before you run it, return to the download page and generate a new command. **The time limit applies to running the *prepare* command, not installing the package**. Once you have successfully generated the installation bundle, you can install the package at any time.

Sample output of TC Prepare Command:

```
sudo ./trust-center-ctl prepare
```



```
[rocky@ip-10-43-0-109 ~]$ sudo ./trust-center-ctl prepare --fqdn jchan.aws.hydra.teradici.com --token eyJhbGciOiJFUzM4NCIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJjdXN0b21lci1vbmJvYXJkaW5nLWF1dGgiLCJzdWIiOiJxcjl4aW
[2024-02-20T17:30:21Z]  INFO trust-center-ctl version 23.12.0-dev1+48-fec4b13120+m
[2024-02-20T17:30:21Z]  INFO Preparing Trust Center darksite install bundle
[2024-02-20T17:30:21Z]  INFO Preparing darksite install bundle for Trust Center
[2024-02-20T17:30:21Z]  INFO Using existing Trust Center install config configPath=config.yaml
[2024-02-20T17:30:21Z]  INFO Existing Trust Center config copied to backup file configBackupPath=config.yaml.1708449724
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center domain
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center admin username
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center admin password
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center container registry FQDN
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center container registry username
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center container registry access token
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center OTA update repository
[2024-02-20T17:30:21Z]  INFO Using existing value for parameter specified in config.yaml parameter=Trust Center OTA update access token
[2024-02-20T17:30:25Z]  INFO Successfully retrieved Trust Center registration cert code=200 status=success
[2024-02-20T17:30:25Z]  INFO Downloading Helm for the darksite bundle version=v3.14.1

[2024-02-20T17:30:26Z]  INFO Downloading K3s installer files for the darksite bundle
[2024-02-20T17:30:31Z]  INFO Downloading K3s SELinux and its dependencies osName=Rocky Linux 8.6 (Green Obsidian) osVersion=8.6
[2024-02-20T17:30:33Z]  INFO Failed to download k3s-selinux from repository, trying alternate provider
[2024-02-20T17:30:44Z]  INFO Downloaded K3s SELinux and its dependencies stdout=Last metadata expiration check: 0:00:01 ago on Tue Feb 20 17:30:32 2024.
Dependencies resolved.
=================================================================================================
 Package                        Arch    Version                                  Repo        Size
=================================================================================================
Installing:
 container-selinux              noarch  2:2.221.0-1.module+el8.9.0+1703+29de406e appstream   68 k
Installing dependencies:
 acl                            x86_64  2.2.53-1.el8.1                           baseos      80 k
 audit-libs                     x86_64  3.0.7-5.el8                              baseos     122 k
 basesystem                     noarch  11-5.el8                                 baseos     9.3 k
 bash                           x86_64  4.4.20-4.el8_6                           baseos     1.5 M
 brotli                         x86 64  1.0.6-3.el8                              baseos     322 k
```

ADDITIONAL NOTES FOR TC PREPARE COMMAND

- Depending on the original setup of the VM, container-selinux package may or may not be installed.
  - k3s-selinux package has container-selinux as a dependency. however, we are locking the version of k3s-selinux, but not the version of container-selinux. This is only an issue if the latest version of container-selinux pulled is not compatiable with v1.4.1 (the current version of k3s-selinux)
  - if the correct repo with k3s-selinux, is already added (this is not implemented within the prepare command), then the prepare command will automatically pull the latest stable version of k3s-selinux
  - **Failed to download k3s-selinux from repository, trying alternate provider** - This is the step that checks whether k3s-selinux is available from one of the repositories added. If not, downloads directly from a remote repo.
- Run `sestatus` to verify that SELinux is enabled on the VM and running. This is a requirement to enable k3s-selinux for K3s server.
- There are a few long running operations without a progress indicator, we can decide whether it is necessary.
- We use the **sha256sum** linux tool to generate the checksum of the tarball. We can add this as a requirement if it is not installed by default.
- The JWT token obtained from the Onboarding JWT Issuer is immediately used by the prepare command to retrieve the TC Reg Cert. That means that there is no expiry for the Trust Center Darksite bundle that is generated i.e. it can be run anytime.

9. Copy downloaded files to the darksite machine

The following files are created by the preparation script. Transfer all three files to the isolated machine that will host the Anyware Trust Center using any acceptable method, such as USB drive or SSH:

- `trust-center-ctl`
- `anyware-trust-center-bundle.tar`
- `anyware-trust-center-bundle.sha`

Place these files in a clearly identified location on the new machine; this will become your installation directory, and subsequent commands will be run there.

Once these files are transferred, the temporary machine is no longer needed.

10. Install Trust Center on the Darksite Machine

Open a terminal window and navigate to your installation directory (the location you used when you copied the installation files). Run the following command:

```
sudo ./trust-center-ctl install darksite
```

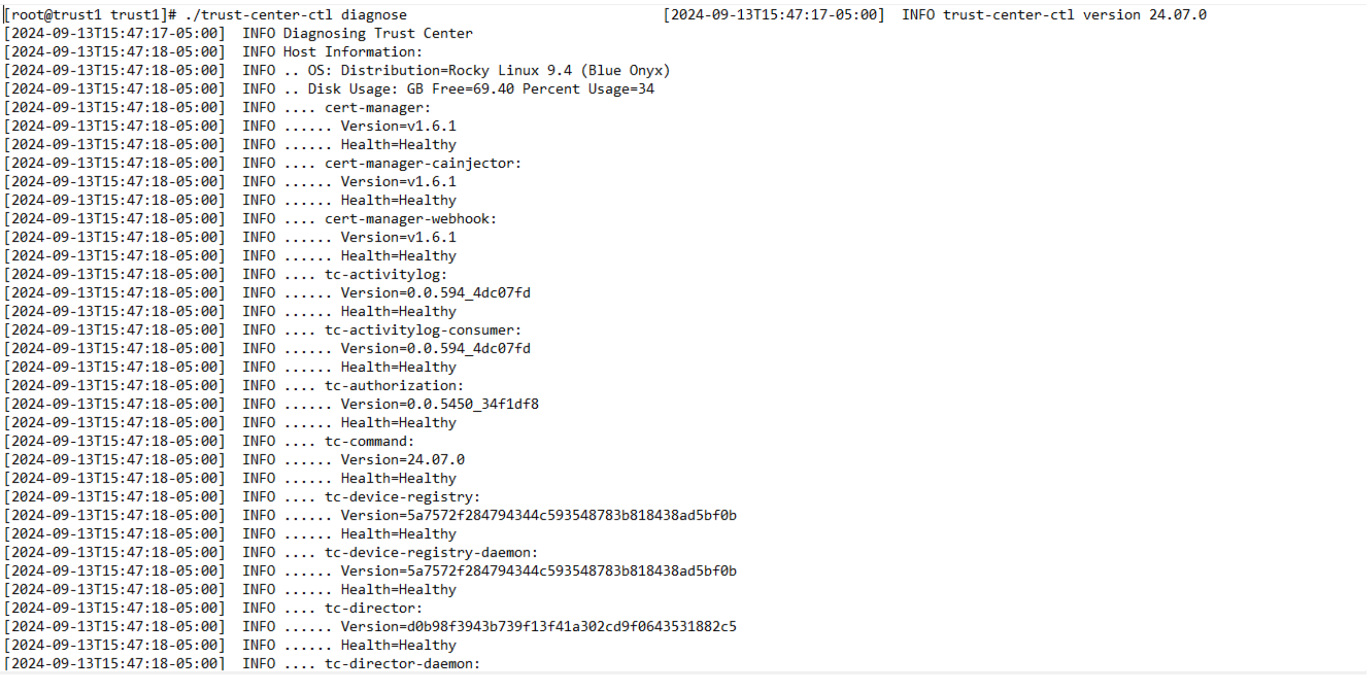
The command installs a new darksite Trust Center.

To validate the installation after it completes, run the following command:

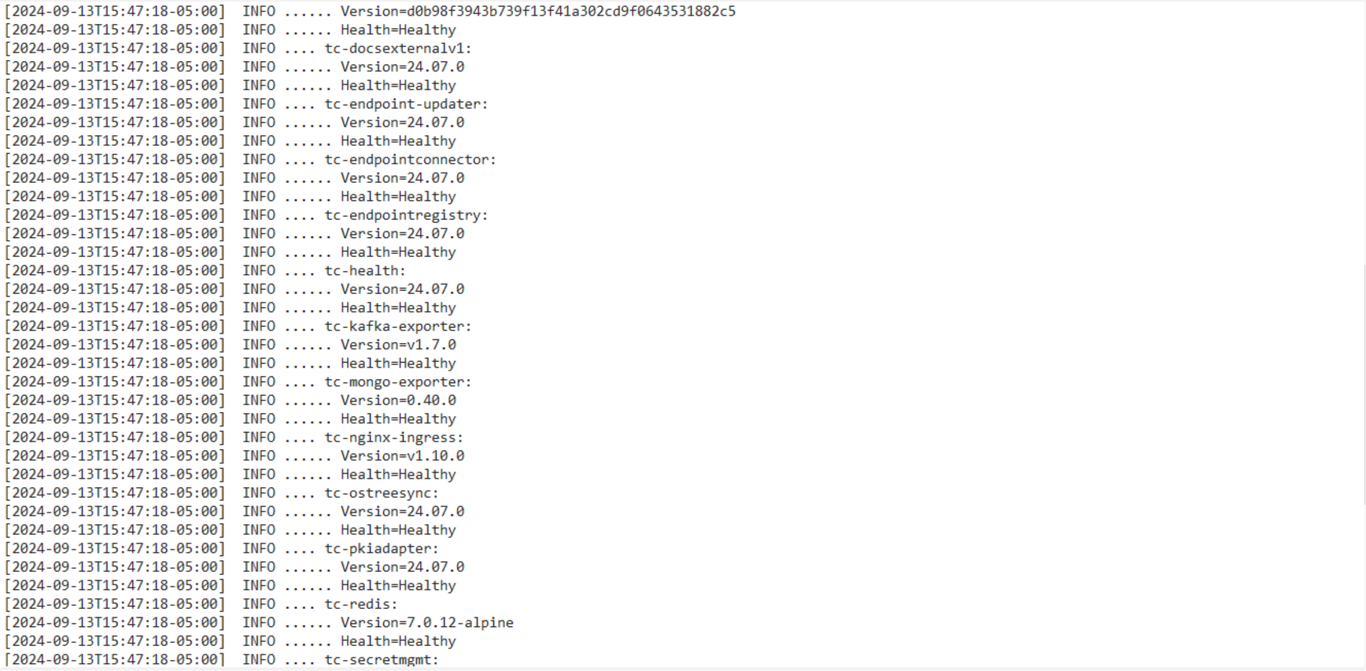
```
sudo ./trust-center-ctl diagnose
```

All services should report healthy.

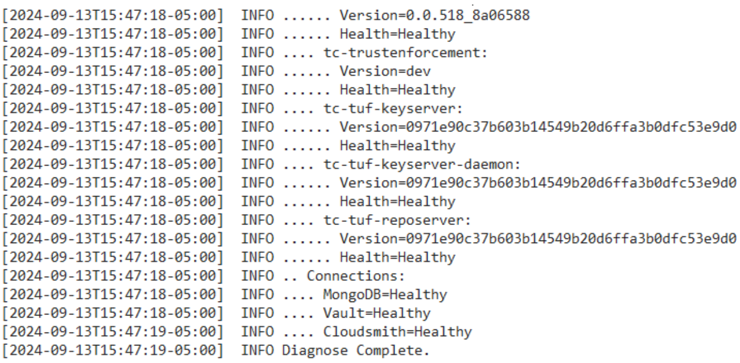
If the diagnostic process finds that the installation completed successfully, you will see log output as shown below, where all service information is indicated as "**Health=Healthy**". You will not see any "**error**" in the log.



```
[root@trust1 trust1]# ./trust-center-ctl diagnose                    [2024-09-13T15:47:17-05:00]  INFO trust-center-ctl version 24.07.0
[2024-09-13T15:47:17-05:00]  INFO Diagnosing Trust Center
[2024-09-13T15:47:18-05:00]  INFO Host Information:
[2024-09-13T15:47:18-05:00]  INFO .. OS: Distribution=Rocky Linux 9.4 (Blue Onyx)
[2024-09-13T15:47:18-05:00]  INFO .. Disk Usage: GB Free=69.40 Percent Usage=34
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager-cainjector:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... cert-manager-webhook:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-activitylog:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-activitylog-consumer:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-authorization:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.5450_34f1df8
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-command:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-device-registry:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-device-registry-daemon:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-director:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-director-daemon:
```



```
[2024-09-13T15:47:18-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-docsexternalv1:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpoint-updater:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpointconnector:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-endpointregistry:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-health:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-kafka-exporter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.7.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-mongo-exporter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.40.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-nginx-ingress:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=v1.10.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-ostreesync:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-pkiadapter:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=24.07.0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-redis:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=7.0.12-alpine
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-secretmgmt:
```

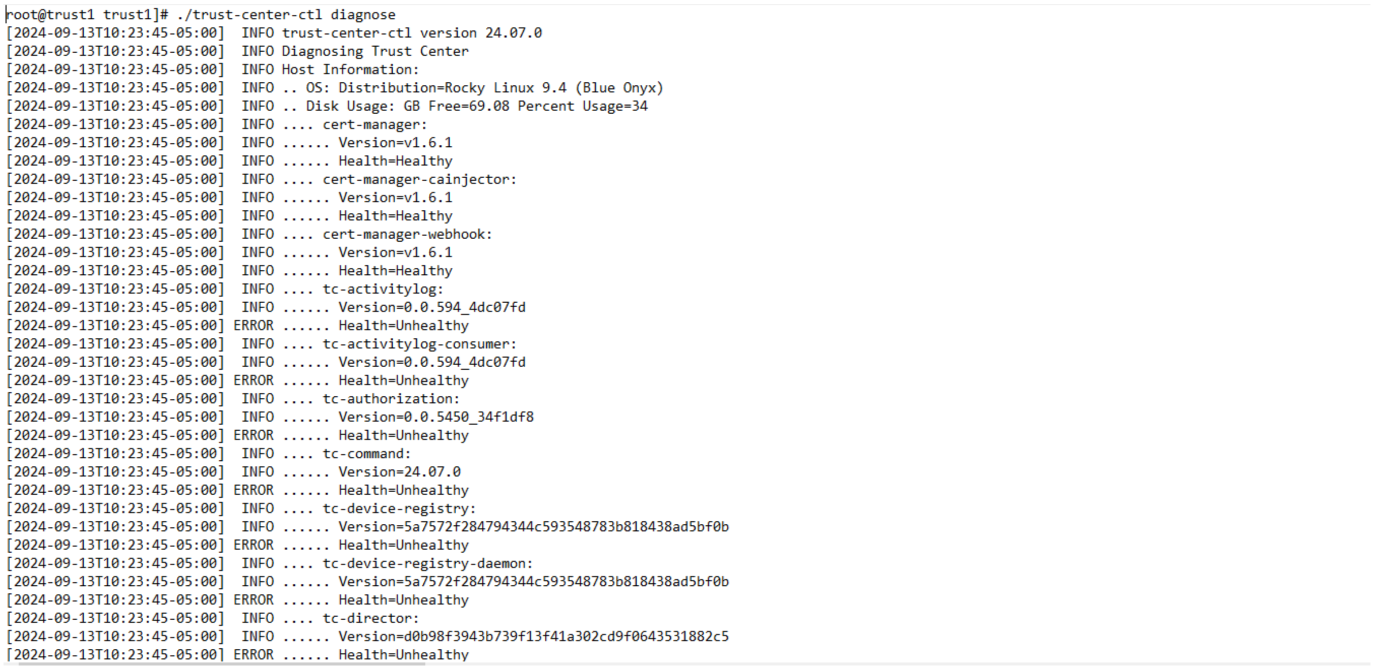


```
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0.0.518_8a06588
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-trustenforcement:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=dev
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-keyserver:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-keyserver-daemon:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... tc-tuf-reposerver:
[2024-09-13T15:47:18-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T15:47:18-05:00]  INFO ...... Health=Healthy
[2024-09-13T15:47:18-05:00]  INFO .. Connections:
[2024-09-13T15:47:18-05:00]  INFO .... MongoDB=Healthy
[2024-09-13T15:47:18-05:00]  INFO .... Vault=Healthy
[2024-09-13T15:47:19-05:00]  INFO .... Cloudsmith=Healthy
[2024-09-13T15:47:19-05:00]  INFO Diagnose Complete.
```

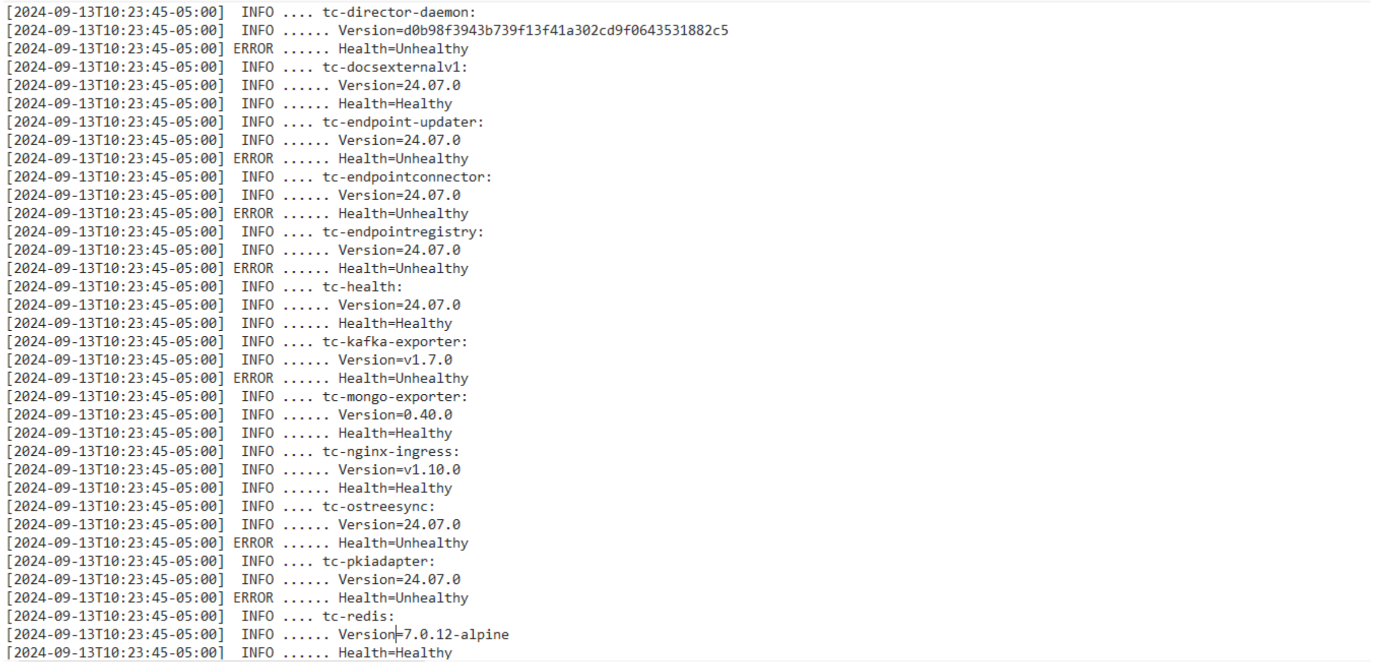
If the diagnostic process finds that the installation did not complete successfully, you will see log output as shown below, where **one or more** services indicate an error with "**ERROR ...... Health=Unhealthy**".

The Trust Center may be unhealthy for the following reasons:

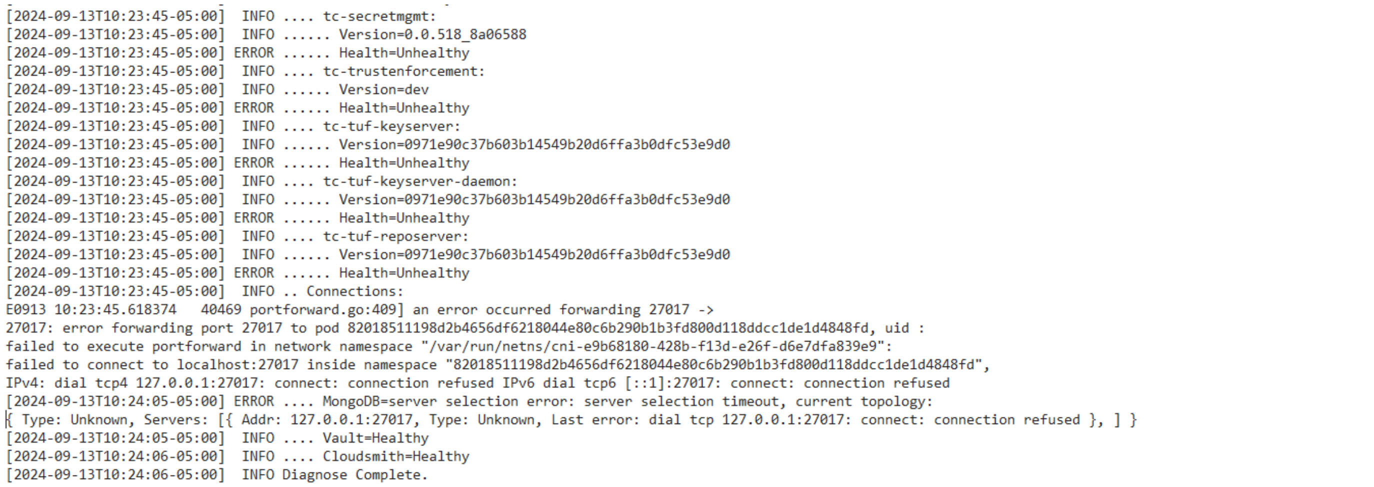
- Some databases used in the Trust Center are not compatible with **Sparse (thin) Virtual Disks**. This incompatibility can lead to installation failures without clear error messages. If you encounter an installation failure and are using Sparse Disk Images, switch to **Thick Disk Provisioning**.
- The firewall may be **blocking k3s functionality**. If this is the case, **disable any firewall rules** that could be obstructing k3s local network communications.



```
root@trust1 trust1]# ./trust-center-ctl diagnose
[2024-09-13T10:23:45-05:00]  INFO trust-center-ctl version 24.07.0
[2024-09-13T10:23:45-05:00]  INFO Diagnosing Trust Center
[2024-09-13T10:23:45-05:00]  INFO Host Information:
[2024-09-13T10:23:45-05:00]  INFO .. OS: Distribution=Rocky Linux 9.4 (Blue Onyx)
[2024-09-13T10:23:45-05:00]  INFO .. Disk Usage: GB Free=69.08 Percent Usage=34
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager-cainjector:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... cert-manager-webhook:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.6.1
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-activitylog:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-activitylog-consumer:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.594_4dc07fd
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-authorization:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.5450_34f1df8
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-command:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-device-registry:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-device-registry-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=5a7572f284794344c593548783b818438ad5bf0b
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-director:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
```



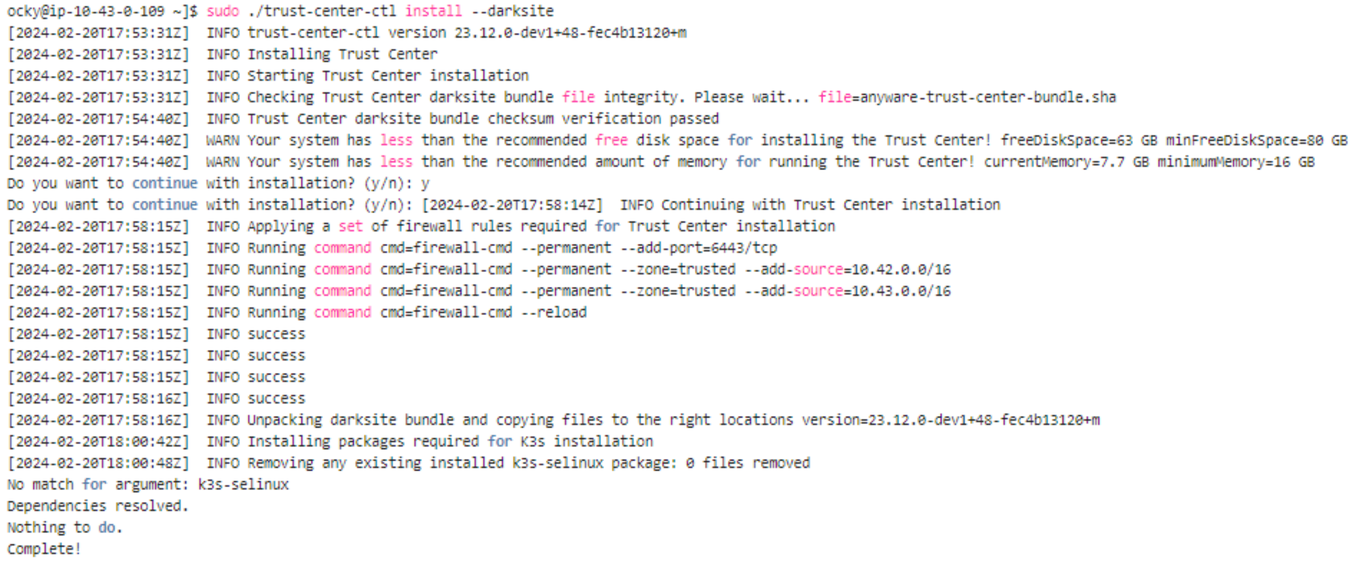
```
[2024-09-13T10:23:45-05:00]  INFO .... tc-director-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=d0b98f3943b739f13f41a302cd9f0643531882c5
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-docsexternalv1:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpoint-updater:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpointconnector:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-endpointregistry:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-health:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-kafka-exporter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.7.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-mongo-exporter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.40.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-nginx-ingress:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=v1.10.0
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-ostreesync:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-pkiadapter:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=24.07.0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-redis:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=7.0.12-alpine
[2024-09-13T10:23:45-05:00]  INFO ...... Health=Healthy
```



```
[2024-09-13T10:23:45-05:00]  INFO .... tc-secretmgmt:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0.0.518_8a06588
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-trustenforcement:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=dev
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-keyserver:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-keyserver-daemon:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .... tc-tuf-reposerver:
[2024-09-13T10:23:45-05:00]  INFO ...... Version=0971e90c37b603b14549b20d6ffa3b0dfc53e9d0
[2024-09-13T10:23:45-05:00] ERROR ...... Health=Unhealthy
[2024-09-13T10:23:45-05:00]  INFO .. Connections:
E0913 10:23:45.618374   40469 portforward.go:409] an error occurred forwarding 27017 ->
27017: error forwarding port 27017 to pod 82018511198d2b4656df6218044e80c6b290b1b3fd800d118ddcc1de1d4848fd, uid :
failed to execute portforward in network namespace "/var/run/netns/cni-e9b68180-428b-f13d-e26f-d6e7dfa839e9":
failed to connect to localhost:27017 inside namespace "82018511198d2b4656df6218044e80c6b290b1b3fd800d118ddcc1de1d4848fd",
IPv4: dial tcp4 127.0.0.1:27017: connect: connection refused IPv6 dial tcp6 [::1]:27017: connect: connection refused
[2024-09-13T10:24:05-05:00] ERROR .... MongoDB=server selection error: server selection timeout, current topology:
{ Type: Unknown, Servers: [{ Addr: 127.0.0.1:27017, Type: Unknown, Last error: dial tcp 127.0.0.1:27017: connect: connection refused }, ] }
[2024-09-13T10:24:05-05:00]  INFO .... Vault=Healthy
[2024-09-13T10:24:06-05:00]  INFO .... Cloudsmith=Healthy
[2024-09-13T10:24:06-05:00]  INFO Diagnose Complete.
```

Sample output of Trust Center Darksite install:

```
sudo ./trust-center-ctl install darksite
```



```
ocky@ip-10-43-0-109 ~]$ sudo ./trust-center-ctl install --darksite
[2024-02-20T17:53:31Z]  INFO trust-center-ctl version 23.12.0-dev1+48-fec4b13120+m
[2024-02-20T17:53:31Z]  INFO Installing Trust Center
[2024-02-20T17:53:31Z]  INFO Starting Trust Center installation
[2024-02-20T17:53:31Z]  INFO Checking Trust Center darksite bundle file integrity. Please wait... file=anyware-trust-center-bundle.sha
[2024-02-20T17:54:40Z]  INFO Trust Center darksite bundle checksum verification passed
[2024-02-20T17:54:40Z]  WARN Your system has less than the recommended free disk space for installing the Trust Center! freeDiskSpace=63 GB minFreeDiskSpace=80 GB
[2024-02-20T17:54:40Z]  WARN Your system has less than the recommended amount of memory for running the Trust Center! currentMemory=7.7 GB minimumMemory=16 GB
Do you want to continue with installation? (y/n): y
Do you want to continue with installation? (y/n): [2024-02-20T17:58:14Z]  INFO Continuing with Trust Center installation
[2024-02-20T17:58:15Z]  INFO Applying a set of firewall rules required for Trust Center installation
[2024-02-20T17:58:15Z]  INFO Running command cmd=firewall-cmd --permanent --add-port=6443/tcp
[2024-02-20T17:58:15Z]  INFO Running command cmd=firewall-cmd --permanent --zone=trusted --add-source=10.42.0.0/16
[2024-02-20T17:58:15Z]  INFO Running command cmd=firewall-cmd --permanent --zone=trusted --add-source=10.43.0.0/16
[2024-02-20T17:58:15Z]  INFO Running command cmd=firewall-cmd --reload
[2024-02-20T17:58:15Z]  INFO success
[2024-02-20T17:58:15Z]  INFO success
[2024-02-20T17:58:15Z]  INFO success
[2024-02-20T17:58:16Z]  INFO success
[2024-02-20T17:58:16Z]  INFO Unpacking darksite bundle and copying files to the right locations version=23.12.0-dev1+48-fec4b13120+m
[2024-02-20T18:00:42Z]  INFO Installing packages required for K3s installation
[2024-02-20T18:00:48Z]  INFO Removing any existing installed k3s-selinux package: 0 files removed
No match for argument: k3s-selinux
Dependencies resolved.
Nothing to do.
Complete!
```

After Installing

After installation completes, you can set up your management tool to interact and manage Trusted Zero Clients via the Anyware Trust Center.

Refer to the API documentation installed with the Anyware Trust Center for complete details.

Note: The administrator password is automatically generated

The administrator password is automatically generated by the Anyware Trust Center installer, and has the ability to create service account keys. The generated password is placed in the `config.yaml` file in your installation directory.

`<installation_folder>/config.yaml`:

```
global:
images:
    registry: "docker.cloudsmith.io/teradici/trust-center"
    username: "teradici/trust-center"
    password: <repository password>
tc:
    domain: <your domain>
    password: <this is the auto-generated password>
    endpointUpdate:
      accessKey: <repository password>
      repository: "teradici/trusted-zero-client"
```

After installation, run the following command to prepare a Trust Center darksite bundle for upgrade:

```
trust-center-ctl prepare upgrade
```

To upgrade an existing darksite Trust Center, run the following command:

```
trust-center-ctl upgrade darksite
```

Checking for a Default Gateway

The Anyware Trust Center requires a default gateway to be set on the darksite machine, even without an internet connection.

To check whether a default gateway exists:

1. Open a console window, and run:

   ```
   ip route | grep default
   ```

If the response looks similar to this example, then a default route already exists, and you can continue with installation:

```
default via 10.X.X.X dev ens5 proto dhcp src 10.X.X.X metric 100
```

2. If the response indicates that no default gateway is present, run the following commands to create a dummy route:

```
ip link add dummy0 type dummy
ip link set dummy0 up
ip addr add 203.0.113.254/31 dev dummy0
ip route add default via 203.0.113.255 dev dummy0 metric 1000
```

Trust Center Installation with DISA STIGs

Virtual machines and physical servers are commonly deployed with a set of security policies/ configurations applied, based on the US DoD's Security Technical Implementation Guides (STIGs). This environment enforces additional security controls, such as file access policies.

To run the Trust Center installer in version 24.10, manual configuration of the `fapolicyd` directive was necessary. With version 25.03, this daemon is included in the DISA STIG policy set. As a result, the `fapolicyd` directive is automatically configured when the Trust Center is installed using the `trust-center-ctl` command. When upgrading to version 25.03, the Trust Center will automatically ensure the correct configuration without manual intervention.

Installation Steps

1. Edit `/etc/yum.conf` and disable the local package GPG signature check requirement:

   ```
   localpkg_gpgcheck=0
   ```

2. Install the Trust Center. Follow the instructions in the topic suited that apply to your scenario:
3. Single-Node Installation
4. Dark Site Installation
5. Upgrading
6. Dark Site Upgrade

Upgrading the Anyware Trust Center

You can upgrade your Anyware Trust Center by running an upgrade script that we provide. The script will download the new package and automatically upgrade your installation.

Note: Upgrade compatibility

The version upgrade compatibilities follow the same guidelines as a normal Trust Center install. Users should only attempt to upgrade a Trust Center by one major release, for which the Anyware team currently provides support. The upgrade compatibility process will be revised in the future, removing the need for incremental upgrades.

Current Trust Center Version	Allowed Upgrade Trust Center Version
23.12	24.03
24.03	24.07
24.07	24.10
24.10	25.03

Note: Support account is required

To download the new Anyware Trust Center package, you must have an account on our support site (https://help.teradici.com). You can create one from the login screen if you don't already have one.

Logs

Users can refer the below paths for the log files:

Location	Description
/var/log/teradici/trust-center-ctl/install_.log	Trust Center installation or TC prepare log file
/var/log/teradici/trust-center-ctl/upgrade_.log	Trust Center upgrade or TC prepare log file

Location	Description
/var/log/teradici/trust-center-ctl/darksite_.log	Trust Center Dark Site install or upgrade dark site log file

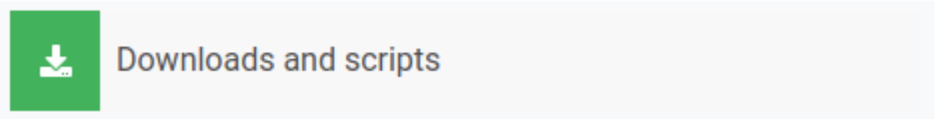
Upgrade Order for the Trusted Endpoints System

Follow this order to upgrade the Trusted Endpoints System:

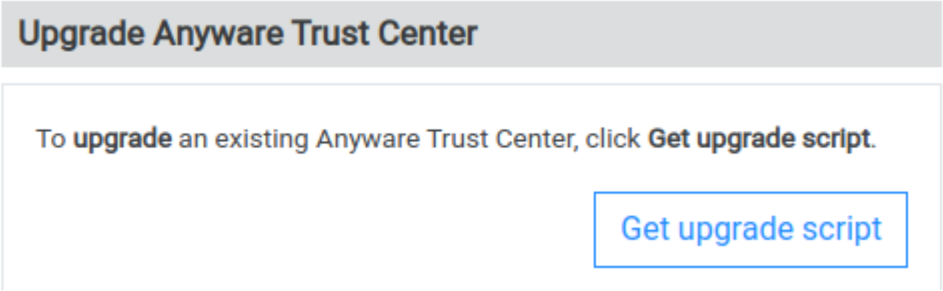
Step I: Upgrade your *Endpoint Management Software (EMS)*. For instructions, consult the documentation of the EMS you are using.
Step II: Upgrade the Trust Center.
Step III: Upgrade your Trusted Zero Clients.

Upgrade Procedure

1. Go to https://anyware.hp.com/find/product/anyware-trusted-endpoints/2025.03/anyware-trust-center.
2. If you are not already logged in, click **Log in to download** and authenticate your session.
3. Click **Downloads and scripts**:

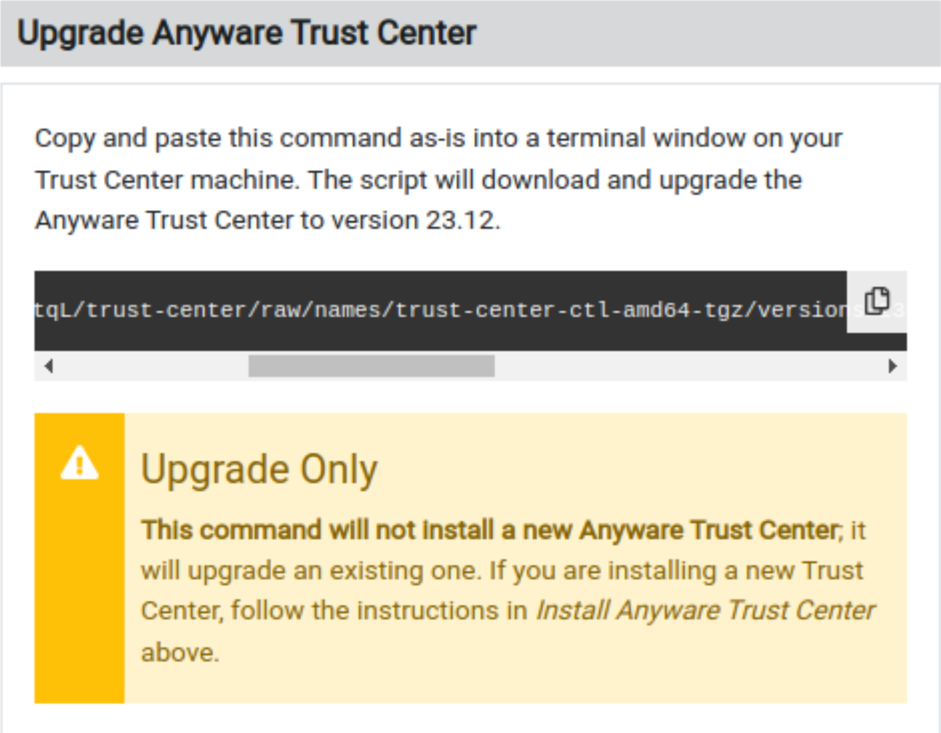


4. Read and accept the *End User License Agreement*. On the next screen, find the *Upgrade Anyware Trust Center* section, and click the **Get upgrade script** button.:


Upgrade Anyware Trust Center

To **upgrade** an existing Anyware Trust Center, click **Get upgrade script**.

5. The website will generate an upgrade command and display it:



Upgrade Anyware Trust Center

Copy and paste this command as-is into a terminal window on your Trust Center machine. The script will download and upgrade the Anyware Trust Center to version 23.12.

```
tqL/trust-center/raw/names/trust-center-ctl-amd64-tgz/version
```

Upgrade Only

This command will not install a new Anyware Trust Center; it will upgrade an existing one. If you are installing a new Trust Center, follow the instructions in *Install Anyware Trust Center* above.

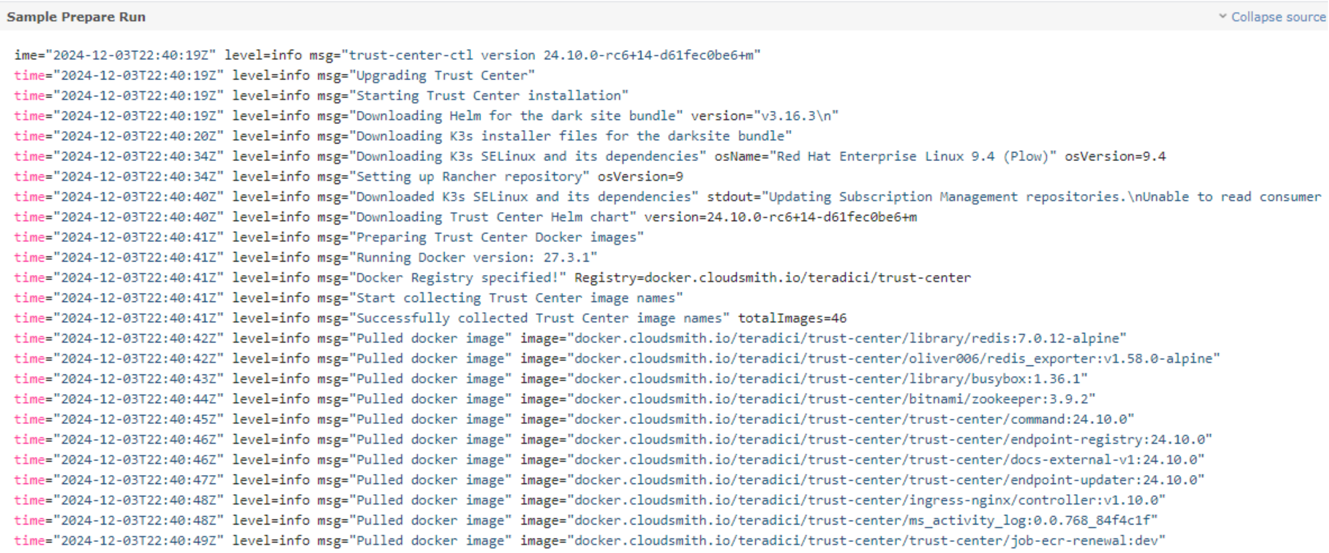
Copy the *entire* command displayed. There are two parts, and both are required: a curl command that downloads the new package, and second command that executes the script.

The upgrade script command looks like this:

```
sudo ./trust-center-ctl prepare upgrade
```

The command `sudo ./trust-center-ctl prepare upgrade` prepare a Trust Center Dark site bundle for upgrade.

Example output of running TC Prepare command:



Sample Prepare Run

```
ime="2024-12-03T22:40:19Z" level=info msg="trust-center-ctl version 24.10.0-rc6+14-d61fec0be6+m"
time="2024-12-03T22:40:19Z" level=info msg="Upgrading Trust Center"
time="2024-12-03T22:40:19Z" level=info msg="Starting Trust Center installation"
time="2024-12-03T22:40:19Z" level=info msg="Downloading Helm for the dark site bundle" version="v3.16.3\n"
time="2024-12-03T22:40:20Z" level=info msg="Downloading K3s installer files for the darksite bundle"
time="2024-12-03T22:40:34Z" level=info msg="Downloading K3s SELinux and its dependencies" osName="Red Hat Enterprise Linux 9.4 (Plow)" osVersion=9.4
time="2024-12-03T22:40:34Z" level=info msg="Setting up Rancher repository" osVersion=9
time="2024-12-03T22:40:40Z" level=info msg="Downloaded K3s SELinux and its dependencies" stdout="Updating Subscription Management repositories.\nUnable to read consumer
time="2024-12-03T22:40:40Z" level=info msg="Downloading Trust Center Helm chart" version=24.10.0-rc6+14-d61fec0be6+m
time="2024-12-03T22:40:41Z" level=info msg="Preparing Trust Center Docker images"
time="2024-12-03T22:40:41Z" level=info msg="Running Docker version: 27.3.1"
time="2024-12-03T22:40:41Z" level=info msg="Docker Registry specified!" Registry=docker.cloudsmith.io/teradici/trust-center
time="2024-12-03T22:40:41Z" level=info msg="Start collecting Trust Center image names"
time="2024-12-03T22:40:41Z" level=info msg="Successfully collected Trust Center image names" totalImages=46
time="2024-12-03T22:40:42Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/library/redis:7.0.12-alpine"
time="2024-12-03T22:40:42Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/oliver006/redis_exporter:v1.58.0-alpine"
time="2024-12-03T22:40:43Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/library/busybox:1.36.1"
time="2024-12-03T22:40:44Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/bitnami/zookeeper:3.9.2"
time="2024-12-03T22:40:45Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/command:24.10.0"
time="2024-12-03T22:40:46Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-registry:24.10.0"
time="2024-12-03T22:40:46Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/docs-external-v1:24.10.0"
time="2024-12-03T22:40:47Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-updater:24.10.0"
time="2024-12-03T22:40:48Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/ingress-nginx/controller:v1.10.0"
time="2024-12-03T22:40:48Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/ms_activity_log:0.0.768_84f4c1f"
time="2024-12-03T22:40:49Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/job-ecr-renewal:dev"
```

6. On the Anyware Trust Center VM, open a terminal window and navigate to the same directory used to install the original Anyware Trust Center.
7. Paste the command you copied in step 5 and press **Enter**.

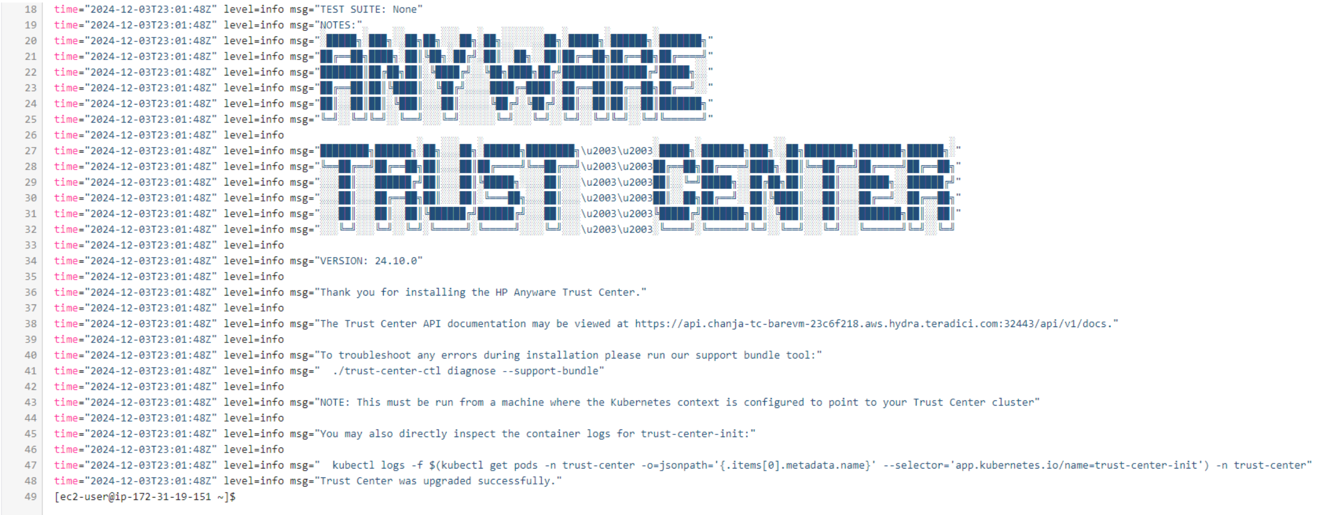
> **Important: Upgrade must run in the Installation directory**
>
> The upgrade script must be run in the same directory used to install the Anyware Trust Center. If you run the script in a different location, the package will be downloaded but the upgrade script will fail.

The command will download the new package and execute an upgrade script.

8. To upgrade an existing Trust Center Dark Site, run the following command:

```
sudo ./trust-center-ctl upgrade darksite
```

Example output of running TC Upgrade Darksite command:



```
time="2024-12-03T23:01:48Z" level=info msg="TEST SUITE: None"
time="2024-12-03T23:01:48Z" level=info msg="NOTES:"
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003"
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003"
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003"
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003"
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003"
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="VERSION: 24.10.0"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="Thank you for installing the HP Anyware Trust Center."
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="The Trust Center API documentation may be viewed at https://api.chanja-tc-barevm-23c6f218.aws.hydra.teradici.com:32443/api/v1/docs."
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="To troubleshoot any errors during installation please run our support bundle tool:"
time="2024-12-03T23:01:48Z" level=info msg="  ./trust-center-ctl diagnose --support-bundle"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="NOTE: This must be run from a machine where the Kubernetes context is configured to point to your Trust Center cluster"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="You may also directly inspect the container logs for trust-center-init:"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="  kubectl logs -f $(kubectl get pods -n trust-center -o=jsonpath='{.items[0].metadata.name}' --selector='app.kubernetes.io/name=trust-center-init') -n trust-center"
time="2024-12-03T23:01:48Z" level=info msg="Trust Center was upgraded successfully."
[ec2-user@ip-172-31-19-151 ~]$
```

Upload OTA packages to Darksite Trust Center

Since darksite Trust Center cannot access external internet, OTA updates cannot be retrieved automatically.

Consequently, the following steps must be performed before uploading the OTA packages to the Darksite Trust Center:

- The token required to download the firmware must be obtained first obtained from the website.
- Firmware packages must be downloaded from an internet-connected Trust Center.

Info

The `trust-center-ctl` command is used for the following purposes:

- To download the firmware packages on the internet-connected Trust Center.
- To upload the firmware on the Darksite Trust Center.

1. To list the firmware available to download into your Trust Center, run this command on the internet-connected Trust Center:

```
sudo ./trust-center-ctl firmware list
```

2. On the Downloads site, go to **Downloads and scripts** > **Darksite OTA update tokens**, and click **Generate upgrade token** to obtain the time-limited token for the firmware of your interest.
3. Copy the token to a text file.
4. Run the following command to download firmware:

   ```
   sudo ./trust-center-ctl download --token <token> <version>
   ```

5. To upload firmware (use `---help` to see available flags), run the following command:

   ```
   sudo ./trust-center-ctl upload <flags>
   ```

Upgrading the Darksite Trust Center

Upgrading Darksite Trust Center is similar to upgrading an internet-connected Trust Center. However, since there is no internet access within a darksite, you must do the following:

- Prepare the Trust Center installation bundle,
- Run the `prepare` command on an internet-connected machine with necessary content to perform the upgrade,
- Upgrade an existing darksite Trust Center, and
- Upload OTA packages on a darksite Trust Center.

Step I: Preparing a Trust Center Bundle

You can use an internet-connected machine to prepare for a darksite installation. Before you begin, you must prepare an installation bundle as described in Bundler System Requirements.

Info

The version upgrade compatibilities follow the same guidelines as an internet-connected Trust Center install. Only attempt to upgrade a Trust Center by one major release, for which the Anyware team currently provides support. The upgrade compatibility process will be revised in the future, removing the need for incremental upgrades.

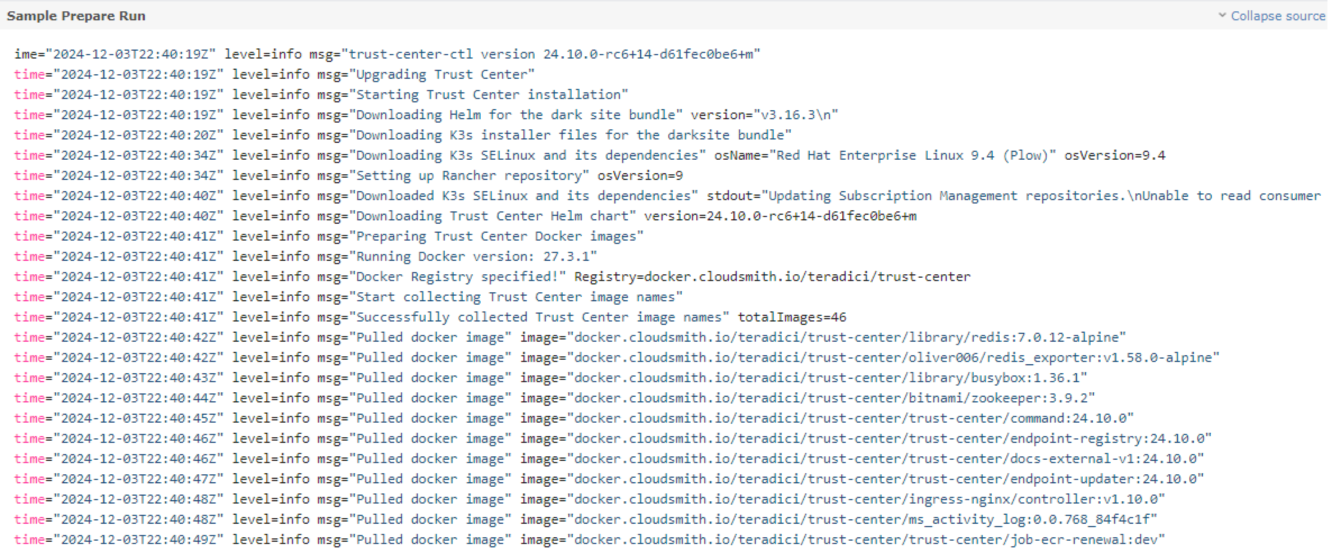
Current Trust Center Version	Allowed Upgrade Trust Center Version
23.12	24.03
24.03	24.07
24.07	24.10
24.10	25.03

Step II: Prepare the Internet-connected Machine

1. Run the following command to prepare a darksite Trust Center bundle for upgrade:

   ```
   sudo ./trust-center-ctl prepare upgrade
   ```

   Example output of running TC Prepare command:

   ```
   ime="2024-12-03T22:40:19Z" level=info msg="trust-center-ctl version 24.10.0-rc6+14-d61fec0be6+m"
   time="2024-12-03T22:40:19Z" level=info msg="Upgrading Trust Center"
   time="2024-12-03T22:40:19Z" level=info msg="Starting Trust Center installation"
   time="2024-12-03T22:40:19Z" level=info msg="Downloading Helm for the dark site bundle" version="v3.16.3\n"
   time="2024-12-03T22:40:20Z" level=info msg="Downloading K3s installer files for the darksite bundle"
   time="2024-12-03T22:40:34Z" level=info msg="Downloading K3s SELinux and its dependencies" osName="Red Hat Enterprise Linux 9.4 (Plow)" osVersion=9.4
   time="2024-12-03T22:40:34Z" level=info msg="Setting up Rancher repository" osVersion=9
   time="2024-12-03T22:40:40Z" level=info msg="Downloaded K3s SELinux and its dependencies" stdout="Updating Subscription Management repositories.\nUnable to read consumer
   time="2024-12-03T22:40:40Z" level=info msg="Downloading Trust Center Helm chart" version=24.10.0-rc6+14-d61fec0be6+m
   time="2024-12-03T22:40:41Z" level=info msg="Preparing Trust Center Docker images"
   time="2024-12-03T22:40:41Z" level=info msg="Running Docker version: 27.3.1"
   time="2024-12-03T22:40:41Z" level=info msg="Docker Registry specified!" Registry=docker.cloudsmith.io/teradici/trust-center
   time="2024-12-03T22:40:41Z" level=info msg="Start collecting Trust Center image names"
   time="2024-12-03T22:40:41Z" level=info msg="Successfully collected Trust Center image names" totalImages=46
   time="2024-12-03T22:40:42Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/library/redis:7.0.12-alpine"
   time="2024-12-03T22:40:42Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/oliver006/redis_exporter:v1.58.0-alpine"
   time="2024-12-03T22:40:43Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/library/busybox:1.36.1"
   time="2024-12-03T22:40:44Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/bitnami/zookeeper:3.9.2"
   time="2024-12-03T22:40:45Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/command:24.10.0"
   time="2024-12-03T22:40:46Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-registry:24.10.0"
   time="2024-12-03T22:40:46Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/docs-external-v1:24.10.0"
   time="2024-12-03T22:40:47Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-updater:24.10.0"
   time="2024-12-03T22:40:48Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/ingress-nginx/controller:v1.10.0"
   time="2024-12-03T22:40:48Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/ms_activity_log:0.0.768_84f4c1f"
   time="2024-12-03T22:40:49Z" level=info msg="Pulled docker image" image="docker.cloudsmith.io/teradici/trust-center/trust-center/job-ecr-renewal:dev"
   ```

2. Transfer the following files to the bare VM using the SCP command:

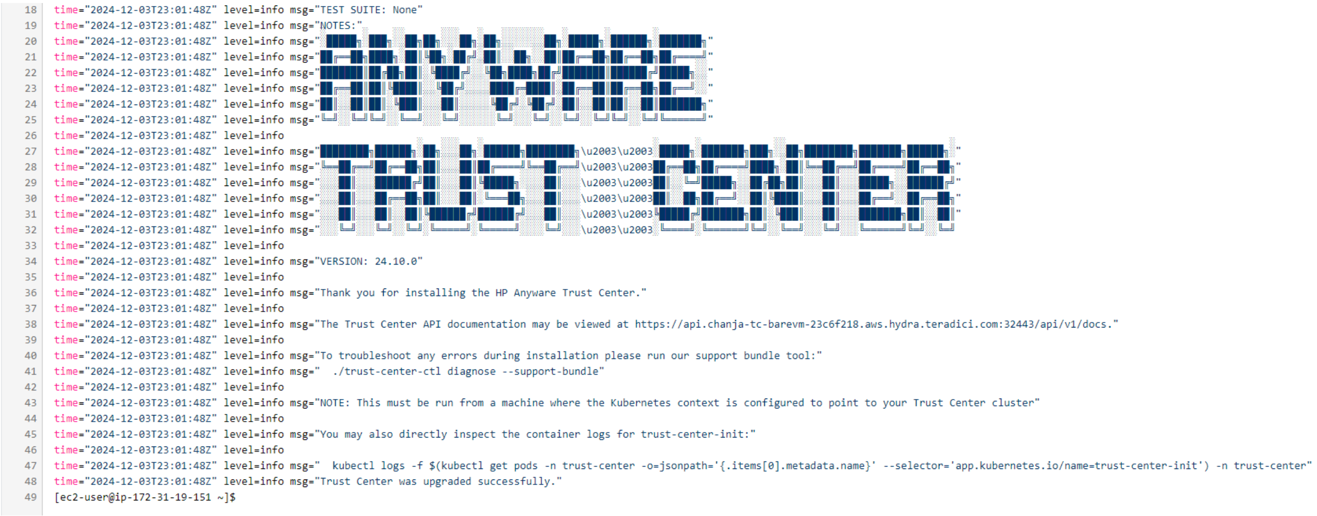
   - `anyware-trust-center-bundle.tar`
   - `anyware-trust-center-bundle.sha`
   - `trust-center-ctl`

Step III: Upgrade Trust Center

To upgrade an existing darksite Trust Center, run the following command:

```
sudo ./trust-center-ctl upgrade darksite
```

Example output of running a Darksite Upgrade command:



```
time="2024-12-03T23:01:48Z" level=info msg="TEST SUITE: None"
time="2024-12-03T23:01:48Z" level=info msg="NOTES:"
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info msg="
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info msg="\u2003\u2003
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="VERSION: 24.10.0"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="Thank you for installing the HP Anyware Trust Center."
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="The Trust Center API documentation may be viewed at https://api.chanja-tc-barevm-23c6f218.aws.hydra.teradici.com:32443/api/v1/docs."
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="To troubleshoot any errors during installation please run our support bundle tool:"
time="2024-12-03T23:01:48Z" level=info msg="  ./trust-center-ctl diagnose --support-bundle"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="NOTE: This must be run from a machine where the Kubernetes context is configured to point to your Trust Center cluster"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="You may also directly inspect the container logs for trust-center-init:"
time="2024-12-03T23:01:48Z" level=info
time="2024-12-03T23:01:48Z" level=info msg="  kubectl logs -f $(kubectl get pods -n trust-center -o=jsonpath='{.items[0].metadata.name}' --selector='app.kubernetes.io/name=trust-center-init') -n trust-center"
time="2024-12-03T23:01:48Z" level=info msg="Trust Center was upgraded successfully."
[ec2-user@ip-172-31-19-151 ~]$
```

Step IV: Upload OTA packages to a Darksite Trust Center

Since a darksite Trust Center cannot access external internet, OTA updates cannot be retrieved automatically.

Consequently, the following steps must be performed before uploading the OTA packages to the Darksite Trust Center:

- The token required to download the firmware must be obtained first obtained from the website.
- Firmware packages must be downloaded from an internet-connected Trust Center.

Info

The `trust-center-ctl` command is used for the following purposes:

- To download the firmware packages on the internet-connected Trust Center.
- To upload the firmware on the darksite Trust Center.

- On the Downloads site, go to **Downloads and scripts** > **Darksite OTA update tokens**, and click **Generate upgrade token** to obtain the time-limited token for the firmware of your interest.
- Copy the token to a text file.
- To list the firmware available to download into your Trust Center, run this command on the internet-connected Trust Center:

```
sudo ./trust-center-ctl firmware list --token {token}
```

- On the internet-connected Trust Center, run the following command to download firmware:

```
sudo ./trust-center-ctl firmware download --token <token> <version>
```

- Copy the **tc_firmware.tar.gz** file to the darksite Trust Center.
- On the darksite Trust Center, run the following command to upload firmware (use `--help` to see available flags):

```
sudo ./trust-center-ctl firmware upload --file tc_firmware.tar.gz --ca-file
tc-api-ca.crt
```

Info

This command uploads the firmware, and also saves the CA certificate to the `tc-api-ca.crt` file. If you do not see the certificate at this file, run the following command to obtain it:

```
sudo ./trust-center-ctl get-api-ca
```

Logs

The following table lists the logs and the locations where they are available.

Location	Description
/var/log/teradici/trust-center-ctl/install_.log	Trust Center log for internet-connected or darksite installation.
/var/log/teradici/trust-center-ctl/upgrade_.log	Trust Center log for internet-connected or Darksite upgrade.
/var/log/teradici/trust-center-ctl/prepare_.log	prepare log for installation or upgrade of darksite Trust Center.

Uninstall the Anyware Trust Center

You can uninstall the Anyware Trust Center completely from your system.

Danger: Data will be removed

Running this uninstall script will also remove all locally-stored data. Be sure to back up your system data if you are not using an external data store.

To uninstall the Anyware Trust Center and remove its data:

1. Open a console window and navigate to the installer directory.
2. In the console window, run the uninstall command:

```
sudo ./trust-center-ctl uninstall
```

Configuring

Enabling Automatic Login on Trusted Zero Clients

You can configure Trusted Zero Clients to automatically login to remote desktops from the Trust Center. This enables the clients to operate in environments where they're being used similar to a kiosk.

With Automatic Login, users can bypass the traditional login steps and directly access desktops, streamlining their login experience.

To enable the Kiosk mode on Trusted Zero Clients, the following properties must be configured:

- `autoConnectIfOneBroker`: This parameter is set on the Trust Center, and enables login without credentials provided that only one broker is configured to connect to the host.
- `autoLaunchIfOneDesktop`: This parameter is set on the broker (Endpoint Management tool), and allows automatic selection of a desktop, provided that only one desktop is available.
- `savedLoginUsername` and `savedLoginPasswordSecret`: This parameter is set on the broker (Endpoint Management tool), and fetches the username and password to be used for login.

Notes

Automatic login works only if the following conditions are met:

- Only one broker is configured to connect to the host.
- The user credentials are current. If the username or the password have expired, the user is directed to the password change window.
- Only one desktop is configured for use. If multiple desktops are available, the **Desktop Selection** window opens, with a list of desktops from which users can select the desktop to connect to.

To enable Automatic Login, configure the Trust Center and the Broker as described below.

Step I: Set a Secret on Trust Center

To begin, set a secret on Trust Center for the Trusted Zero Client. The Trust Center encrypts the secret value with the Trusted Zero Client's public key, which is available in the client's birth certificate.

The secret represents the password required for automatic login, and is retrieved while authenticating login attempts from a Trusted Zero Client. It is also required while configuring the broker.

> **Tip**
>
> The exact property names depend on the management tool you are using.

1. Open the Endpoint Management tool.
2. Set a secret using the `set-secret` command for the Trusted Zero Client.
3. Set the password secret to the `secretName` configured in the step above.
4. Do this for all the Trusted Zero Clients on which you want to enable automatic login.

Step II: Configure the Broker

Configure a broker for establishing PCoIP sessions. During configuration, provide the secret and the username that will be used for authentication. The secret and username will be verified for each connection attempt.

> **Info**
>
> The secret must be the same value as the Secret you set in **Step I**.

Configuration also involves enabling the automatic launch of desktops.To do this, set the `autoLaunchIfOneDesktop` to "True".

The following table lists the parameters that can be configured on the broker:

Value	Type	Description	Notes
`autoLaunchIfOneDesktop`	Boolean	This parameter allows automatic selection of a	

Value	Type	Description	Notes
		desktop, **provided that only one desktop** is available.	Set this value to `True` to enable Auto Login.
`savedLoginPasswordSecret`	String	This parameter fetches the password encrypted in the endpoint.	This value must match the secret that was set in **Step I**. For example, if you set the secret as `mysecret`, set this parameter to `mysecret` as well. The Secret will be used retrieved every time a connection attempt is made to authenticate the user.
`savedLoginUsername`	String	This parameter represents the username to be used for login.	The username will be used retrieved every time a connection attempt is made to authenticate the user.
`enableLoginUsernameCaching`	Boolean	This parameter allows users to control the ability to save their usernames, and display them on the client login window. This parameter is optional to the procedure.	

To configure the broker:

1. Open the Endpoint Management tool.
2. Set **Auto Connect if Only One Connection** to "True".
3. Set **Auto Select Desktop if Only One Desktop** to "True".
4. Set a username. The exact configuration for this depends on the management tool.

Step III: Enable Automatic Login on Trust Center

Finally, enable automatic login by setting the `autoConnectIfOneBroker` flag to "True". This flag allows automatic login, **provided that only one broker** is configured to connect to the host.

1. Open the Endpoint Management tool.
2. Set **Auto Connect if One Broker** to "True".

Enabling the Kiosk Mode on Trusted Zero Clients

You can configure Trusted Zero Clients from the Trust Center to operate in the Kiosk mode. This enables the clients to operate as fixed purpose devices such as point-of-sale terminals and digital signs.

To enable the Kiosk mode on Trusted Zero Clients, the following properties must be configured:

- `autoConnectIfOneBroker`: This parameter is set on the Trust Center, and enables login without credentials provided that only one broker is configured to connect to the host.
- `autoLaunchIfOneDesktop`: This parameter is set on the broker (Endpoint Management tool), and allows automatic selection of a desktop, provided that only one desktop is available.
- `savedLoginUsername` and `savedLoginPasswordSecret`: This parameter is set on the broker (Endpoint Management tool), and fetches the username and password to be used for login.
- `kioskMode`: This parameter is set on the Trust Center, and enables Kiosk mode on the Trusted Zero Clients.

Notes

Kiosk Mode works only if the following conditions are met:

- Only one broker is configured to connect to the host.
- The user credentials are current. If the username or the password have expired, the user is directed to the password change window.
- Only one desktop is configured for use. If multiple desktops are available, the **Desktop Selection** window opens, with a list of desktops from which users can select the desktop to connect to.

Step I: Set a Secret for each Trusted Zero Client

Tip

The exact property names depend on the management tool you are using.

To begin, set a secret on Trust Center for the Trusted Zero Client. The Trust Center encrypts the secret value with the Trusted Zero Client's public key, which is available in the client's birth certificate.

The secret represents the password required for automatic login, and is retrieved while authenticating login attempts from a Trusted Zero Client. It is also required while configuring the broker.

1. Open the Endpoint Management tool.
2. Set a secret using the `set-secret` command for the Trusted Zero Client.
3. Set the password secret to the `secretName` configured in the step above.
4. Do this for all the Trusted Zero Clients on which you want to enable Kiosk mode.

Step II: Configure the Broker

As a next step, configure a broker for establishing PCoIP sessions and enabling the automatic launch of desktops. While configuring, enter the secret and username that will be used for authentication. These credentials will be verified for each connection attempt.

> **Info**
>
> The secret must be the same value as the Secret you set in **Step I**.

The following table lists the parameters that can be configured on the broker:

Value	Type	Description	Notes
`savedLoginPasswordSecret`	String	This parameter fetches the password encrypted in the endpoint.	This value must match the secret that was set in **Step I**. For example, if you set the secret as `mysecret`, set this parameter to `mysecret` as well. The Secret will be used retrieved every time a connection attempt is made to authenticate the user.
	Boolean		

Value	Type	Description	Notes
`autoLaunchIfOneDesktop`		This parameter allows automatic selection of a desktop, **provided that only one desktop** is available.	Set this value to `True` to enable Auto Login.
`savedLoginUsername`	String	This parameter represents the username to be used for login.	The username will be used retrieved every time a connection attempt is made to authenticate the user.
`enableLoginUsernameCaching`	Boolean	This parameter allows users to control the ability to save their usernames, and display them on the client login window. This parameter is optional to the procedure.	

To configure the broker:

1. Open the Endpoint Management tool.
2. Set **Auto Connect if Only One Connection** to "True".
3. Set **Auto Select Desktop if Only One Desktop** to "True".
4. Set a username. The exact configuration for this depends on the management tool.

Step III: Enable Automatic Login on Trust Center

Next, enable automatic login by setting the `autoConnectIfOneBroker` flag to "True". The ability to automatically login is necessary for the Trusted Zero Clients to operate in Kiosk mode.

1. Open the Endpoint Management tool.
2. Set **Auto Connect if One Broker** to "True". This flag allows automatic login, **provided that only one broker** is configured to connect to the host.

Step IV: Enable the Kiosk Mode on Trusted Zero Clients

Finally, enable the Kiosk mode on Trusted Zero Clients, using the `kioskMode` parameter. This parameter can have two values:

- True: When enabled, Trusted Zero Clients can automatically log in to remote desktops, such as in kiosk-like environments.
- False: When disabled, Trusted Zero Clients follow the standard login process to connect to remote desktops.
- Open the Endpoint Management tool.
- Set **kioskMode** to "True". This flag enables the Kiosk mode, **provided that only one broker** is configured to connect to the host.

Configuring the Login Experience on the Trusted Zero Clients

You can configure the login experience on Trusted Zero Clients from the Trust Center.

Depending on the configuration, Trusted Zero Clients can skip one or more of the following login steps:

- Connecting to a broker
- Providing user credentials
- Selecting a desktop

The ability to bypass one or more traditional login steps simplifies and streamlines the login experience.

> **Info**
>
> Once the parameters have been set on the Trust Center, they cannot be changed on the Trusted Zero Clients.

To configure the login experience:

1. Open the Endpoint Management tool.
2. Enable or disable **Auto Connect if One Broker**. This parameter is set on the Trust Center, and enables login without credentials provided that only one broker is configured to connect to the host.
3. Enable or disable **Auto Select Desktop if Only One Desktop**. This parameter allows automatic selection of a desktop, provided that only one desktop is available.
4. Enable or disable `enableLoginUsernameCaching`. This parameter allows users to control the ability to save their usernames, and display them on the client login window.
5. Enable or disable the **Remember Username** feature as the default setting. You can disable the feature in the EMS to ensure that the username is never remembered.

Enabling Imprivata Authentication

You can enable authentication of Trusted Zero Clients connecting to Horizon hosts using Imprivata OneSign Single Sign-On in the Trust Center. Imprivata OneSign enables users to access corporate networks, desktops, and applications with Imprivata single sign on.

> **Info**
>
> While Imprivata OneSign Single Sign-On supports a range of authentication options, at present, only proximity cards are supported.

This topic describes the process of enabling authentication using the Imprivata OneSign server.

Step I: Configure the Imprivata OneSign Single Sign-On

Imprivata OneSign Single Sign-On allows users to access authorized applications using a single set of credentials. In the Trusted endpoints setup, Imprivata OneSign Single Sign-On acts as the single-sign on provider, and handles authentication for Trusted Zero clients connecting to Omnissa Horizon hosts.

Imprivata OneSign Single Sign-On must be set up **before** configuring the Trust Center. This setup is separately performed and is outside the scope of Trust Center. Additional instructions can be found on the Imprivata Customer Experience Center.

Step II: Enable Imprivata Authentication

Next, configure the Trust Center to direct connection attempts from Trusted Zero Clients to Imprivata OneSign Single Sign-On for authentication.

1. Open the Endpoint Management tool.
2. Set **connectionType** to `oneSignServer`.
3. In the **address** field, enter the IP address or FQDN of the OneSign server. The IP address must be in the IPv4 format.

4. Save your changes.

Troubleshooting

Installation failures

Installation can fail on some distributions or environments unless additional configuration is done. Check the additional configuration requirements listed above.

If any steps were missed:

1. Uninstall the Anyware Trust Center.
2. Perform the relevant configuration steps.
3. Install the Anyware Trust Center again. You will likely need to return to the download site and generate a new download command.

Troubleshooting Hostname Changes

If the hostname of the machine on which the Anyware Trust Center is installed changes after installation, the Trust Center will not start properly.

You can follow the below procedure to troubleshoot this issue.

1. Uninstall the Anyware Trust Center.
   ```
   sudo ./trust-center-ctl uninstall
   ```
2. Set the hostname.
   ```
   hostnamectl set-hostname <\your-host-name>
   ```
3. Install the Anyware Trust Center again.
   For Single Node Installation, refer to the Run the Installation Script section. For Dark Site Installation, see the Installation Command.
4. Verify that it works with DMS again, or run the diagnostic command to ensure all services are healthy.
5. Re-start the machine.
6. Verify that it still works with DMS, or run the diagnostic command again.

Support

Support

If you encounter a problem setting up or using the Anyware Trust Center, there are a number of troubleshooting and support resources you can access.

- We maintain an extensive **knowledge base** which answers many questions and documents solutions to common problems. The knowledge base is part of the Knowledge Center; click on the *Articles* tab to access it, or enter a search query in the search field at the top of the page.
- We host a **community forum**, allowing you to ask questions and get answers from other IT professionals and our support team, which monitors this channel. The forum is part of the Knowledge Center; click on the *Discussions* tab to access it.
- If you need more help, open a support ticket and our support team will engage with you directly.

Creating a Support Bundle

Support bundles are archives that capture the current state of the Anyware Trust Center, and are used by our support team to troubleshoot issues you may experience.

The HP Anyware Support team may request the support bundle from your system in order to diagnose issues.

> **Note: Support bundle includes a README file**
>
> The generated support bundle includes a README file at the root of the archive, containing information about viewing the files and folders in it.

To create a support bundle:

1. Open a console window and navigate to the working directory.
2. In the console window, run the following command:

   ```
   sudo ./trust-center-ctl diagnose --support-bundle --cluster-type k3s
   ```

Reference

Trust Center 25.03.0 Image Inventory

This document describes each container image in use in the Trust Center version 25.03.0 deployment.

You can download this content as a PDF by clicking here.

Contents

Component List

Container Image	Component
trust-center/trust-center-ctl	Trust Center Init Job
library/busybox	Busybox
ms_activity_log	Activity Log Service
ms_authorization	Authorization Service
trust-center/asset-mgmt	Asset Management Service
trust-center/command	Command Service
trust-center/endpoint-connector	Endpoint Connector Service
trust-center/endpoint-registry	Endpoint Registry Service
trust-center/endpoint-updater	Endpoint Updater Service

Container Image	Component
trust-center/health	Health Service
trust-center/ostree-sync	OSTree Sync Service
trust-center/pki-adapter	PKI Adapter Service
job_rotate_signing_key	Rotate Signing Key Job
ms_secret_mgmt	Secret Management Service
trust-center/trust-enforcement	Trust Enforcement Service
trust-center/vault-unseal	Vault Unseal Job
trust-center/docs-external-v1	External API Docs
hashicorp/vault	Vault
library/redis	Redis
oliver006/redis_exporter	Redis Prometheus Exporter
confluentinc/cp-kafka	Kafka
danielqsj/kafka-exporter	Kafka Prometheus Exporter
library/mariadb	MariaDB
library/mongo	MongoDB
bitnami/mongodb-exporter	MongoDB Prometheus Exporter
ingress-nginx/controller	NGINX Ingress Controller
fluent/fluent-bit	Fluent Bit
fluent/fluentd	Fluentd
jetstack/cert-manager-cainjector	cert-manager CA Injector
jetstack/cert-manager-controller	cert-manager Controller
jetstack/cert-manager-webhook	cert-manager Webhooks
## Verifying Container Images	

Container Image	Component
First, copy the container registry password from `global.images.password` in your Trust Center's `config.yaml`.	

Then, log into the container registry:

```
$ docker login docker.cloudsmith.io
Username: teradici/trust-center
Password: <Password>
```

(note: If using a beta release, use `teradici/trust-center-beta` instead)

Next, check the details for a specific container image in the remote registry:

```
$ docker buildx imagetools inspect <Image tag>
Name:      <Image tag>
MediaType: application/vnd.docker.distribution.manifest.v2+json
Digest:
sha256:002f688e9756d464d2064b526d4446306210198e8c8b234b36c9a8d5399b80d7
```

`<Image tag>` should be the full URI to the image, e.g.: `docker.cloudsmith.io/teradici/trust-center/fluent/fluentd:v1.16-2`

Now, pull the image to download it locally:

```
$ docker pull <Image tag>
[...]
$ docker inspect --format='{{index .RepoDigests 0}}' <Image tag>
<Image
tag>@sha256:002f688e9756d464d2064b526d4446306210198e8c8b234b36c9a8d5399b80d7
```

The image sha256 hash should match between the remote container registry and the local copy. Additionally, the hash calculated here should match the image hash listed for each container image in these READMEs.

Component Details

Trust Center Init Job

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/trust-center-ctl
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:b2efc1157a4ea0feb8c18537b922bf21f946e0cb53ad1971a70d6a462d69d0aa

Description

Container which runs on initial installation and upgrade of the Trust Center. Initializes and upgrades Trust Center service configuration.

Back to overview

Busybox

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/library/busybox
Product	Trust Center
Supplier	Open Source
Version	1.36.1
Image Hash	sha256:023917ec6a886d0e8e15f28fb543515a5fcd8d938edb091e8147db4efed388ee

Description

Used for various init containers preventing services from starting up before dependencies are ready.

We use the official Docker image for Busybox: https://hub.docker.com/_/busybox

Back to overview

Activity Log Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/ms_activity_log
Product	Trust Center
Supplier	HP Inc.
Version	0.0.768_84f4c1f
Image Hash	sha256:67dea90c8be993dfc79ec697d89647d13474fcf3a0abed979638782ad598f7c9

Description

The Activity Log service handles events generated by Trust Center services, and exposes an API to query activity logs.

Back to overview

Authorization Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/ms_authorization
Product	Trust Center
Supplier	HP Inc.

Field	Value
Version	0.0.5559_fde52ff
Image Hash	sha256:1f667811704697c58b9f98785b6f039a0dfbcd2bae35733abdc91a3f6611e093

Description

The Authorization service handles authentication and authorization for Trust Center API service accounts.

Back to overview

Asset Management Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/asset-mgmt
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:0b1d80810c435b5e3ab4bf2e602bedc9b491fdee446f37632a6db82f9d539019

Description

The Asset Management service enables storing and retrieving assets (such as support bundles, branding assets) within the Trust Center.

Back to overview

Command Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/command
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:45743bbbd2e471515be901112cbbc9736bdee937b6bb57ade21cccb7f09fb5b9

Description

The Command service enables sending commands to endpoints connected to the Trust Center and processing command status updates.

Back to overview

Endpoint Connector Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-connector
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:d81a2da2016fff638685e2e24d737c6ef010b76c2603164c831a3bda36a0ebc3

Description

The Endpoint Connector service provides APIs which Trusted Zero Clients and other endpoints use to communicate with the Trust Center.

Back to overview

Endpoint Registry Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-registry
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:d416949a06e0ff8984ba1cebedb3e9dc65758a78d1f69716af1378c486d09b4a

Description

The Endpoint Registry service maintains endpoint digital twins and provides APIs for management of endpoint configuration.

Back to overview

Endpoint Updater Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/endpoint-updater
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:03632a2b29b9c6aaa030f0c59dca3b10ac94d5021b7f2bb73cb6daadfb2586db

Description

The Endpoint Updater service is responsible for triggering OTA updates for connected endpoints when requested in endpoint configuration.

Back to overview

Health Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/health
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:42dc2ba1d4d6aa7e9c5b0a1e11f48549359186d663e1a07c42b2158d95560dfa

Description

The Health service provides API endpoints for Trust Center deployment health-checks.

Back to overview

OSTree Sync Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/ostree-sync
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0

Field	Value
Image Hash	sha256:3d1f135e6bfdc26784ac36d10952f0f484b8565b1e271b6557b82f592295efe5

Description

The OSTree Sync service is responsible for storing Trusted Zero Client OTA update images and serving them to endpoints when requested.

Back to overview

PKI Adapter Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/pki-adapter
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:6590ca883905e7fd593223c5ac5d5908e9956ec4216a43b5d5b2ce9970bd59bc

Description

The PKI Adapter Service is responsible for for providing an interface for Trust Center services to request certificates and tokens generated by internal and external issuers.

Back to overview

Rotate Signing Key Job

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/job_rotate_signing_key
Product	Trust Center
Supplier	HP Inc.
Version	0.0.306_1fd114b
Image Hash	sha256:2dd340a6ae9d7f6b9cb880aa3f3196cbbaf2c037b54480df0879dc234200e982

Description

The Rotate Signing Key job is used as a perodic CronJob in the Trust Center to rotate internal token signing keys.

Back to overview

Secret Management Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/ms_secret_mgmt
Product	Trust Center
Supplier	HP Inc.
Version	0.0.690_b709211
Image Hash	sha256:ed8044a52a74886470b84ea3ddfba3762eef537fed16d6ef3e8568f99ae4370f

Description

The Secret Management service provides an interface for Trust Center services to access key/value secrets from internal (Vault) and external secret storage providers.

Back to overview

Trust Enforcement Service

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/trust-enforcement
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:21ba3bc68aebd76e4a0ef85fd6cafde54c14ff325663ad639933f38d2223af46

Description

The Trust Enforcement Service is responsible for facilitating policy evaluation and enforcement on endpoints connected to the Trust Center.

Back to overview

Vault Unseal Job

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/vault-unseal
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:8797c865fa259dab02f5b79d30fc43b7e806510c3f64113d3a11e78b41be12ca

Description

The Vault Unseal job is a CronJob used by the Trust Center to ensure the internal Vault instance (for on-prem deployments) is unsealed.

Back to overview

External API Docs

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/trust-center/docs-external-v1
Product	Trust Center
Supplier	HP Inc.
Version	25.03.0
Image Hash	sha256:0b43981ec016021277aeaf82fbfc1d21002c70d83833464d6e86621dd6160d7c

Description

This container serves a copy of the External API documentation corresponding to this version of the Trust Center.

Back to overview

Vault

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/hashicorp/vault
Product	Hashicorp Vault
Supplier	Hashicorp

Field	Value
Version	1.18.2
Image Hash	sha256:0d40cc366fd251520002c170f3f3c9a89e935d303313ed2f36cbc58fd3a530ef

Description

Hashicorp Vault is a third party component deployed with the Trust Center in on-premises deplyoments to securely store deployment secrets.

We use the official Docker image for Hashicorp Vault: https://hub.docker.com/r/hashicorp/vault

Back to overview

Redis

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/library/redis
Product	Redis
Supplier	Redis Ltd.
Version	7.4.1-alpine
Image Hash	sha256:7438ca8459132b9fe507a95fe6838fecd7c55f8611ed835742a014d7a92618e4

Description

Redis is a third-party component deployed with the Trust Center to function as an in-memory cache.

We use the official Docker image for Redis: https://hub.docker.com/_/redis

Back to overview

Redis Prometheus Exporter

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/oliver006/redis_exporter
Product	Redis
Supplier	Open Source - Oliver006
Version	v1.66.0-alpine
Image Hash	sha256:617b1e5b51498d0e98d0b2e55abfe45a017dd0d08c37ca88e3c973c0d77fa47b

Description

Small third-party component used to export Prometheus metrics from Redis.

Uses mirrored Docker Hub image: https://hub.docker.com/r/oliver006/redis_exporter

Back to overview

Kafka

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/confluentinc/cp-kafka
Product	Kafka
Supplier	Confluent Inc.
Version	7.7.1
Image Hash	sha256:a21737d09496a8b9bb38b995ab021e94e952259a5a2756ee22cef1cc84f5d9fe

Description

Kafka is deployed as part of the Trust Center to handle message queueing.

We use the Kafka Docker image (Community Version) maintained by Confluent Inc.: https://hub.docker.com/r/confluentinc/cp-kafka/

Back to overview

Kafka Prometheus Exporter

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/danielqsj/kafka-exporter
Product	Kafka
Supplier	Open Source - Daniel Qian
Version	v1.8.0
Image Hash	sha256:16bbe1d1647128a7060da21c36ae27b6f052bf5b8dedba0a5cb3460dee2f7b51

Description

Small third-party component used to export Prometheus metrics from Kafka.

Uses mirrored Docker Hub image: https://hub.docker.com/r/danielqsj/kafka-exporter

Back to overview

MariaDB

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/library/mariadb
Product	MariaDB
Supplier	MariaDB Foundation
Version	10.4.29

Field	Value
Image Hash	sha256:f9f3c4b8fd9dc7717a903c79d847af9c783771b9e0ff3cc4fc983a40e9e5972d

Description

MariaDB is included in this release to facilitate data migration on upgrade from older Trust Center versions which required it. It will be removed in a subsequent release.

We use the official Docker image for MariaDB: https://hub.docker.com/_/mariadb

Back to overview

MongoDB

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/library/mongo
Product	MongoDB
Supplier	MongoDB Inc.
Version	5.0.30
Image Hash	sha256:b3857ebaf1cf7d0c75090776ef76fb01cc142fe1ca0939be51da61fd5936a911

Description

MongoDB is included in on-premises deployments of the Trust Center to handle data persistence.

We use the official Docker image for MongoDB: https://hub.docker.com/_/mongo

Back to overview

MongoDB Prometheus Exporter

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/bitnami/mongodb-exporter
Product	MongoDB
Supplier	Bitnami
Version	0.42.1
Image Hash	sha256:3aeaedd3faf7f9e16e919fdefc954153c5a0179eb733cce509d961fb2ed9885a

Description

Small third-party component used to export Prometheus metrics from MongoDB.

Uses mirrored Docker Hub image: https://hub.docker.com/r/bitnami/mongodb-exporter/

Back to overview

NGINX Ingress Controller

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/ingress-nginx/controller
Product	NGINX
Supplier	NGINX Inc.
Version	v1.11.3
Image Hash	sha256:38b51d8833e79d97d4adf825e0bf893e322d19be54ff65a88d9320139a68adfb

Description

The Trust Center uses the NGINX Ingress controller to handle ingress to Trust Center APIs (including TLS, WAF, etc.)

We use the official Docker image for nginx-ingress: https://hub.docker.com/r/nginx/nginx-ingress

Back to overview

Fluent Bit

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/fluent/fluent-bit
Product	Fluentd
Supplier	Fluent
Version	3.2.1
Image Hash	sha256:905e3e329840de5b843c9277911ab3d82205a57851ad22b79d671b47012860c5

Description

Fluent Bit is a third party log processor deployed with the Trust Center to facilitate log aggregation.

We use the official Docker image for Fluent Bit: https://hub.docker.com/r/fluent/fluent-bit

Back to overview

Fluentd

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/fluent/fluentd

Field	Value
Product	Fluentd
Supplier	Fluent
Version	v1.17-1
Image Hash	sha256:c795c1bf9918c77a5415e2fda5825f9341f2dd0645d9adfb91f8cae3a3e6b240

Description

Fluentd is a third party log data collector deployed with the Trust Center to facilitate log aggregation.

We use the official Docker image for Fluentd: https://hub.docker.com/r/fluent/fluentd

Back to overview

cert-manager CA Injector

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/jetstack/cert-manager-cainjector
Product	cert-manager
Supplier	cert-manager Project
Version	v1.16.2
Image Hash	sha256:0a1f62ea3390a73239c0b4214e0ada1fb89c52d30677aebcdc3ca54508996511

Description

We include cert-manager in the Trust Center deployment to automatically manage API ingress certificates.

We use the Docker image for the cert-manager CA injector managed by Jetstack: https://quay.io/repository/jetstack/cert-manager-cainjector

Back to overview

cert-manager Controller

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/jetstack/cert-manager-controller
Product	cert-manager
Supplier	cert-manager Project
Version	v1.16.2
Image Hash	sha256:de97c3767802e33d3096ad9b276598ceee3ed92a0c67907221581b36c8ad055f

Description

We include cert-manager in the Trust Center deployment to automatically manage API ingress certificates.

We use the Docker image for the cert-manager controller managed by Jetstack: https://quay.io/repository/jetstack/cert-manager-controller

Back to overview

cert-manager Webhooks

Metadata

Field	Value
Container Image	docker.cloudsmith.io/teradici/trust-center/jetstack/cert-manager-webhook
Product	cert-manager
Supplier	cert-manager Project
Version	v1.16.2
Image Hash	sha256:25d87dff68f00587a3e76a1e5d530d40b6f0f7872e6d634db01a593047849109

Description

We include cert-manager in the Trust Center deployment to automatically manage API ingress certificates.

We use the Docker image for the cert-manager webhooks managed by Jetstack: https://quay.io/repository/jetstack/cert-manager-webhook

Back to overview