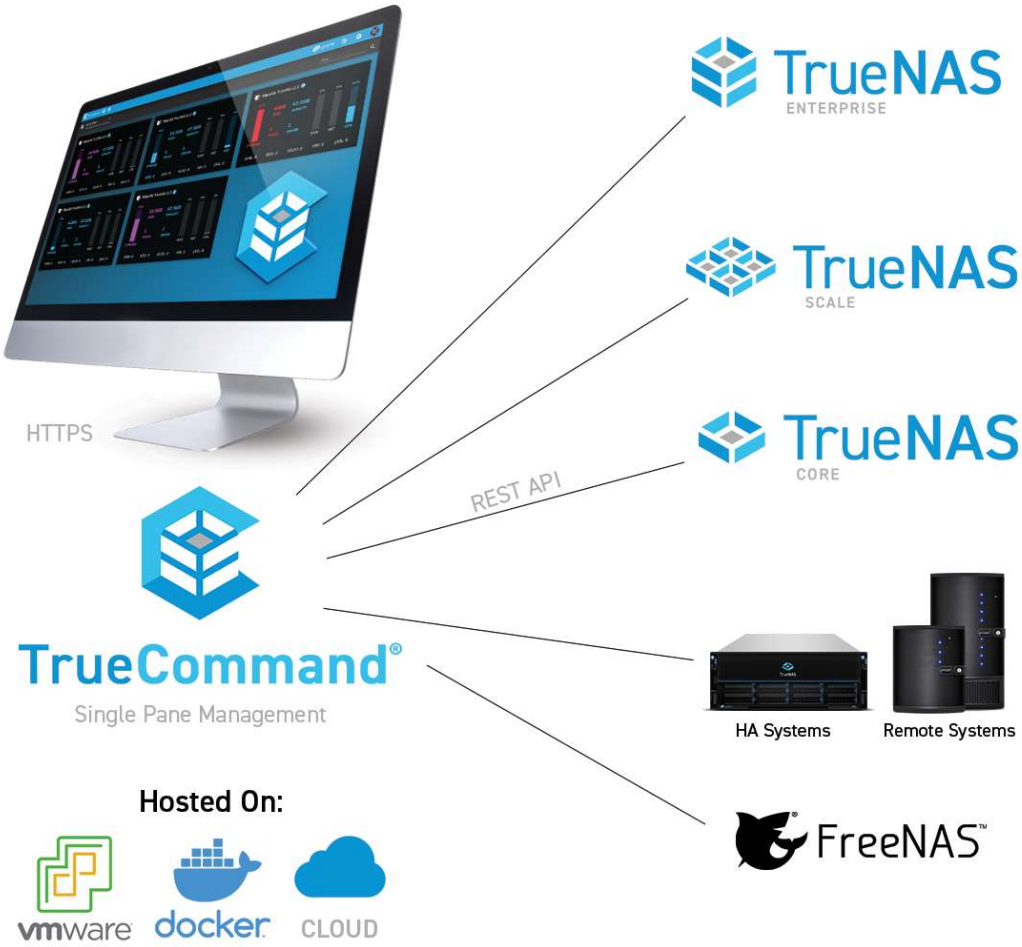
Print
Back to Docs Hub

TrueCommand

TrueCommand is a multi-system management "Single pane of Glass" system that helps control and monitor your TrueNAS fleet. TrueCommand assists in managing TrueNAS systems through REST APIs, WebSocket APIs, and a web user interface. The TrueCommand web interface provides single sign-on functionality and unified administration of users and TrueNAS systems.

TrueCommand can monitor an entire fleet of TrueNAS systems and thousands of online storage devices simultaneously. This includes displaying statistics on storage usage, network activity, active services, and more. TrueCommand also has the ability to create custom reports about individual systems or a combination of many systems.



What Features does TrueCommand have?

Multiple Deployment Options
TrueCommand docker container can be deployed as a VM since vhdk and vmdk are no longer supported in version 2.0. TrueCommand Cloud is also available as a cloud-based subscription option that allows you to offload TrueCommand resources and deployment and only focus on fine-tuning your configuration.

NAS Fleet Dashboard
The TrueCommand dashboard provides visibility to an organization's entire TrueNAS fleet. TrueCommand includes an auto-discovery tool that expedites identifying and integrating systems into TrueCommand.

Single Sign-on to all NAS Units
Authorized administrators can quickly log into a TrueNAS system through TrueCommand This allows for quicker and simpler signons instead of looking up IP addresses and login credentials. This is even more beneficial when using different secure passwords for each TrueNAS instance instead of a single password across multiple systems.

Centralized system updates
Easily update any connected TrueNAS system. Monitor update progress, reboot the system, or even roll it back if something goes wrong.

Customized Alerts and Reports

TrueCommand centralizes the management of alerts across a fleet of TrueNAS systems. In addition to the standard system alerts, administrators can define custom alerts.

Administrators can also create custom graphical reports. Reports are configurable and can span as many systems as desired and/or set of metrics. This brings the information that the administrators deem the most relevant immediately to visibility. Report data can be exported in CSV or JSON for other uses.

Alerts for all managed systems are shown in TrueCommand's web-based dashboard. Notification groups can also be defined so that unique groups receive specific alerts via email. This enables TrueCommand to keep the right individuals informed of any current or potential problems.

Enterprise Security with Role-Based Access Control (RBAC)
TrueCommand administrators can define varied levels of system access. These access levels can be assigned to system groups. Individuals can be assigned to teams or departments. Doing so allows the administrator to control the level of access appropriate to each individual or group in a manageable and atomic fashion. TrueCommand's RBAC controls can leverage pre-existing LDAP and Active Directory identities and groups in your infrastructure, eliminating redundant management overhead.

Audit Logs
TrueCommand records all administration actions in secure audit logs. This allows for quick identification of what has been changed and who changed it.

What Does it Cost?

TrueCommand is free to use for up to 50 drives. Licenses to expand TrueCommand capabilities are purchased from the iXsystems account portal. Pricing is based on the number of drives and the desired level of support.

Where do I get it?

TrueCommand is downloaded from the TrueNAS website. TrueCommand Cloud subscriptions are available at the iXsystems Account Services Portal.

What is TrueCommand Cloud?

TrueCommand Cloud is a secure SaaS offering that includes a WireGuard VPN capability to connect TrueNAS systems through firewalls. TrueCommand Cloud is compatible with TrueNAS versions **12.0+ or SCALE** for the Wireguard VPN capability. Subscribe to and set up TrueCommand Cloud using these instructions.

1 - Introduction

Welcome to TrueCommand!

This section contains licensing information and additional details about software support offerings from iXsystems, Inc.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the **<** symbol to expand the menu to show the topics under this section.

1.1 - Support

Free Support

The TrueCommand Community Forum is an active online resource for asking questions, troubleshooting issues, and sharing information with other TrueCommand users. Registering is required for posting. New users are encouraged to briefly introduce themselves and review the forum rules before posting.

Paid Support

iXsystems offers different Support packages for TrueCommand customers. To find more details about the different Warranty and Service Level Agreement (SLA) options available, see the TrueCommand Support overview.

TrueCommand Cloud

If any issues are found when using TrueCommand Cloud or an iX Portal account, log in to the Portal Account and click *Manage* > *Request Support*. Fill out the *Request Support* form with specific details of the issue and click *Send Request*. A copy of the support request is emailed to the registered email account.

2 - Developer's Notes

Recent Updates

> 04/09/2021 - ISCSI creation process completed. Cluster creation routines finished up and streamlined.

> 03/17/2021 - Large update to Cluster creation/management. Requires latest TrueNAS SCALE nightlies to work properly (API's just changed on their end).

> 02/25/2021 - Initial nightly image release for TrueCommand 2.0

System Requirements

- Docker Environment (64-bit AMD or Intel system)
- 2GB of RAM (recommended minimum)
- 20GB of disk space (recommended minimum)

Nightly Docker Images

Nightly images for TrueCommand are built every 24 hours. These images are automatically pushed to the "nightly" tag on DockerHub if they pass the automated QA testing procedure.

Download information:

- DockerHub
- Example in Documentation, replace "latest" with "nightly" in the docker pull commands.

Current Status

The nightly images are always considered a "work-in-progress" toward the next release of TrueCommand. They should be suitable for adventurous users and developers who are not afraid of diagnosing issues and opening up bug reports with the TrueCommand developers.

Ticket Tracker: Jira

Current Nightly Version: 2.0-Master

Summary of changes in version 2.0

- Version 2.0 is a complete rewrite of the middleware and database used in TrueCommand, as well as a complete re-integration with the TrueNAS middleware for statistics and analysis. Early tests indicate a sharp improvement in the performance of the system (details below), and some of the new features that this enables in TrueCommand 2.0 are: NAS metrics and state updates in realtime - no more 30s delay!
- The "Storage Explorer" interface lets you inspect the datasets and files on your storage pools, while also giving you easy access to creating and managing snapshots, shares, zvols, and more.
- The "ISCSI Manager" is a new dashboard system that lets you view and create ISCSI volumes in bulk across your entire NAS fleet.
- "Cluster Volumes" is a new dashboard system that lets you view and create clustered datasets which span across multiple TrueNAS SCALE systems in your fleet.
- Marked performance improvements:
- Docker image ~50% smaller
- Network bandwidth usage ~40% less
- CPU usage ~5% lower
- Database growth rate ~99% lower

Table of features and current status (Timestamp references when the item status was last updated):

Feature	Status	Timestamp	Description

Feature	Status	Timestamp	Description
Users	**OK**	02/26/2021	Create and manage users and user permissions
Teams	**OK**	02/26/2021	Create and manage teams of users and permissions
Systems	**OK**	02/26/2021	Register NAS's and maintain connections/status info
Alert Rules	**OK**	02/26/2021	Create and manage custom alert rules
Alert Notices	**OK**	02/26/2021	Rolling feed of alerts that have been triggered with comment and resolution systems
Alert Services	**OK**	06/07/2021	Submission of new alert notices to external notification systems (email/pagerduty)
Reports	**OK**	02/26/2021	Historical charts of system information
Logs	**OK**	02/26/2021	Security logs of changes from users
System Administration	**OK**	02/26/2021	Configuration of TrueCommand system (SSL certificates, licensing, AD/LDAP, etc)
Dashboard	**OK**	06/07/2021	Top-level look at NAS state and information
NAS Explorer	**OK**	06/07/2021	Detailed inspection/management of storage on individual NAS's
Cluster Volumes	**OK**	06/07/2021	Create and manage clusters of TrueNAS SCALE systems (glusterfs)
ISCSI Manager	**OK**	06/07/2021	Create and manage ISCSI volumes in bulk

Migration Notice

Due to the change in database between the 1.x and 2.x versions of TrueCommand, there is an automatic database migration routine that will run the first time you start up the v2.0 image of TrueCommand.

Information Migrated:

- User accounts
- Teams
- System Registrations
- System Groups
- TrueCommand System Configuration
- NAS configuration backups

Information **NOT** migrated due to drastic changes in how these are performed now.

- Historical metrics from NAS's
- Alerts (both rules and notices)
- User-defined reports
- Security Logs

When you are using an LDAP-enabled system for user logins, please have your non-LDAP admin user credentials handy before updating. The LDAP integration systems between 1.x and 2.x are different, and you need to login and verify that everything is still configured properly after the migration.

Minimum Supported TrueNAS Versions

Due to the changes in integrating with the TrueNAS middleware, the minimum version for full-support of functionality has changed with TrueCommand 2.0:

- FreeNAS/TrueNAS 11.3 series - No longer supported. Does not provide realtime statistics or storage information, but you can still connect to them and use TrueCommand to initiate updates.
- TrueNAS 12 CORE/Enterprise - Supported after 12.0-U3. 12.0-U2.1 and older are missing some key metrics in the realtime stats (disk/network usage metrics in particular), but work otherwise.
- TrueNAS SCALE 21.03+ - Fully Supported (SCALE-20.12+ is supported excluding cluster functionality)

3 - Getting Started

Thank you for trying TrueCommand! This Guide walks you through the initial installation and set up of TrueCommand.

3.1 - Installing or Updating

TrueCommand is incredibly versatile and offers several different install options. TrueCommand Cloud is the preferred method for using TrueCommand, as this option requires no local resources or specific hardware requirements to get started!

Install Options

Click one of the tabs below to see instructions for your preferred deployment method.

VM Deployment

Deploying TrueCommand on a virtual machine (VM) requires different methods depending on what operating system you intend to use.

You can find VM images and setup instructions on our TrueCommand-install GitHub repository.

Linux

Debian

If you don't already have it, you can download the VM image here.

> Ensure you have the "wget" utility installed first: `apt-get install wget`

Run this command (as root) from a system terminal:
```
wget https://raw.githubusercontent.com/iXsystems/truecommand-install/main/debian/setup.sh -O - | bash
```

Alpine

If you don't already have it, you can download the VM image here.

> Ensure you have the "wget" utility installed first: `apk add wget`.
> Ensure that you have the "community" package repository enabled:
>
> - Edit the */etc/apk/repositories* file as root and uncomment the community repository line.
> - Run `apk update` to refresh the list of available packages.

Run this command (as root) from a system terminal:
```
wget https://raw.githubusercontent.com/iXsystems/truecommand-install/main/alpine/setup.sh -O - | sh
```

Void

If you don't already have it, you can download the VM image here.

> Ensure you have the "wget" utility installed first: `xbps-install -y wget`

Run this command (as root) from a system terminal:
```
wget https://raw.githubusercontent.com/iXsystems/truecommand-install/main/void/setup.sh -O - | bash
```

Windows

If you don't already have it, you can download the VM image here.

1. On your Windows platform (VM or Bare-Metal) install Docker for Windows.
2. Open Windows PowerShell (**Start > Windows Power Shell > Windows Power Shell**)

3. Run the following command inside powershell to start TrueCommand:

```
docker run --pull=always --restart unless-stopped --detach -v "[hostdirectory]:/data" -p [portnumber]:80 -p
[sslportnumber]:443 ixsystems/truecommand
```

> Replace *[hostdirectory]* with a path to where you want TrueCommand to store its local database. Replace *[portnumber]* and *[sslportnumber]* with the ports you wish to expose for TC access.

If the command was successful, you should be able to access TrueCommand on *http://localhost:80*.

Cloud Deployment

TrueCommand Cloud is a SaaS offering of TrueCommand with a WireGuard VPN capability to connect TrueNAS systems through firewalls. TrueCommand Cloud is compatible with TrueNAS version v12.0 and newer.

Register an iXsystems Account

Open https://portal.ixsystems.com and click **Register**.

Fill out the form using the email address you want to use.

This email account must be verified. Check the address spam folder if the email does not arrive within a few minutes. When the email is in the spam folder, mark it as *not spam* and add the account to the address book so future emails arrive at the inbox. After receiving the verification email, open the link provided to verify the account.

Create a New Subscription

Log in to the verified account and click **New Subscription**.

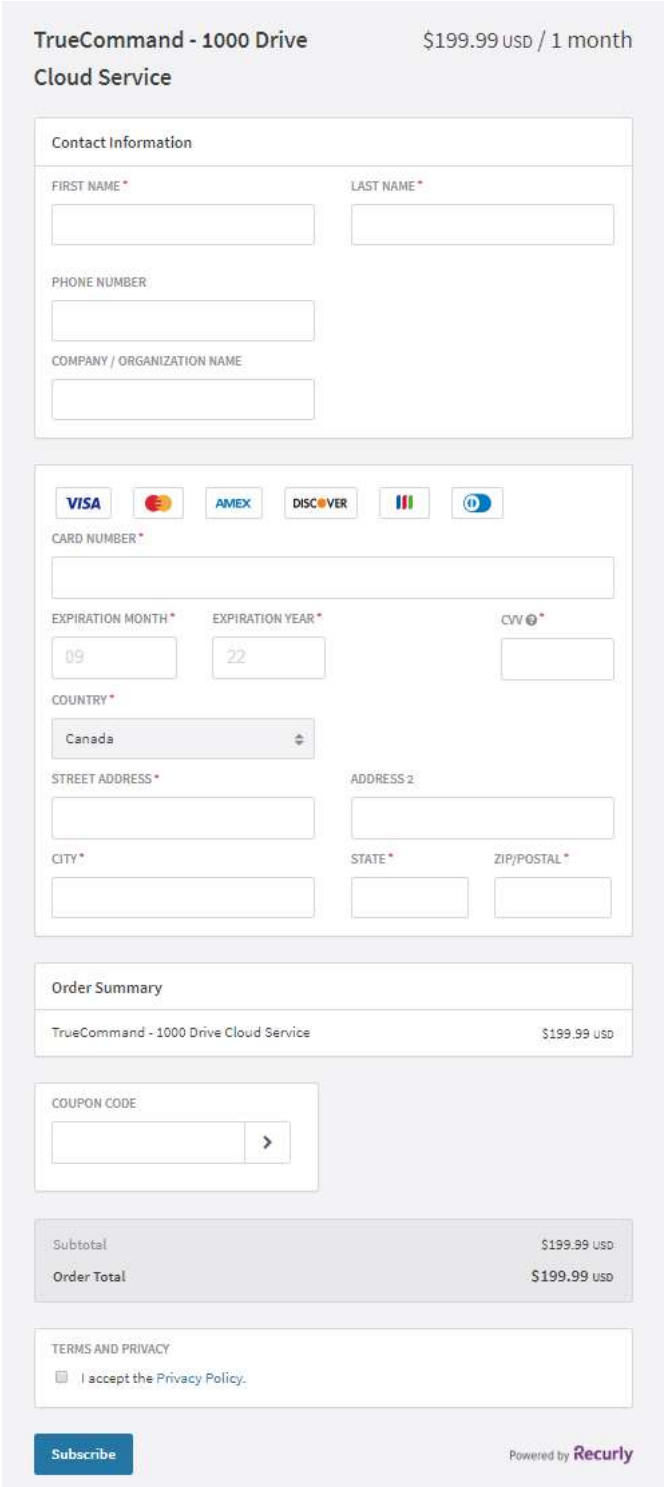

iXsystems TrueNAS FreeNAS TrueCommand iX Community
Account Services
Logout
Welcome jt@obs-sec.com
Account Settings
No active subscriptions!
New Subscription
Trial License
TrueCommand 60 Day Trial
Manage
TrueCommand Quick Links
User Guides and Documentation
Release Notes
Docker Images
Latest VM Image (VHDX)
Latest VM Image (VMDK)
By using this site you agree to the iXsystems EULA and Privacy Policy
2020 © iXsystems Inc - Website Support


iXsystems TrueNAS FreeNAS TrueCommand iX Community
Account Services
Back
Please select a subscription plan:
TrueCommand Cloud (Early Access)
Please select an option
TrueCommand Site License (Self hosted)
Please select an option
By using this site you agree to the iXsystems EULA and Privacy Policy
2020 © iXsystems Inc - Website Support

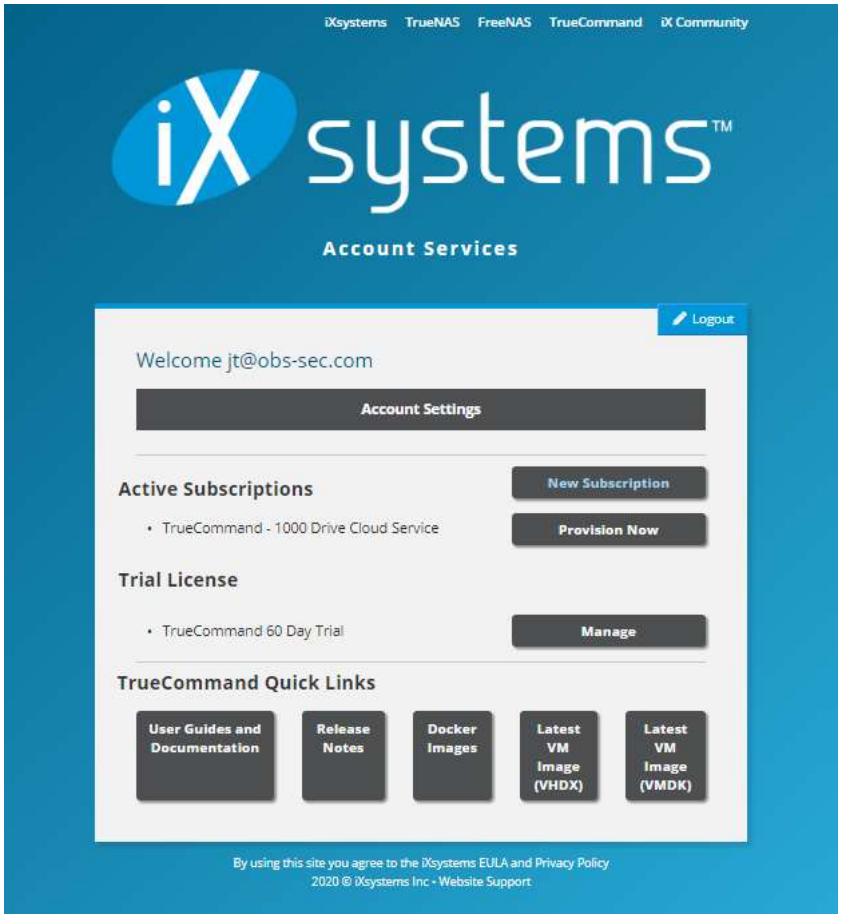
Select the TrueCommand Cloud option and choose the subscription plan that best fits your current needs. This can be changed later.

Click *Continue* to proceed.

Next, fill the payment form.



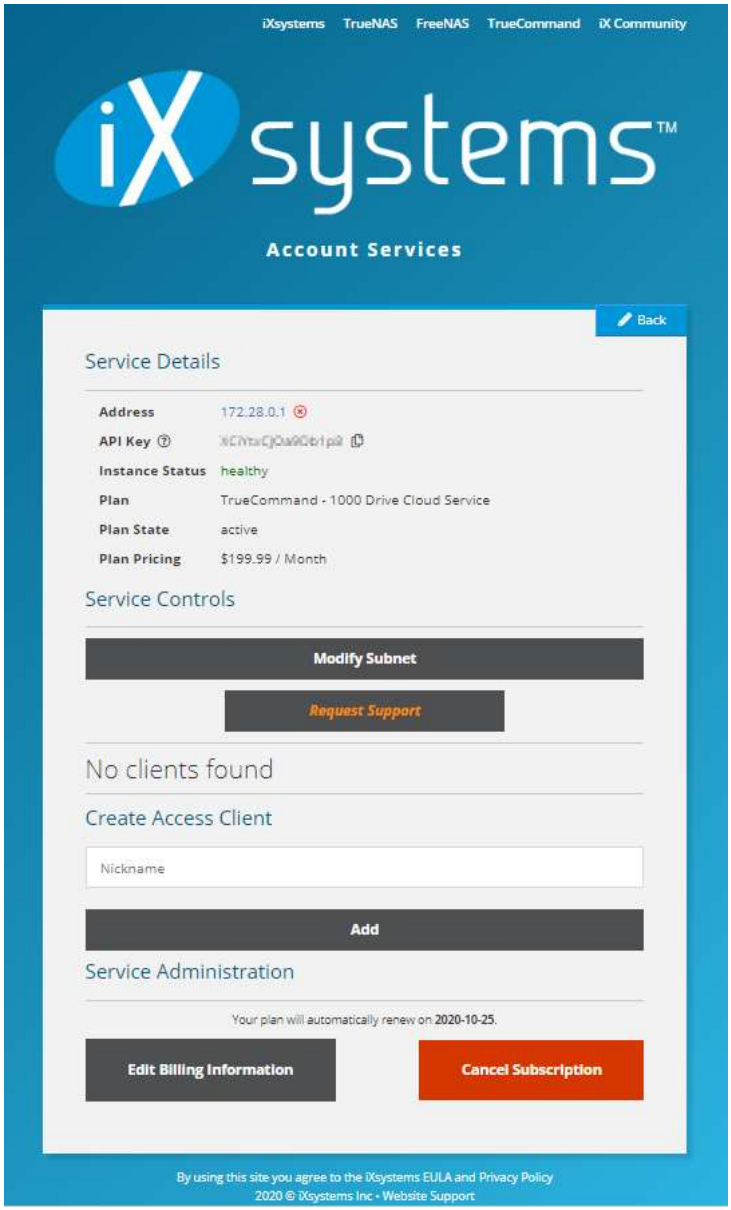
Submit and wait for the form to be accepted. When ready, click *Provision Now*.



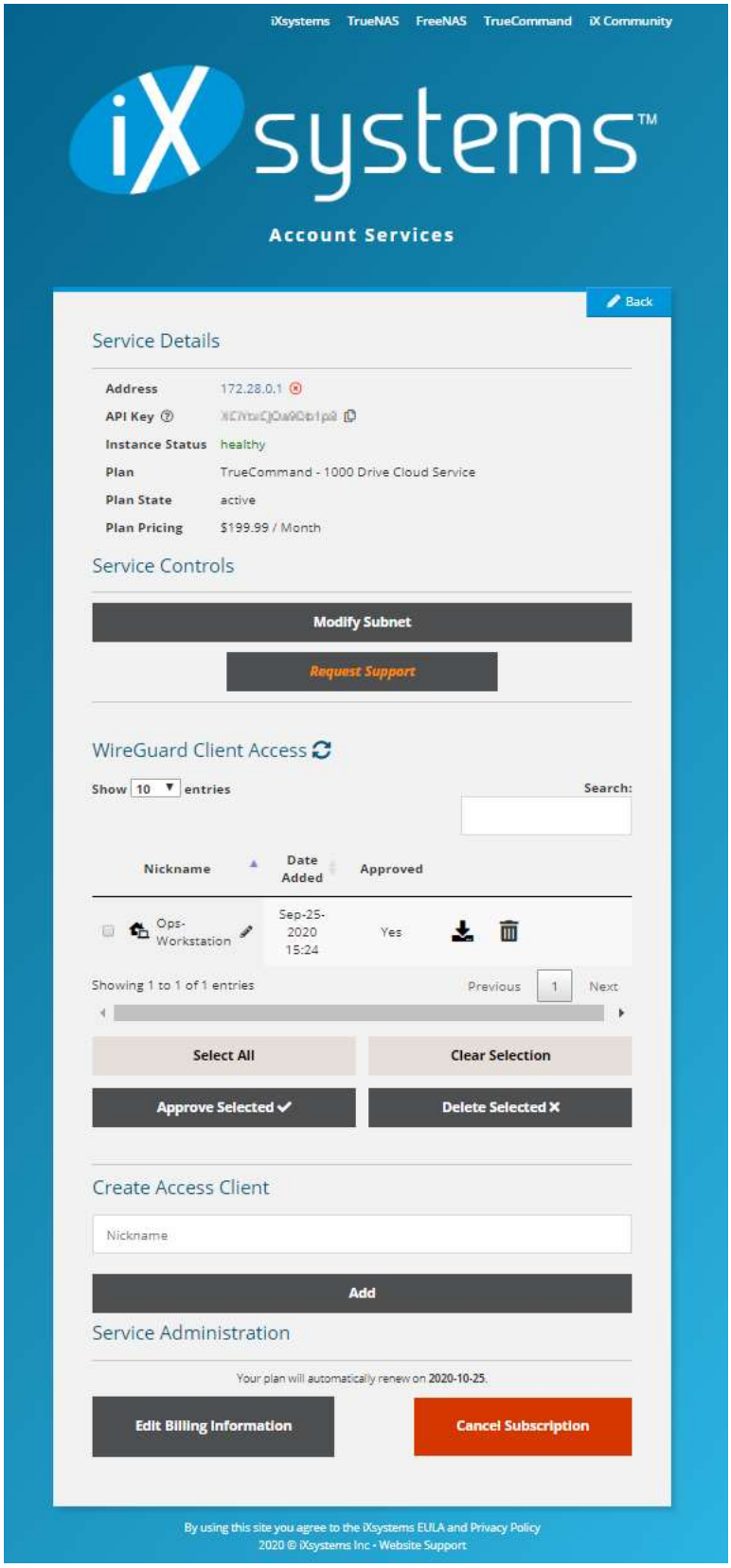
Select a *Subnet* that is not currently used on the network.

Managing a TrueCommand Cloud Account

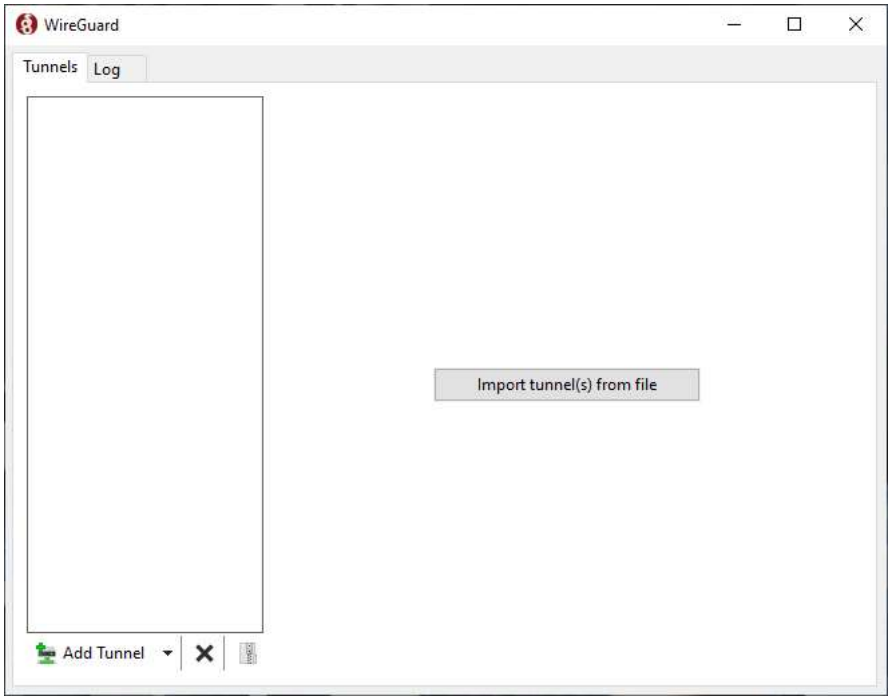
From the account home page, click *Manage*. Add a client for desktop or laptop to obtain a TrueCommand WireGuard Config file.



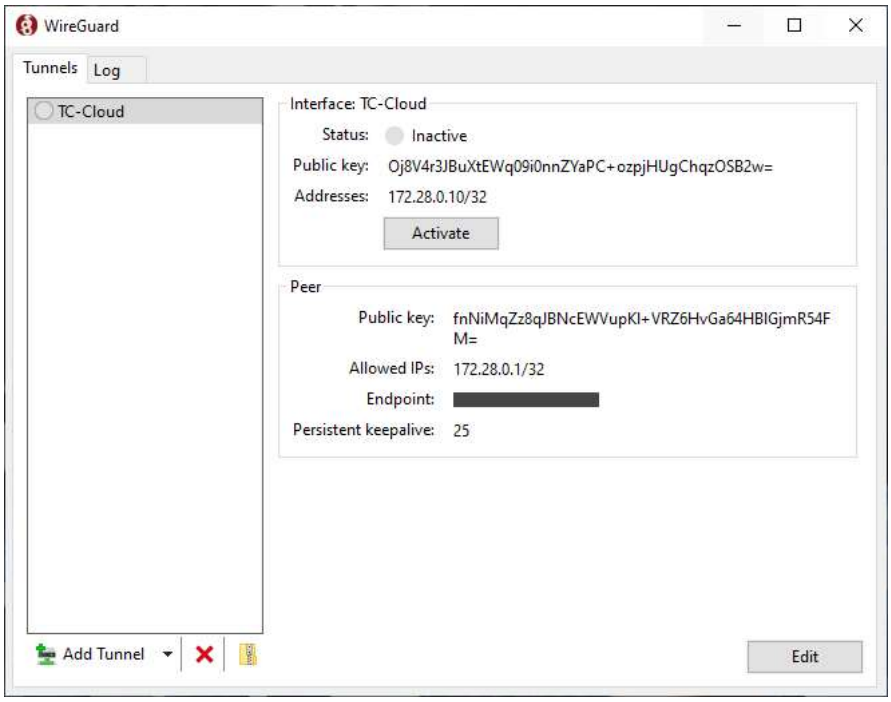
When the client account is created, click to download the configuration file.



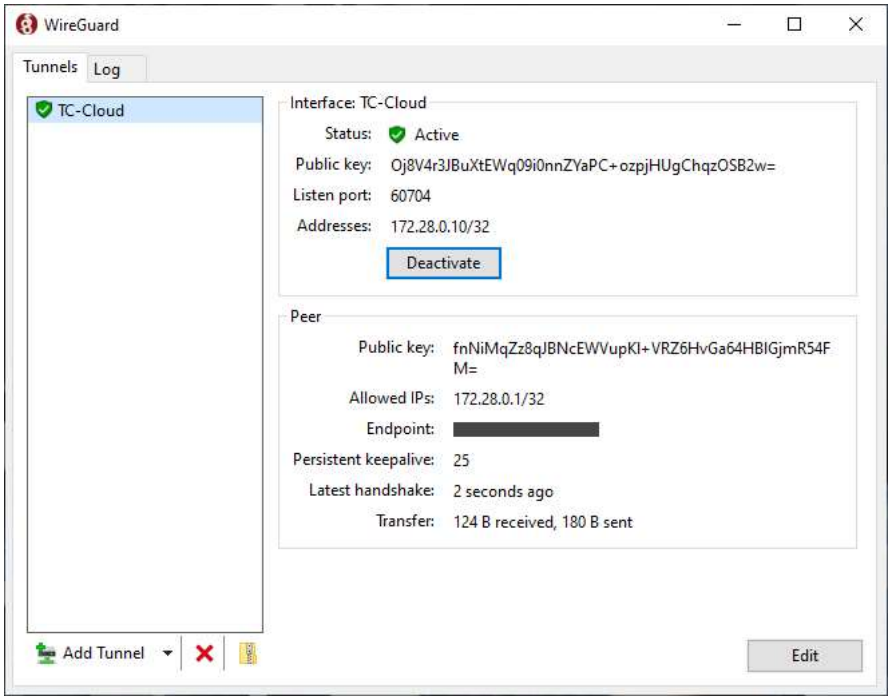
Open Wireguard on your machine and click *Add Tunnel*.



Select the TrueCommand WireGuard Configuration file that was downloaded from the portal. the configuration file into WireGuard on your machine and activate the tunnel.



Click *Activate* to initialize the Wireguard tunnel.

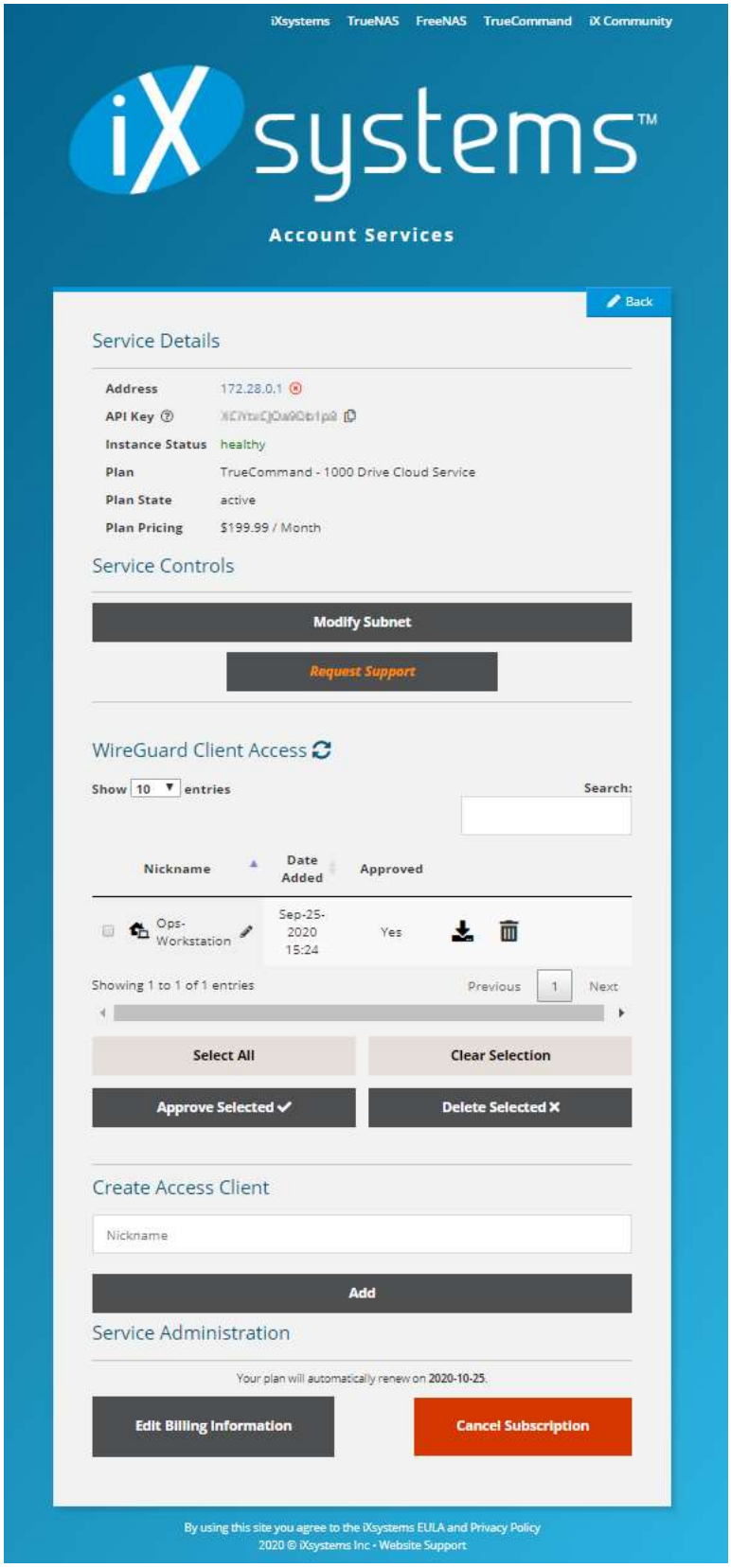


Further information on WireGuard and WireGuard clients is found on the WireGuard home page. The TrueCommand Cloud IP address displays in the iXsystems Account Portal page.

After WireGuard is active, log in to the TrueCommand Cloud Interface by clicking the TrueCommand IP address listed on the portal, or manually entering the TrueCommand Cloud IP in a browser.

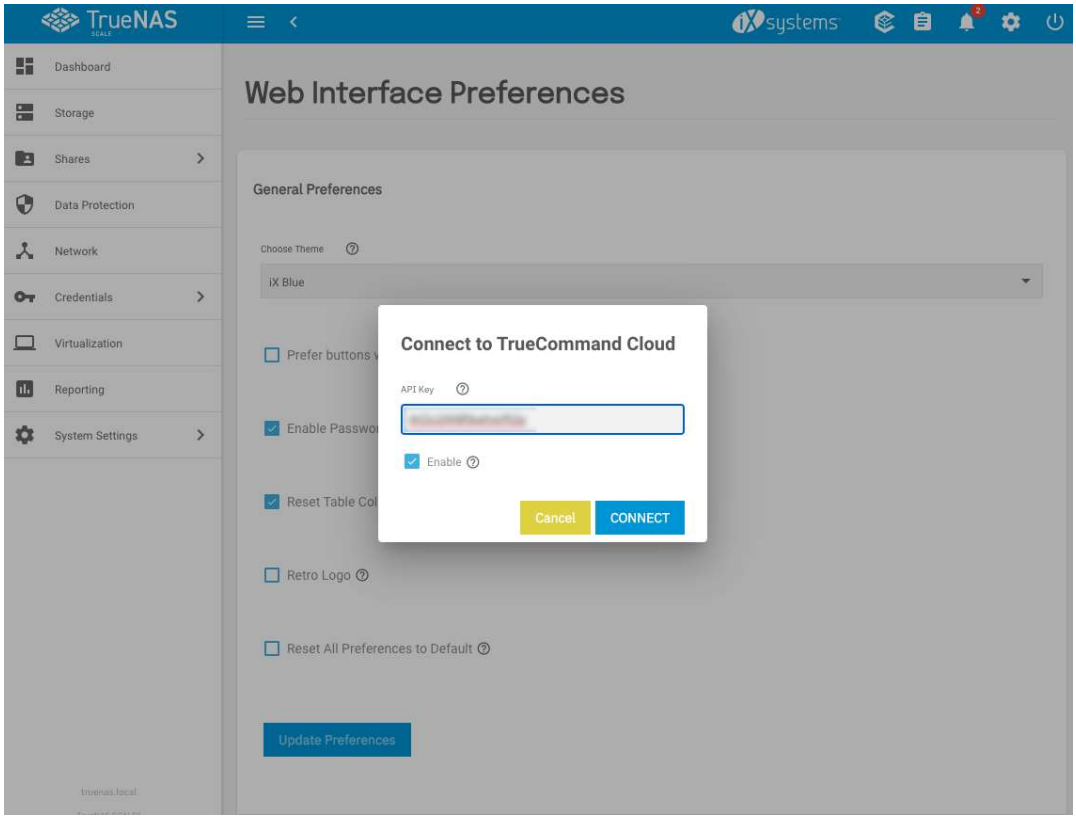
Connecting Systems to a TrueCommand Cloud Instance

Log into the ixSystems cloud account and click *Manage*. Under **Service Details**, copy the *TrueCommand API Key*.



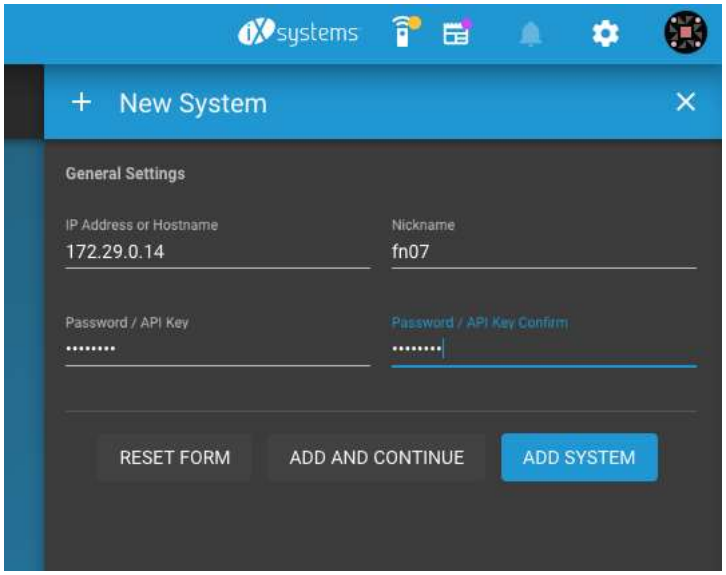
Log into a TrueNAS system and click the TrueCommand icon in the upper right.

Paste the TrueCommand API Key copied from the iXsystems Account Portal into the TrueNAS dialog window.



When the True Command logo starts moving, check the TrueCommand Cloud email address for a verification message. The email contains a link to the Portal to confirm the connection and activate the TrueNAS system.

Click on the **New System** alert, fill in the information from the TrueNAS system, and click *Add System*.



It can take 10 to 15 minutes for the TrueNAS instance to fully sync up with TrueCommand Cloud. When all systems are connected to TrueCommand Cloud, refer to the TrueCommand Administration articles for more instructions about setting up configuration backups, alerts, reports, and role-based access control.

Docker (Linux)

Installing the TrueCommand Container

> Docker Desktop for Windows uses Hyper-V. This interferes with other virtualization applications. For example, Docker Desktop and VMware Workstation Player cannot simultaneously run.

Before fetching the TrueCommand docker image, create a local directory. Enter `mkdir {DIRECTORY}`, where *{DIRECTORY}* is the new name.

After creating the new directory, fetch and run the TrueCommand Docker image. Open a Command Line Interface (CLI) and enter `docker run \--detach -v "/{HOSTDIR}:/data" -p {PORT}:80 -p {SSL}:443 ixsystems/truecommand:latest`. *{HOSTDIR}* is a directory on the

host machine for Docker container data, *{PORT}* is the TrueCommand web interface port number, and *{SSL}* port number for secure web interface access.

To install the container with an earlier TrueCommand release, replace `latest` with the desired TrueCommand version tag:

```
docker run \--detach -v "/DockerDir:/data" -p 9004:80 -p 9005:443 ixsystems/truecommand:1.3.2
```

> Use Windows compatible syntax when specifying paths in the Windows file system. For example, if the created directory for the TrueCommand image was created in the Windows Documents folder, the `docker` command would be: `docker run \--detach -v C:\Users\\Example\\Documents\\DockerDir`. In this command *C* is the drive letter, *Example* is the current user name, and *DockerDir* is the TrueCommand image directory.

Although there are different ways to run a Docker container, `-v /*hostdirectory*:/data` is required for TrueCommand to function.

> Do not try to use the same `hostdirectory` for two different containers! This results in file conflicts and database corruption.

Accessing the TrueCommand Web Interface

After fetching the TrueCommand Docker container, enter `docker ps` to see details about running containers.

Use the port assigned to the container to access the web interface. The list from `docker ps` contains a *PORTS* column. Find the port associated with the `ixsystems/truecommand:latest` *IMAGE*. The *PORTS* entry is listed as `0.0.0.0:port->80/tcp`, `0.0.0.0:sslport->443/tcp` where `port` and `sslport` are the ports specified earlier.

To access the web interface with no encryption, enter `hostsystemIPaddress:port` in a browser address bar, where `hostsystemIPaddress` is the IP address of the host system that is running the TrueCommand Docker container. To access the web interface with standard SSL encryption, enter `https://hostsystemIPaddress:sslport` in a browser address bar.

The connection can't be established?
When a connection to the web interface cannot be established, add the container ports as an exception to the host system firewall.

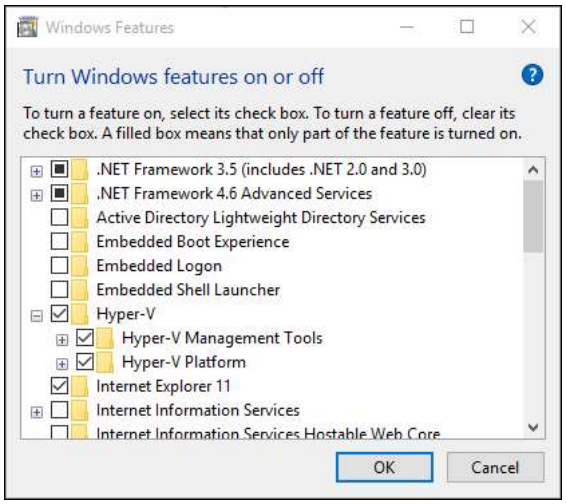
Docker Desktop (Windows)

The requirements to run TrueCommand in Docker Desktop for Windows are:

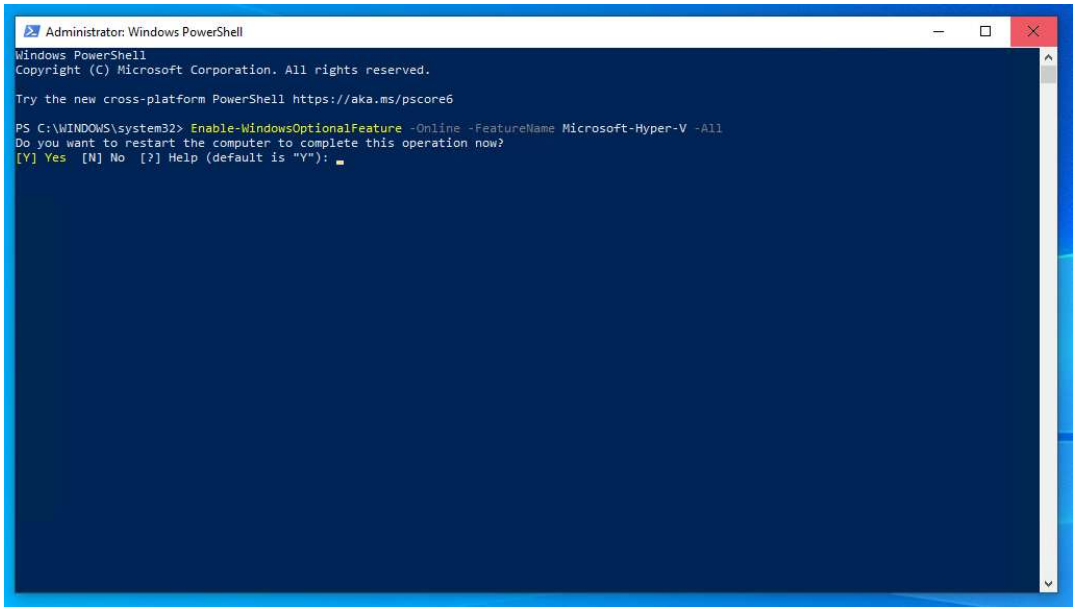
- Windows 10 Enterprise, Pro, or Education editions.
- 64-bit Processor with Second Level Address Translation (SLAT).
- CPU support for VM Monitor Mode Extension (VT-c on Intel CPUs).
- Hyper-V is enabled in Windows 10.
- 4 GB memory at minimum.
- Docker Desktop needs to be installed in Windows.

Enable Hyper-V

To enable Hyper-V, click on Windows Start button and select or search for *Apps & Features*. Select *Programs and Features* under **Related settings** and *Turn Windows Features on or off* (Administrator action). Set the Hyper-V option and click *Ok*. You will need to restart your restart your computer for the change to take effect.



Alternatively, Hyper-V can be enabled with the **Powershell**. To do this, run Powershell as a Windows Administrator and enter `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All`. If an error is returned that says the command could not be found, verify that you are running PowerShell as the Administrator. After the command successfully runs, reboot the computer.



Install Docker Desktop

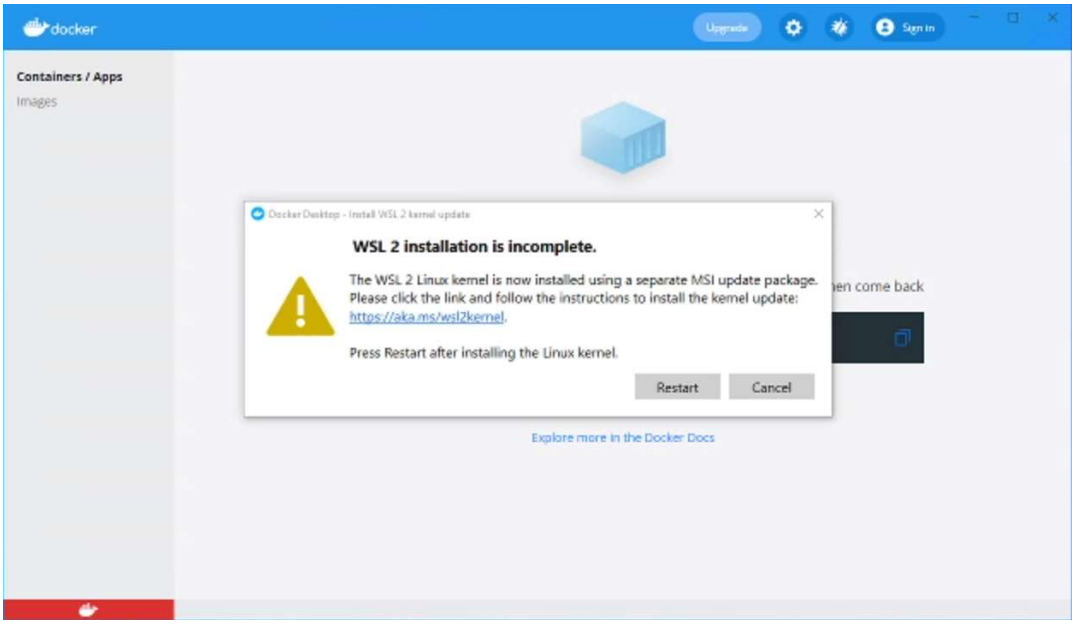
Open Docker Hub and click *Get Docker*.

Run the installer after the download completes. When the installer is finished, reboot the system.

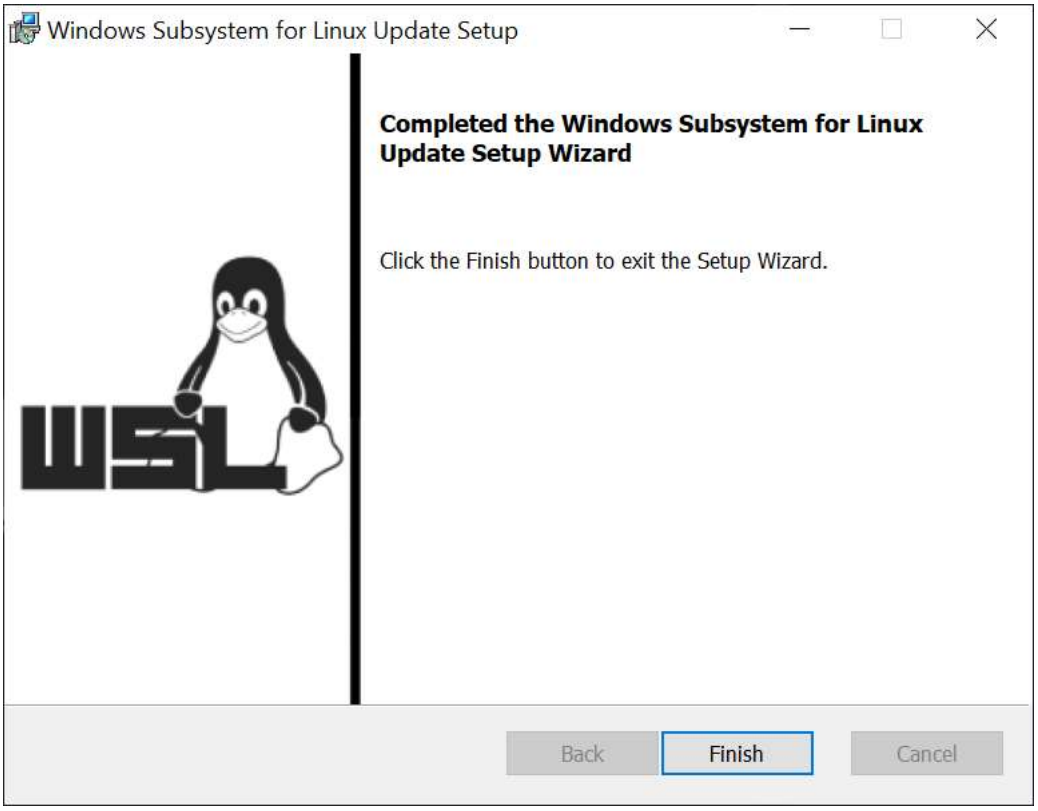
Different Admin accounts?
If the admin account is different from your Windows user account, the user must be added to the `docker-users` group. Run *Computer Management* as an administrator and go to **Local Users and Groups > Groups > docker-users** to add the user to the group. Changes take effect after logging out and back in.

WSL 2 Install Incomplete?

If this error message appears after rebooting, install the Linux Kernel Update Package:

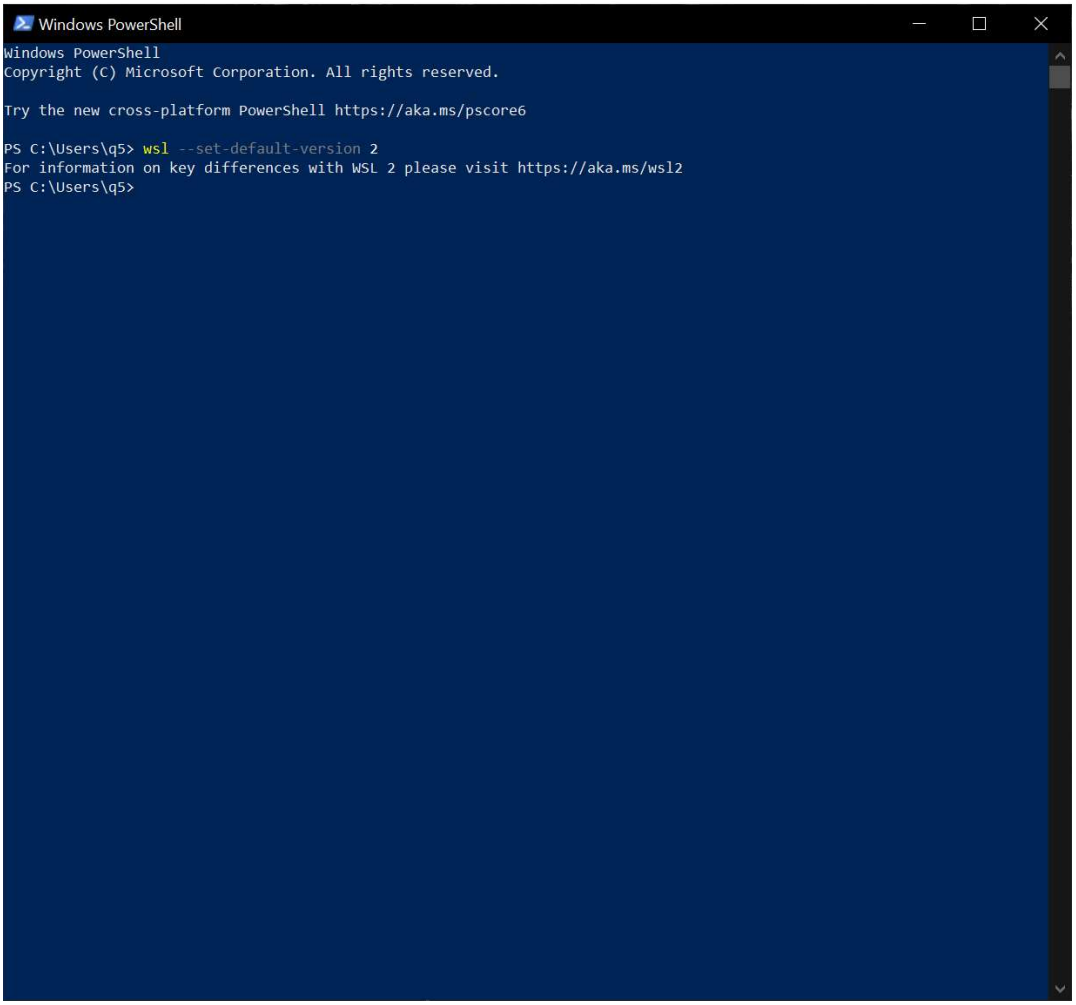


The update package is downloaded from a Windows storage location.



Microsoft has additional documentation available for assistance with downloading the Linux kernel update.

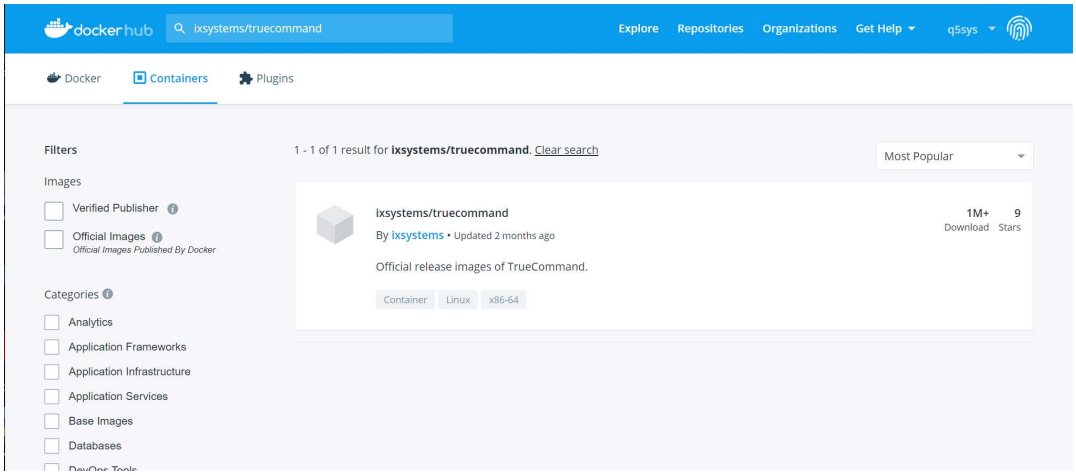
After installing the kernel update, set the WSL default version to `version 2` by opening the Powershell and entering `wsl --set-default-version 2`.

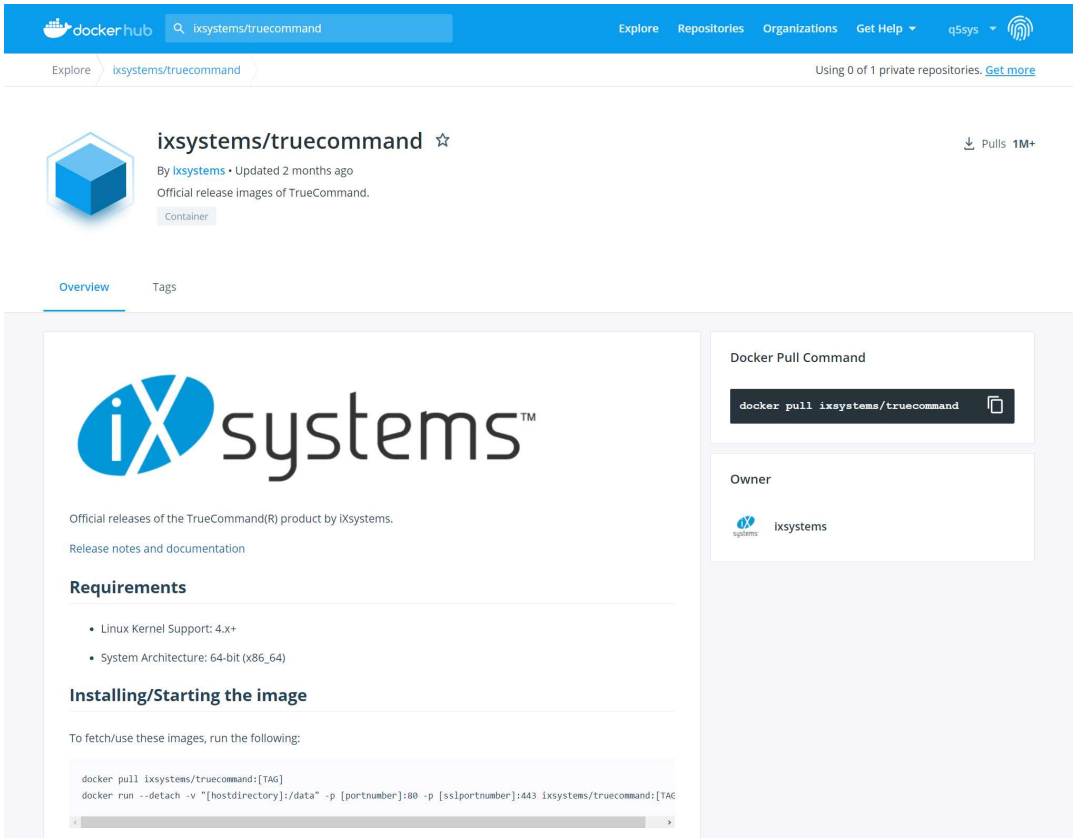


The system must be rebooted after changing the default version.

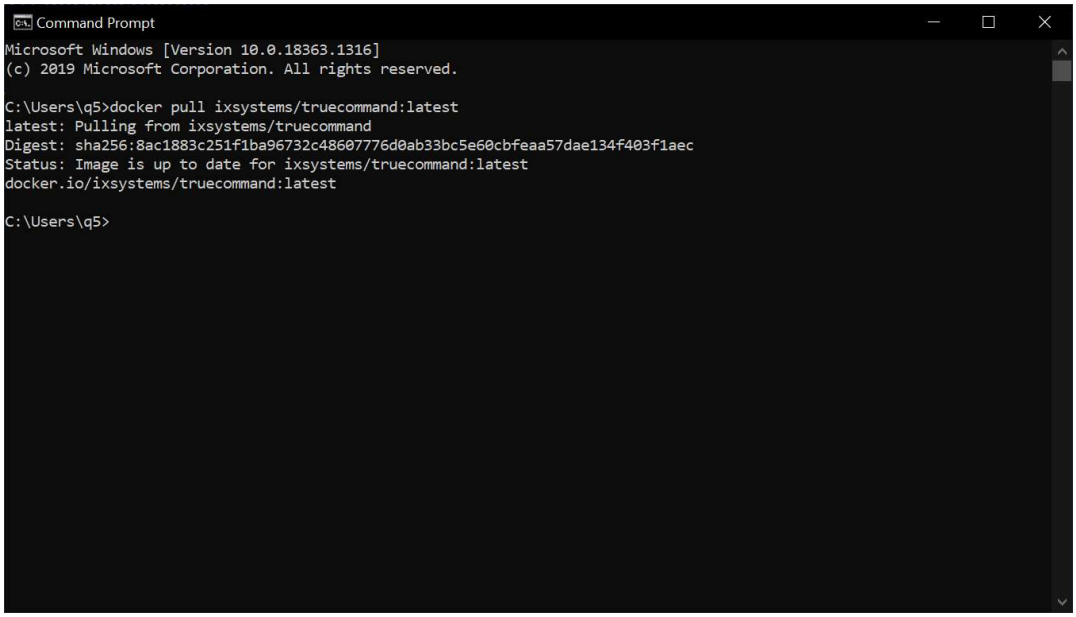
Installing the TrueCommand Docker Container

Open the Docker Hub in a browser and search for `ixsystems/truecommand`.

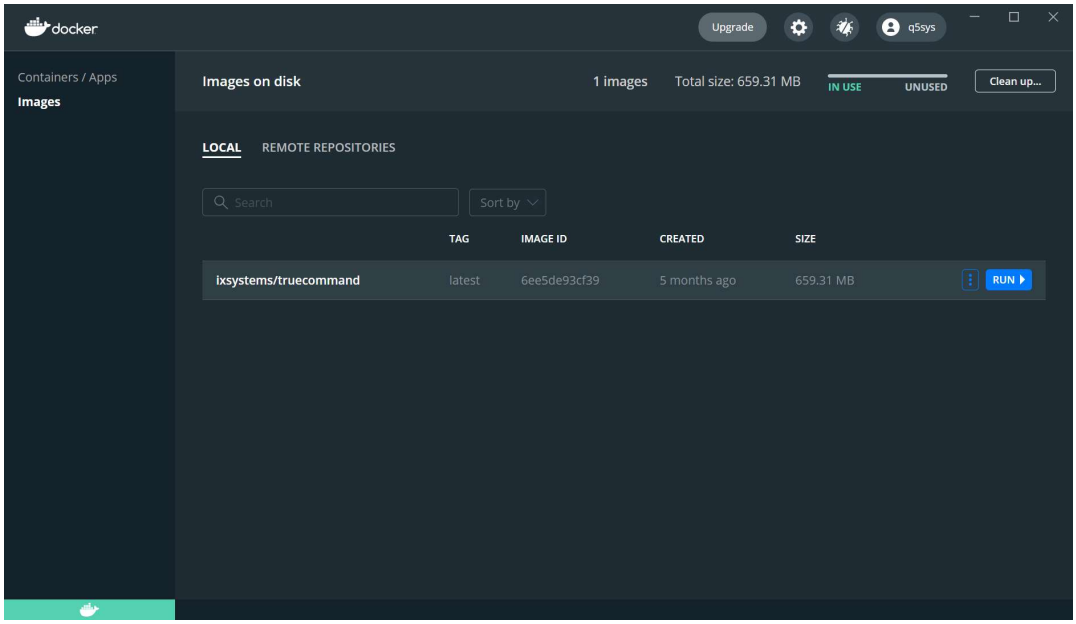




Verify the pull command required and run it from a command line. Example: `docker pull ixsystems/truecommand:latest`.



When the container is downloaded, open the Docker Desktop and select *Images*. Hover over the *ixsystems/truecommand* entry to show the **Run** button, then click it.

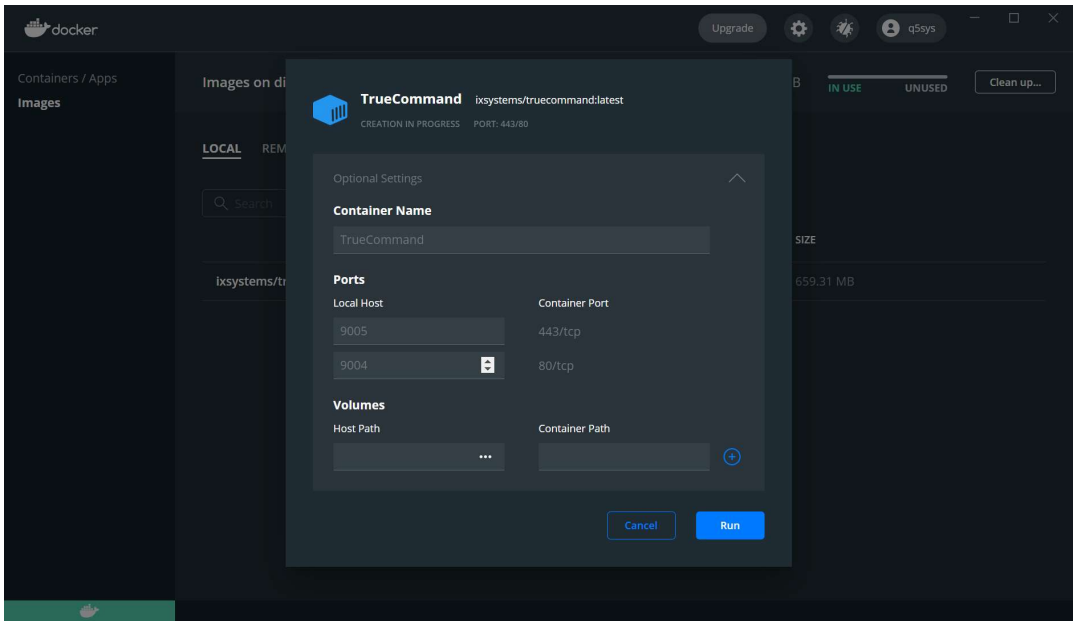


Open the *Optional Settings* drop down menu, name the container, and set the following port values. Investigate your network environment or check with your **IT** department to ensure that these ports will not conflict with any other running services.

- Local Host Port: `9005`
- Container Port `443`

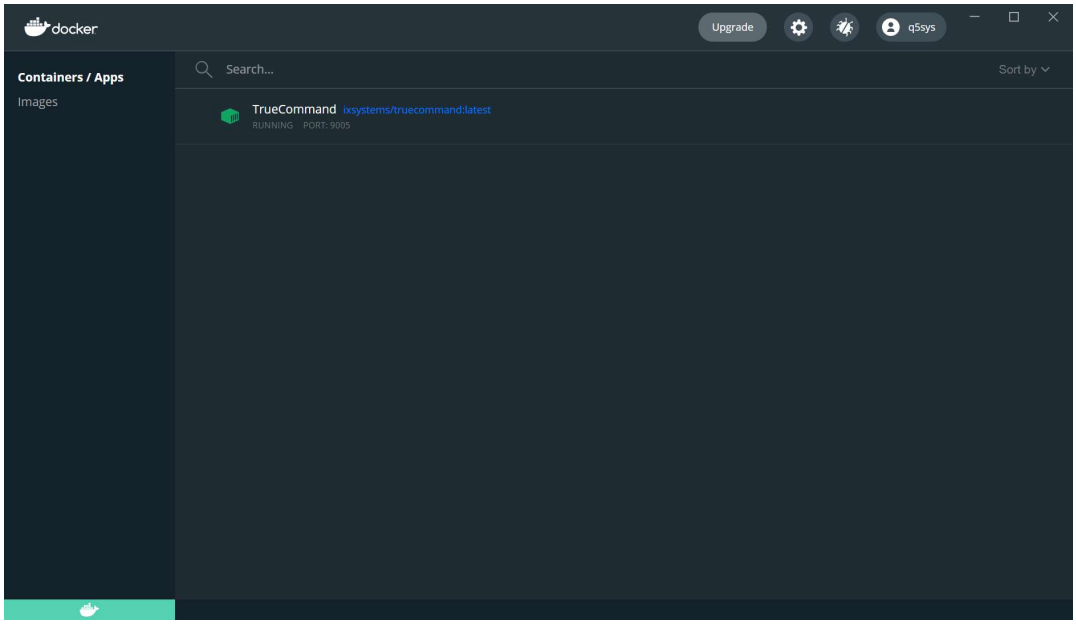
Click the `+` sign to add a second set of ports.

- Local Host Port `9004`
- Container Port `80/tcp`



Setting the **Volume** is not usually required for TrueCommand. Click *RUN* after configuring the settings.

When Docker Desktop shows the container status as **RUNNING**, open a new browser tab and go to `https://127.0.0.1:9005`.

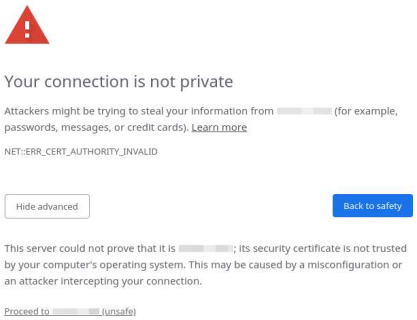


Adding Browser Security Exceptions

TrueCommand uses a self signed certificate for a secure connection. Because of this, many Internet browsers consider the IP address or DNS hostname untrustworthy. In these cases, the IP address or DNS hostname must be added as an exception to the browser to access the web interface. The process of adding an exception is shown here for two different browsers, but the procedure is similar for most browsers.

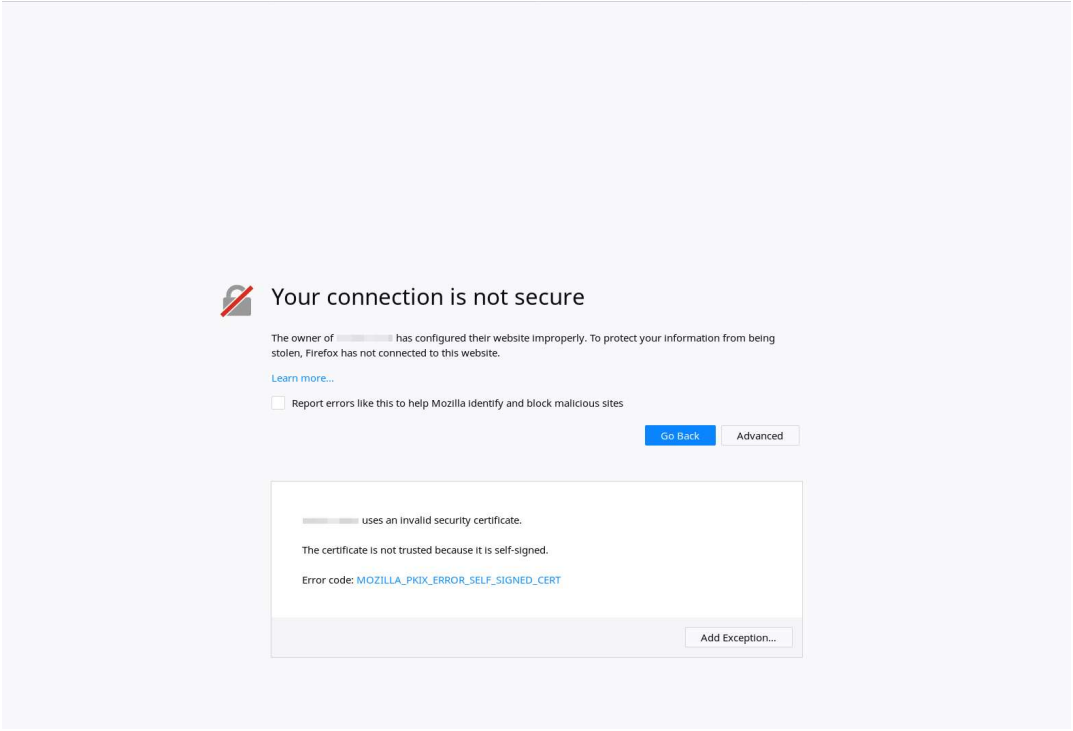
Chrome

Click *Advanced* to view information about the error code. Click *Proceed to {hostname} (unsafe)*.



Firefox

Click *Advanced* to view information about the error code.



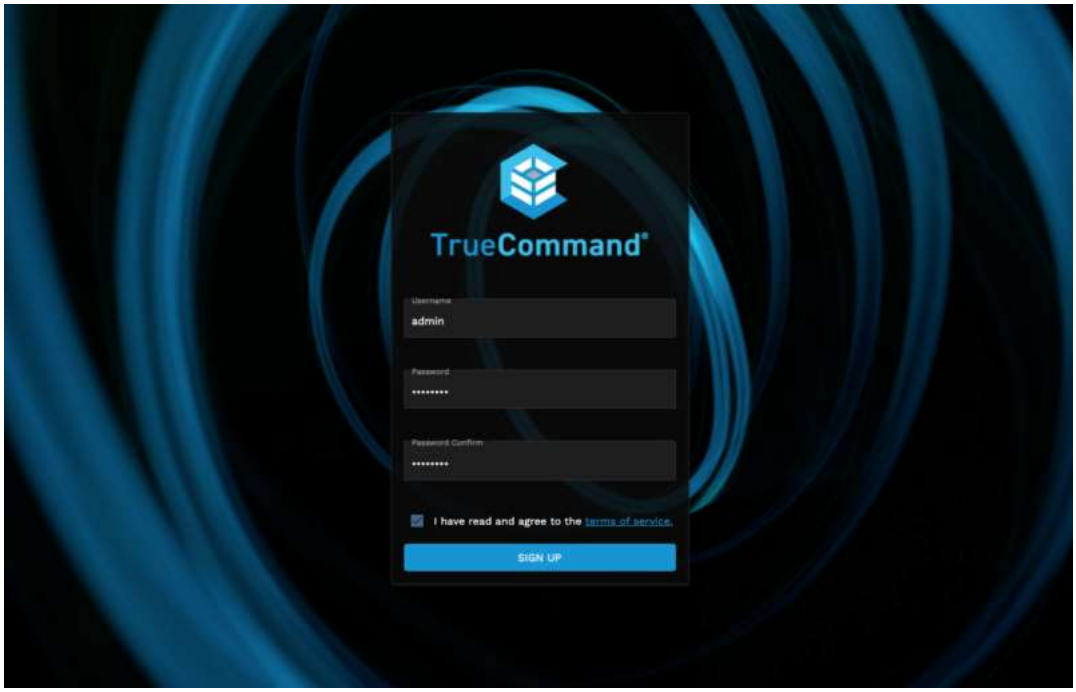
Click *Add Exception…*. Set *Permanently store this exception* to keep the IP address or DNS hostname permanently stored in Firefox. Click *Confirm Security Exception*.

Creating the Administrator Account

Accessing the interface for the first time prompts to create an administrator account.

Follow these steps to create a new admin user:

- Enter a username and password.
- Read the Terms of Service, set *I have read and agree to the terms of service*, and click *SIGN UP*.



- The TrueCommand login screen reappears and you can now use these administrator credentials to log in to the TrueCommand web interface and begin connecting TrueNAS systems, creating more login accounts, and configuring statistical reports.

3.1.1 - Update Docker

Updating TrueCommand installed in a Docker container requires stopping the existing container, obtaining the latest software image from the *ixsystems/truecommand* hub, and starting an updated container using the preexisting TrueCommand storage volume.

This article shows how to do this using the command line, but different container management applications can be used to accomplish the same task. Log in to the Docker host system for the container update process.

> On Linux systems, `docker` commands need to be run as the *root* account. You might need to add `sudo` in front of the example command to run the command as *root*: `sudo docker image pull ixsystems/truecommand`.

To view all active containers, enter `docker ps`:

```
joe@joe-minty:~$ sudo docker ps
[sudo] password for joe:
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STATUS                  PORTS
d595961d9024        ixsystems/truecommand:latest   "/start.sh"              15 minutes ago      Up 15 minutes           443/tcp, 0.0.0.0:8080-
```

For the rest of the examples in this article, we'll be referring to `TrueCmd_contained` for the container name. Be sure to replace this with your TrueCommand container name.

You will also need to note the path to the volume that the container uses for your TrueCommand configuration. You'll need to use this volume when starting the updated Docker container to continue using your existing TrueCommand configuration.

Docker Container Commands

There are a few general Docker commands to remember when interacting with a TrueCommand container:

To start or stop the TrueCommand container, enter `docker start <container name>` or `docker stop <container name>` on the Docker host system.

To have the container automatically start when the Docker host system boots, ensure that the Docker daemon is configured to run at system boot and add the `--restart` flag to the initial `docker run` command:

```
docker run --name=<the name to call the container> -v=”<local directory>:/data” -p <host port>:80 sslport <host port>:443 --detach --restart ix
```

For a full history of every container that the host has run, use `docker ps -a`:

```
joe@joe-minty:~$ sudo docker ps -a
[sudo] password for joe:
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STATUS                  PORTS
d595961d9024        ixsystems/truecommand:latest   "/start.sh"              15 minutes ago      Up 15 minutes           443/tcp, 0.0.0.0:8080-
214a0275a216        phpmyadmin/phpmyadmin          "/docker-entrypoint.…"   7 weeks ago         Exited (0) 11 days ago
0a68db912cce        phpwork                "docker-php-entrypoi…"   4 months ago        Exited (0) 11 days ago
d0ae8d0a839f        mysql:5.7                      "docker-entrypoint.s…"   4 months ago        Exited (0) 11 days ago
```

Update Process

To update, download the latest TrueCommand image and remove the existing TrueCommand container. Then restart the container using the latest TrueCommand image and preexisting TrueCommand storage volume.

To remove the existing container, enter `docker rm TrueCmd_contained`. Now run `docker image pull ixsystems/truecommand`. By default, the latest image of TrueCommand is pulled to the Docker host. Start a new container that uses the new image, but make sure to use the preexisting volume that was being used for the original TrueCommand container:

```
docker run --name <the name to call the container> -v ”<local host directory>:/data” -p <host port>:80 sslport <host port>:443 --detach ixsyste
```

Example without https:

```
sudo docker run --name TrueCmd_contained -v "/home/joe/Documents/TrueCommandContainer:/data" -p 8080:80 -d ixsystems/truecommand:latest
```

When the container is created, Docker will use the image previously downloaded with `docker pull`. A page refresh might be required to view the changes, but previous settings and systems remain available due to the volume reference.

3.1.2 - Migrate Legacy to 1.2+

Starting with TrueCommand 1.2, TrueCommand is built and offered as a Docker container to drastically reduce system overhead and simplify TrueCommand updates. Migrating data can be done before or after installing the Docker container version of TrueCommand. The procedure is similar in both situations, with just a couple extra steps when the Docker container version of TrueCommand is already installed.

Process Summary

- Preparing an existing container
  - Turn off the container
  - Wipe the container database
- Migrating a previous TrueCommand Configuration
  - Find/Create local system directory to store TrueCommand Docker container data
  - Copy existing TrueCommand configuration files to new directory
  - Transform `ixdb` database into `ixdb.sql` and move *.sql* into container database directory

Preparing an Existing Container for Migration

> Migrating the configuration from a previous version of TrueCommand will overwrite any existing configuration! Migrating the configuration before installing the Docker container is recommended, or as soon as possible after installing to prevent making and then losing any new configuration settings.

Migrating a previous configuration into an existing TrueCommand Docker container installation requires wiping the existing database from the container and replacing with the `ixdb.sql` database from the previous version of TrueCommand. Make sure the container is turned off. Open the directory you specified to use for managing the container and find the `ixdb` directory. Remove all existing files from this directory. The container is ready for data migration from the previous version of TrueCommand.

Follow the steps in the next section to transfer the certificate, license, and database files into the existing container configuration directory.

Migrating a Previous TrueCommand Configuration

To move an existing TrueCommand 1.1 or earlier configuration to a Docker container version, follow these migration steps:

1. Create a local system directory for Docker container data. This step is only needed when the Docker container version of TrueCommand is **not** already installed. This directory will contain all the TrueCommand docker container data, including configuration files. For the rest of these instructions, this directory will be referred to as `localhostdirectory/`. When the Docker container is already installed, find the existing `localhostdirectory/` you specified during container installation.
2. Find and copy any existing TrueCommand 1.1 or earlier configuration files to the new `localhostdirectory/`. Using a command like `ssh` or `rsync` is recommended. The Docker container will read these files and apply the existing configuration to the container when it is installed. The table lists the default location and required destination for all the different configuration files TrueCommand 1.1 or earlier can create. Only files that already exist need to be copied to the new TrueCommand `localhostdirectory/`.

Files from TrueCommand 1.1 and earlier	Copy destination in local host directory	Description
`/usr/local/etc/truecommand/server.[crt	key].custom`	`localhostdirectory/truecommand/`
`/var/nas-db-backup`	`localhostdirectory/`	Directory tree of NAS configuration backups.
`/var/db/.tv_license.sha512`	`localhostdirectory/`	License and signature for the license.

3. For the TrueCommand 1.1 `/var/db/ixdb/` database, use `pg_dump ixdb > ixdb.sql` to transform the database into a single *.sql* file. Then move `ixdb.sql` to the `localhostdirectory/` for the TrueCommand Docker container.

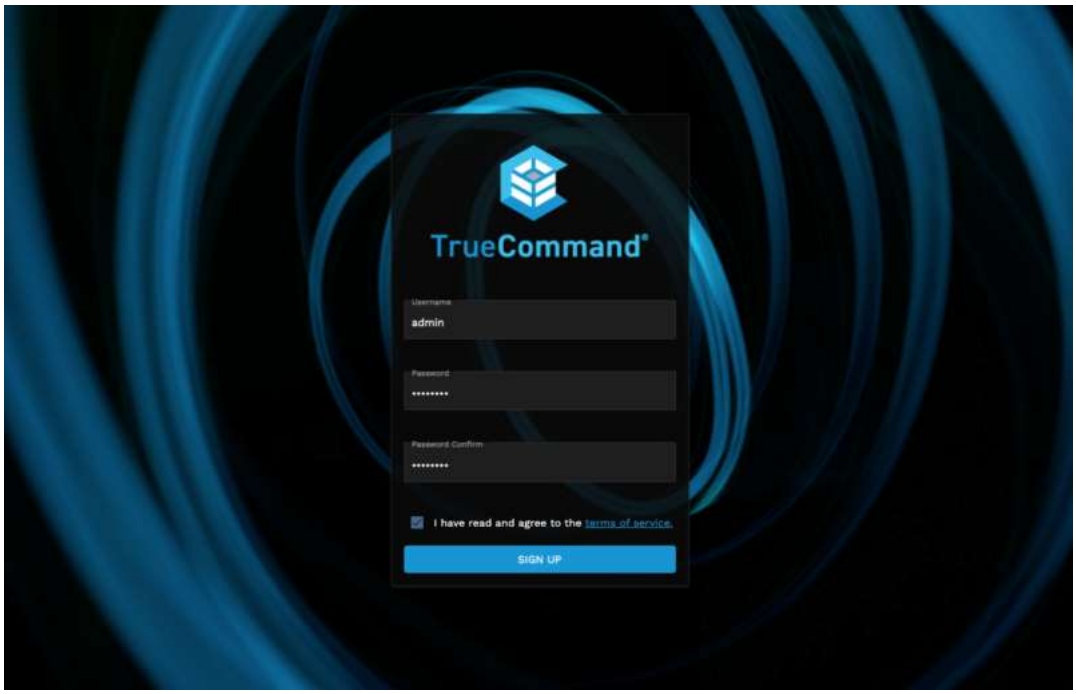
You're now ready to install or start the TrueCommand Docker container. Be sure to specify the `localhostdirectory/` during container installation for TrueCommand to load the migrated data.

3.2 - Interface Overview

First Time Login

Creating the Administrator Account

When accessing the interface for the first time you will need to create an admin account.



- Enter a username and password.
- Read the Terms of Service, set **I have read and agree to the terms of service**, and click **SIGN UP**.
- The admin login credentials will be created and you will be presented with the login page.

You can now log in to the TrueCommand web interface with the new administrator account credentials.

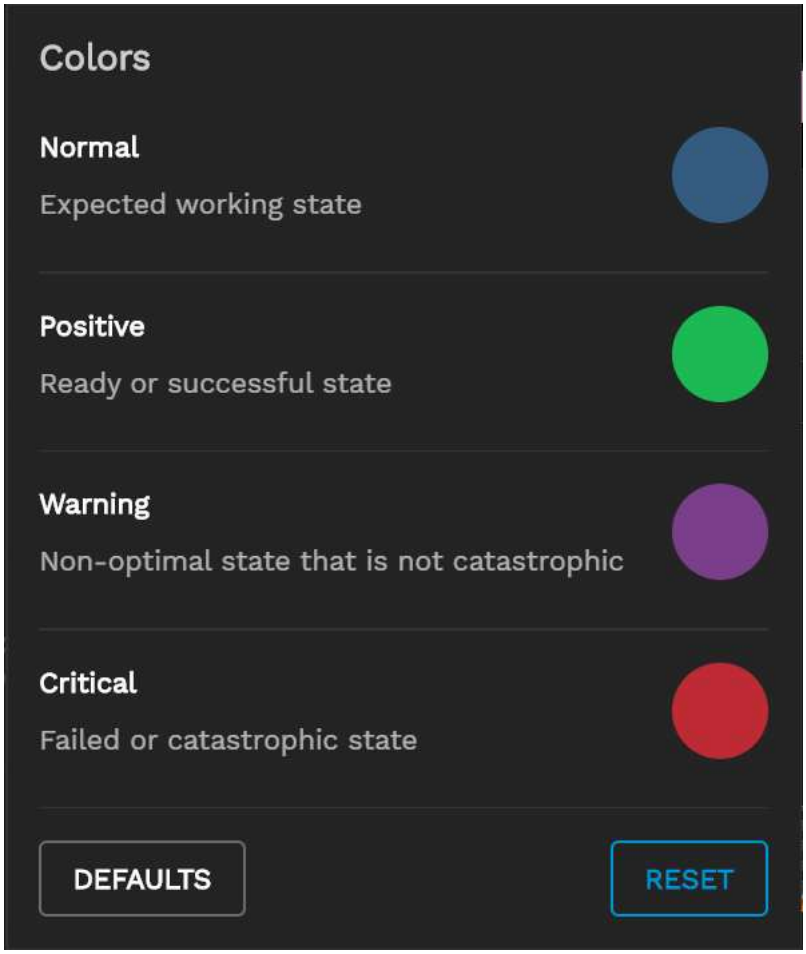
Top Bar

The Top Bar has various quick links, configuration options, Alerts, and Menus.

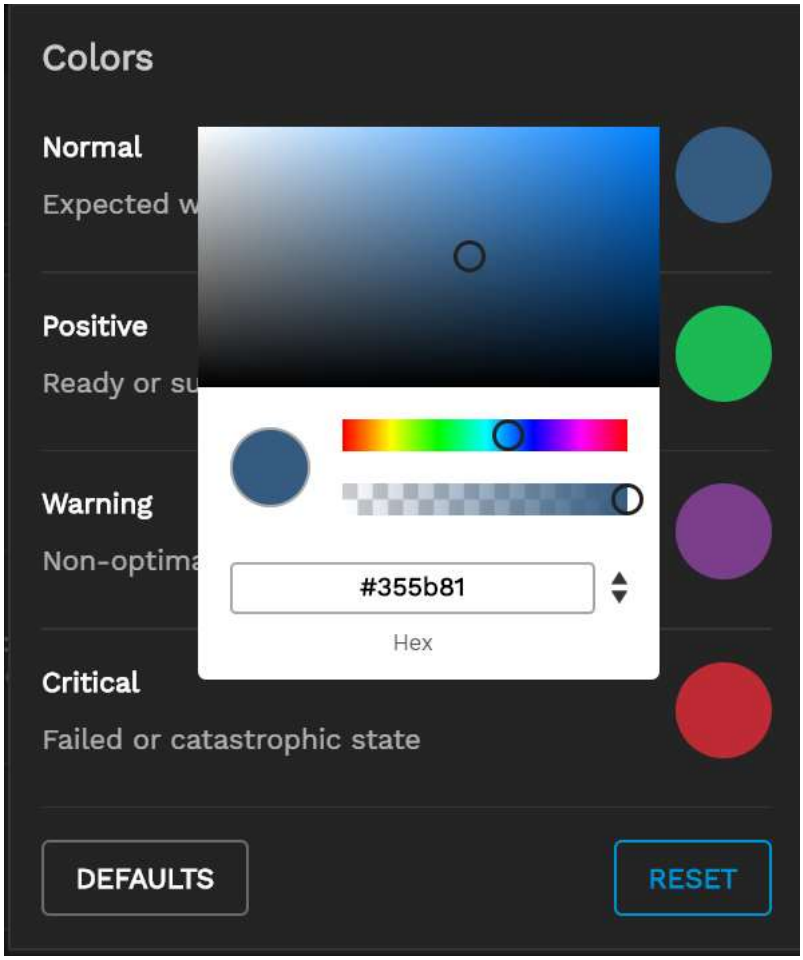
- Clicking opens the Cluster Volume Page.
- Clicking opens the Reports page.
- Clicking toggles Documentation Tooltips.
- Clicking opens the Theme Settings Dropdown.
- Clicking opens the Alert Notifications page.
- Clicking opens the Settings Menu dropdown.
- The User Menu will display your user avatar. If no avatar has been set it will show your default user gravtar. Clicking the User menu will open the the User Menu dropdown.

Themeing

TrueCommand includes the ability to customize the alert colors to user preferences. The Theme pallet is located in the top banner on the right. To open the theme configuration menu, click the icon.



To change a color, click on the color to open a selection menu. Select the desired color or enter its HEX color value.



To remove changes and revert to the currently saved settings, click *Reset*. To reset all colors to the application defaults, click *Defaults*.

Settings Menu

The Settings mention has the following options:

- Clicking opens the main TrueCommand Dashboard.
- Clicking opens the Cluster Volume page.
- Clicking opens the iSCSI Manager page.
- Clicking opens the Reports page.
- Clicking opens the Alerts page.
- Clicking opens the Alert Rules page.
- Clicking opens the Alert Services page.
- Clicking opens the Systems page.
- Clicking opens the Users page.
- Clicking opens the Teams page.
- Clicking opens the Logs page.
- Clicking opens the Administration page.

User Menu

The Settings mention has the following options:

- Clicking opens the User Profile page.
- Clicking opens the API testing page.
- Clicking opens the TrueCommand EULA.
- Clicking logs the user out of TrueCommand.

3.3 - Creating User Accounts

TrueCommand has a robust user management system designed to allow TrueCommand administrators to personalize the TrueCommand experience for each user account. You can create user accounts in the TrueCommand interface. Alternatively, LDAP can automatically create new user accounts when someone logs into TrueCommand with their LDAP credentials.

User accounts also organize into “Teams” for simultaneous management of large numbers or related user accounts.

Administrator Accounts

TrueCommand has two levels of accounts - Administrators and Users:

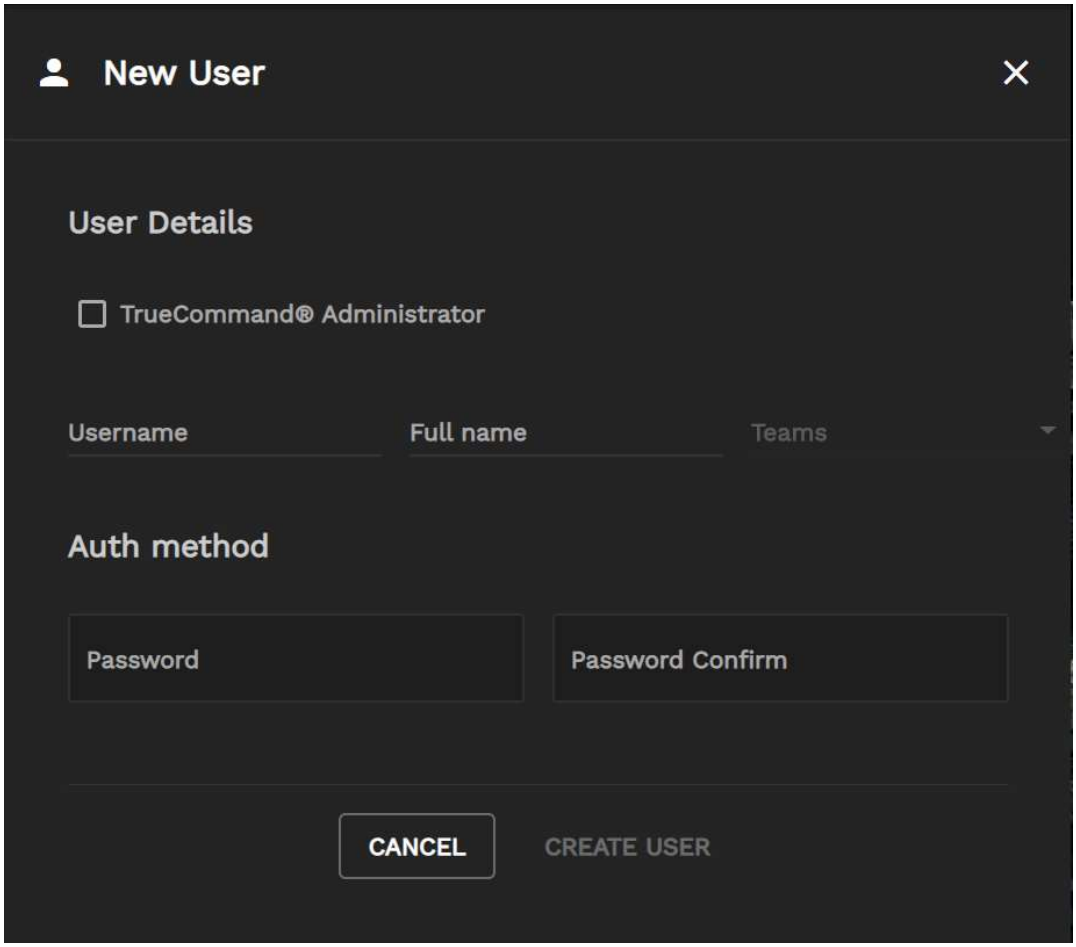
Administrators can add and remove users and servers. Administrators can also assign Users to Teams and Servers to Groups. Administrators have full access to all Alerts and Reports.

Users on the other other hand can only interact with the servers they have been assigned by an Administrator.
Users can configure alerts and generate reports on their respective systems.

Users and Teams

To create a new user account, open the **Configure** menu and click *Users* > + *NEW USER*. Enter a descriptive user name and an authentication method for the user.

TrueCommand uses the *DEFAULT* authentication method to create unique credentials for logging in to the web interface. The administrator has to provide these credentials to the intended user.



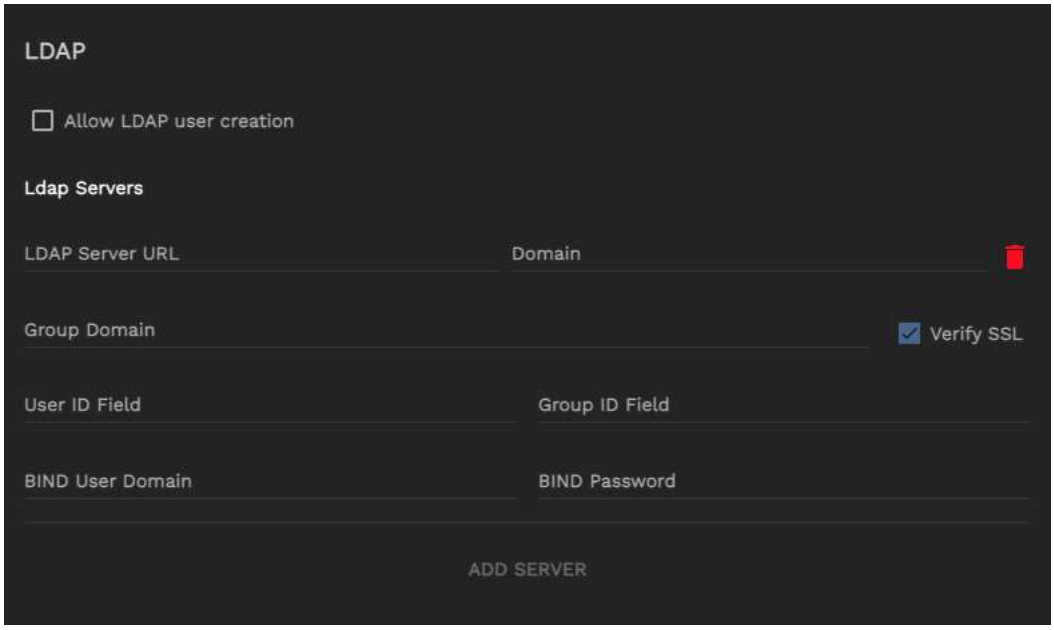
Automatic Creation with LDAP

TrueCommand supports using LDAP to better integrate within an established network environment. *LDAP/AD* allows using single sign-on credentials from the Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). This means a user can log in

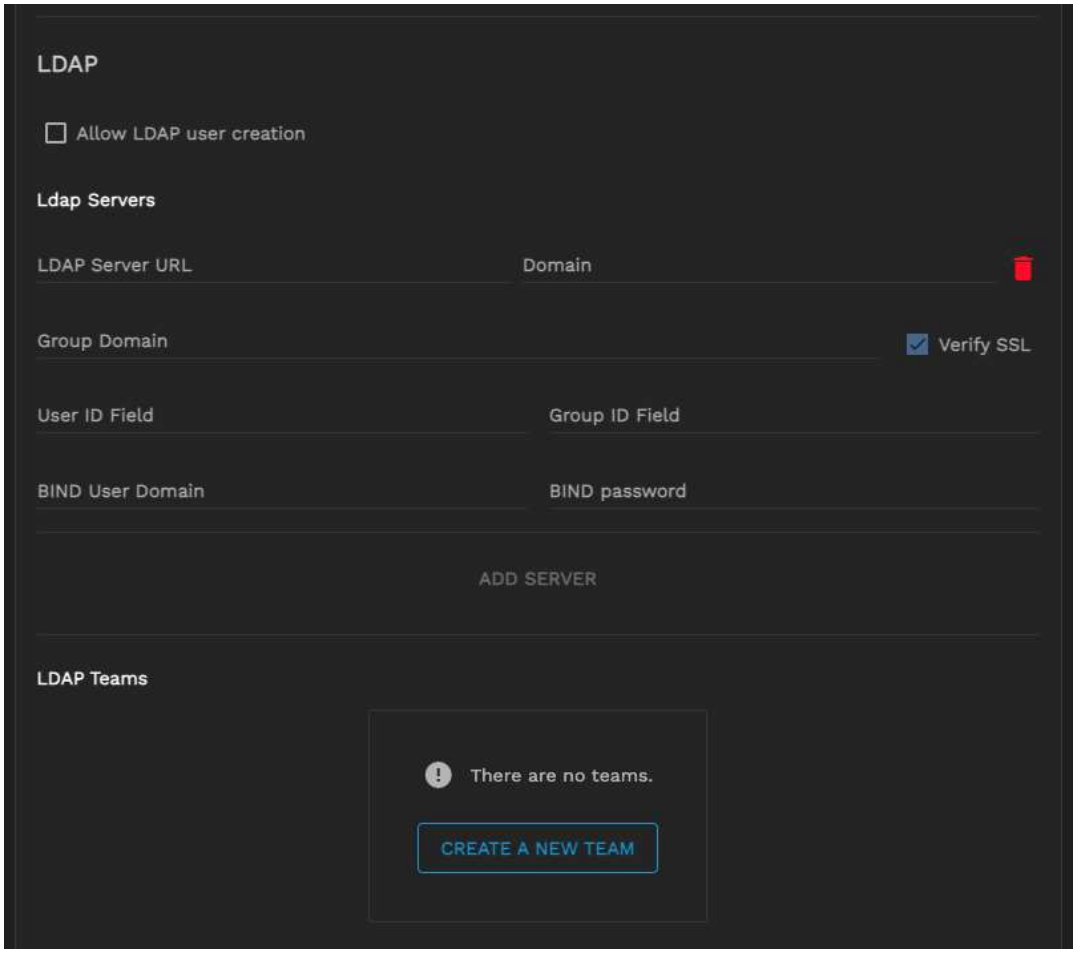
with an LDAP or AD account without creating a separate TrueCommand login.

The LDAP server IP address or DNS hostname and Domain are required to use LDAP/AD. The LDAP or AD Username (optional) is required when the TrueCommand user name does not match the LDAP or AD credentials.

Click on the **(Gear) > Administration**.
Open the *Configuration* Tab to access the LDAP configuration section.



To configure LDAP, add an LDAP server IP address or DNS hostname, fill in the *Domain*, and click *ADD SERVER*. Multiple LDAP servers and Domains can be added.



Field	Value

Field	Value
LDAP Server URL (string, Required)	IP or DNS name of the LDAP server, with port number on the end. Example: “ldap.mycorp.com:636” (SSL port is typically 636 for AD/LDAP)
Domain (string, Required)	Base domain settings of the user. Example: “dc=mycorp,dc=com” for a typical username@mycorp.com user account
Group Domain (string)	The alternative domain setting to use when searching for groups. The Default value is the same as *Domain*
Verify SSL (bool)	Require strict SSL certificate verification. The default value is false. Disable this option if the hostname of the system is different than the one listed on the SSL certificate, an IP is used for the connection instead of the DNS hostname, or if a self-signed certificate is used by the LDAP server.
User ID Field (string)	Domain fieldname to use for user-matching. The default value is “uid” (user ID). Another field commonly-used is “cn” (common name)
Group ID Field (string)	The domain fieldname to use when searching for a group name. The default value is “cn” (common name).
BIND User Domain (string)	The full domain setting for a pre-authenticated bind to the server. Example: “uid=binduser,cn=read-only-bind,dc=mycorp,dc=com” For an unauthenticated bind set this field to just a name (example: “truecommand-bind”). This is sometimes used for logging purposes on the LDAP, but otherwise is not validated.
Bind Password (string)	The password to use for the bind user. For an unauthenticated bind, leave this field blank while setting the *BIND User Domain* to a non-empty value.

LDAP connection options

TrueCommand supports two common methods of validating LDAP user credentials:

Direct Bind

The Direct Bind method uses the *Domain* and *User ID Field* to create a static domain string which is then used to authenticate the user.

Example:

- Domain: “dc=mycorp,dc=com”
- User ID Field: “uid”

When user “bobby.singer” attempts to login, TrueCommand will establish an SSL-secure connection to the LDAP server and then attempt to bind with the static domain “uid=bobby.singer,dc=mycorp,dc=com” and the user-provided password. If successful, then the user authentication has been verified and Bobby Singer is allowed access to TrueCommand.

Indirect Bind

The Indirect Bind authentication method is much more dynamic and searches for the proper user domain settings rather than making assumptions about the format. With TrueCommand, Indirect Bind configures a “bind user” (typically a read-only, minimal-permissions user account) with a known domain/password to perform the initial bind to the LDAP server. Once logged in, TrueCommand searches for the user domain currently requesting to login. It then attempts a second bind with the user domain and provided password.

Example:

- Domain: “dc=mycorp,dc=com”
- User ID Field: “uid”
- BIND User Domain: “uid=binduser,cn=read-only-bind,dc=mycorp,dc=com”
- BIND Password: “pre-shared-key”

When “bobby.singer” attempts to login, TrueCommand will establish an SSL-secure connection to the LDAP server. TrueCommand will use the *BIND User Domain* and *BIND Password* settings to perform an initial bind using pre-known settings from your LDAP provider. Once bound, TrueCommand will search for the user matching “uid=bobby.singer”, but only within the subdomains that include the “domain” setting (“dc=mycorp,dc=com” in this example). If TrueCommand finds a user, it will use the full user domain string from the search result to initialize a second bind along with the user-provided password. If successful, TrueCommand verifies the user authentication and Bobby Singer is allowed access to TrueCommand.

SSL/TLS Connection Info

WARNING: AD/LDAP authentication *requires* SSL connections.

If the LDAP server uses an SSL certificate generated by a custom certificate authority (CA), then one of two things must occur before TrueCommand can use the LDAP server:

- (Option 1) Users must register the custom certificate authority with TrueCommand via the *Certificates* tab in *Administrator Settings*.
- (Option 2) Users can disable the *Verify SSL* option to accept whatever SSL certificate the server provides. Users may need to choose Option 2 if the LDAP server hostname is different than the one listed on the certificate, or if the server uses a self-signed SSL certificate.

Enabling *Allow LDAP user creation* means TrueCommand creates user accounts when someone logs in to the User Interface with their LDAP credentials. *JOIN TEAM* automatically adds LDAP users to specific TrueCommand teams.

Teams and Permissions

You can assign users to existing *Teams* by selecting a team from the drop-down to add the user to that team. You can assign users to multiple teams. TrueCommand applies team permissions to any user added to a team, but setting a specific permission for the user can override a related team permission. For more indepth information regarding teams, see the Teams Documentation.

To limit the access that non-administrative accounts have to the connected systems, configure the **System Access** and/or **System Groups** sections. This requires that system connections and/or system groups have already been configured in TrueCommand.

Click *ADD SYSTEM* and select a system from the drop-down to give the user access to that system. To restrict the user to only viewing details about the system, set the *read* permission. To remove a user's access to a particular system, click minus on the desired system.

When system groups are available, an *ADD GROUP* button appears. Click *ADD GROUP* and select a group from the drop-down to give the user access to all the systems in that group. To assign user's type of access to the group, choose *read* or *read/write* permissions. To remove a user's access to a particular system group, click - *(minus)* on the desired group.

3.4 - Connecting TrueNAS Systems

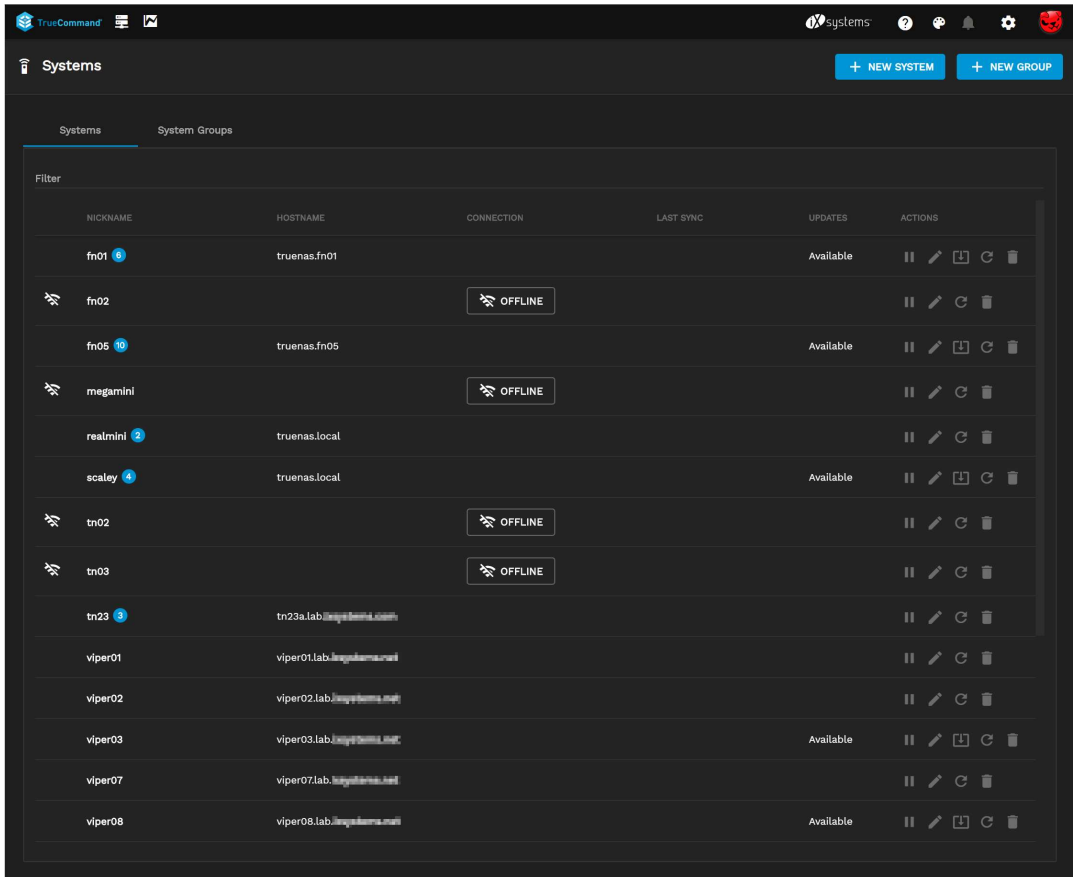
Connecting Systems to TrueCommand

To connect a system to TrueCommand, open the **Configure** ⚙ menu and click **Systems.** This menu is organized into two tabs: **Systems** and **System Groups.** The **Systems** and **System Groups** tabs contain all the options to connect and organize systems in TrueCommand. All added systems are listed in the **Systems** tab with the current connection status.

Adding a System Manually

To connect a new system, click **+ NEW SYSTEM.**

Enter the system IP address or DNS hostname, the nickname, and the password. If a mistake is made, the form can be reset by clicking **RESET FORM.**



Adjusting Systems

Systems that are misconfigured (e.g. if you entered an incorrect password) appear offline in both the TrueCommand **Dashboard** and **Systems** list.

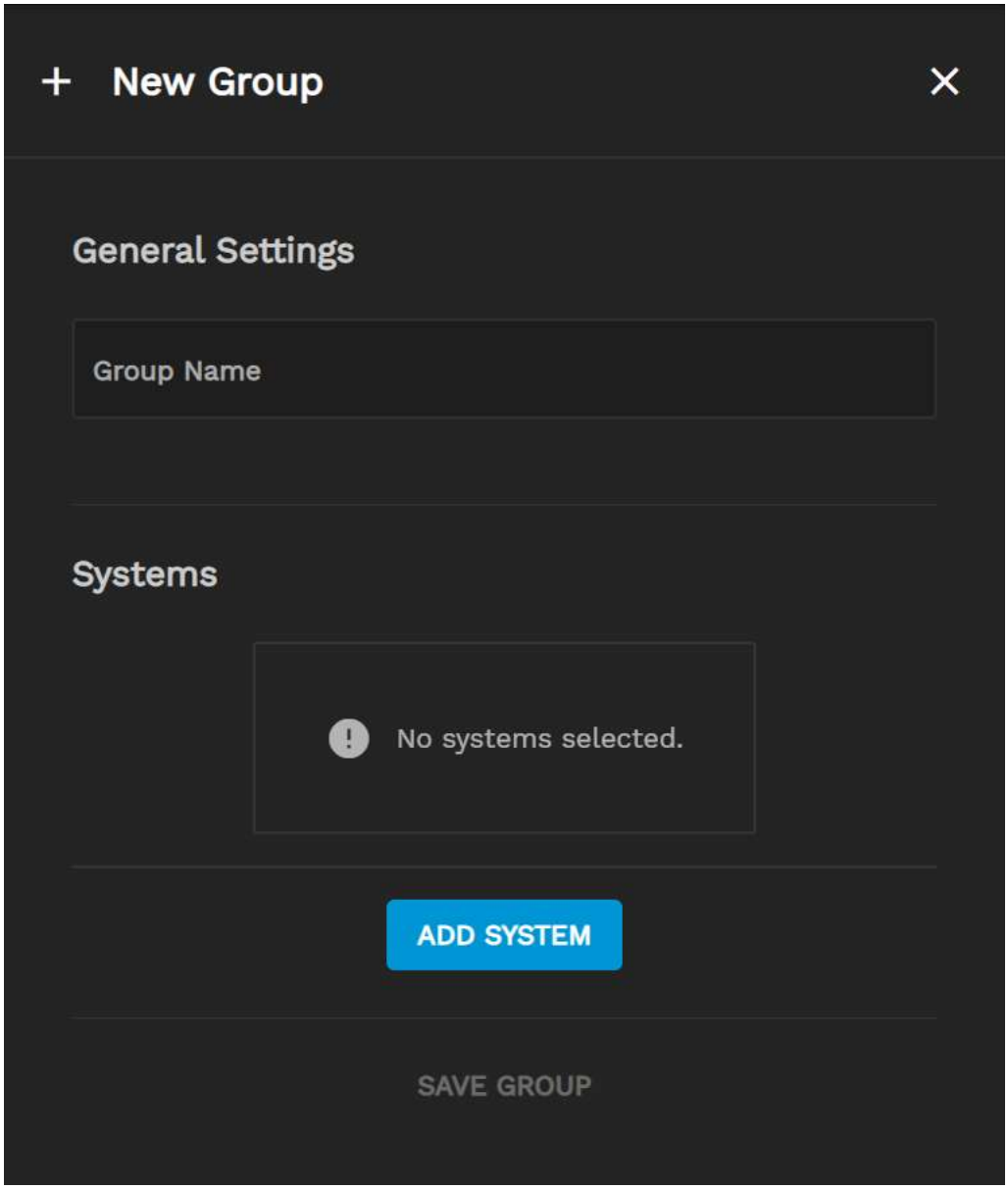
You can edit a system from the Systems list and enter new connection details. To go back to the original contents of the fields, click **RESET FORM.**

To remove a system from TrueCommand monitoring, click **Delete.**

Organizing Systems into Groups

Groups are collections of systems that are organized by TrueCommand administrators. Grouping systems allows efficient management of system permissions and reporting.

Open the **System Groups** tab to view the list of created groups and the systems they contain. Create a Group by clicking **Configure** **> Systems > + NEW GROUP.** Enter a name for the new group and click *ADD SYSTEM* to add a system to the group. When all the desired systems are added to the group, click *CREATE GROUP*.



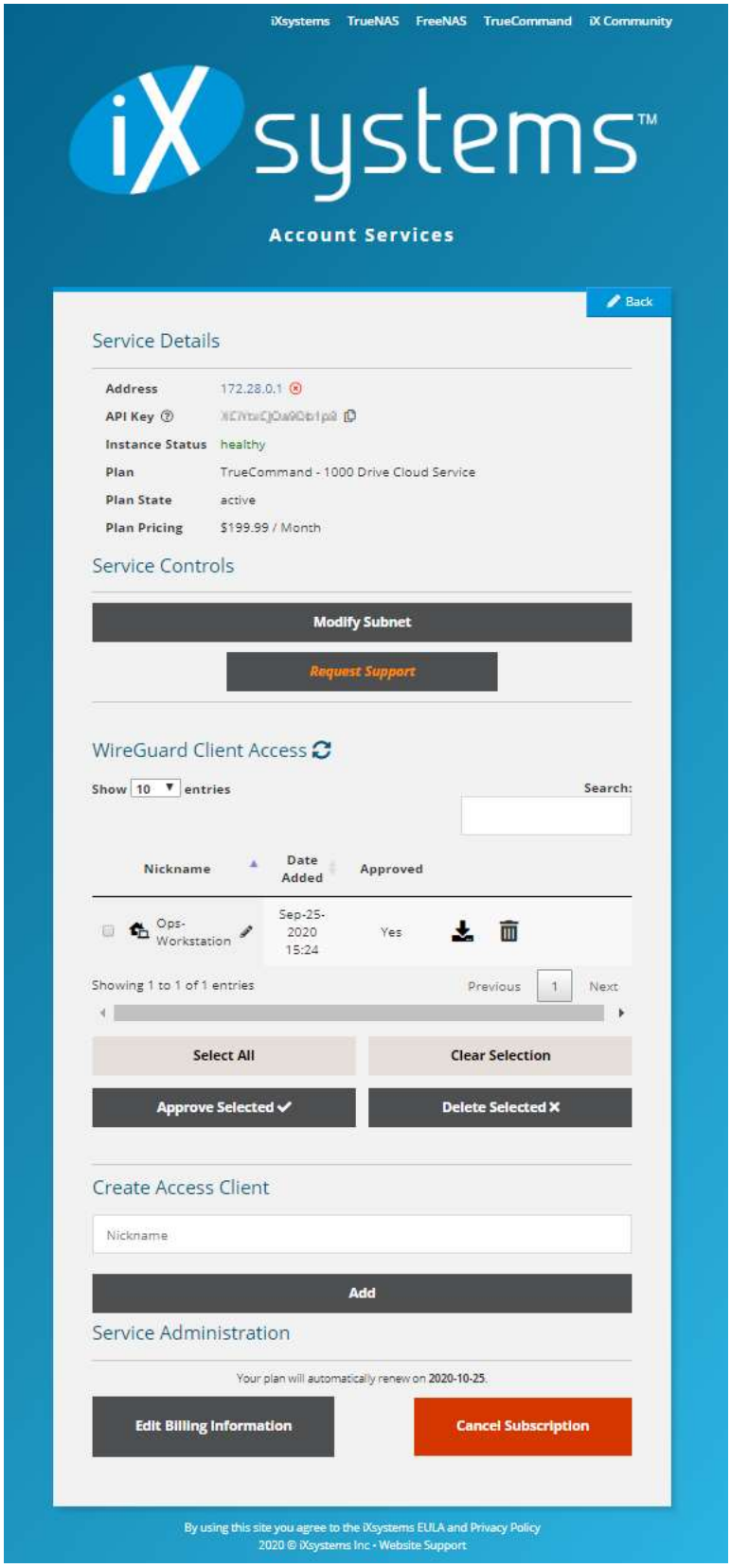
Editing a group allows you to update the group name or change which systems are members of that group.

To delete a system group, click *Delete* . Confirm the deletion by clicking *YES*.

Connecting Systems to a TrueCommand Cloud Instance

Get an API Key

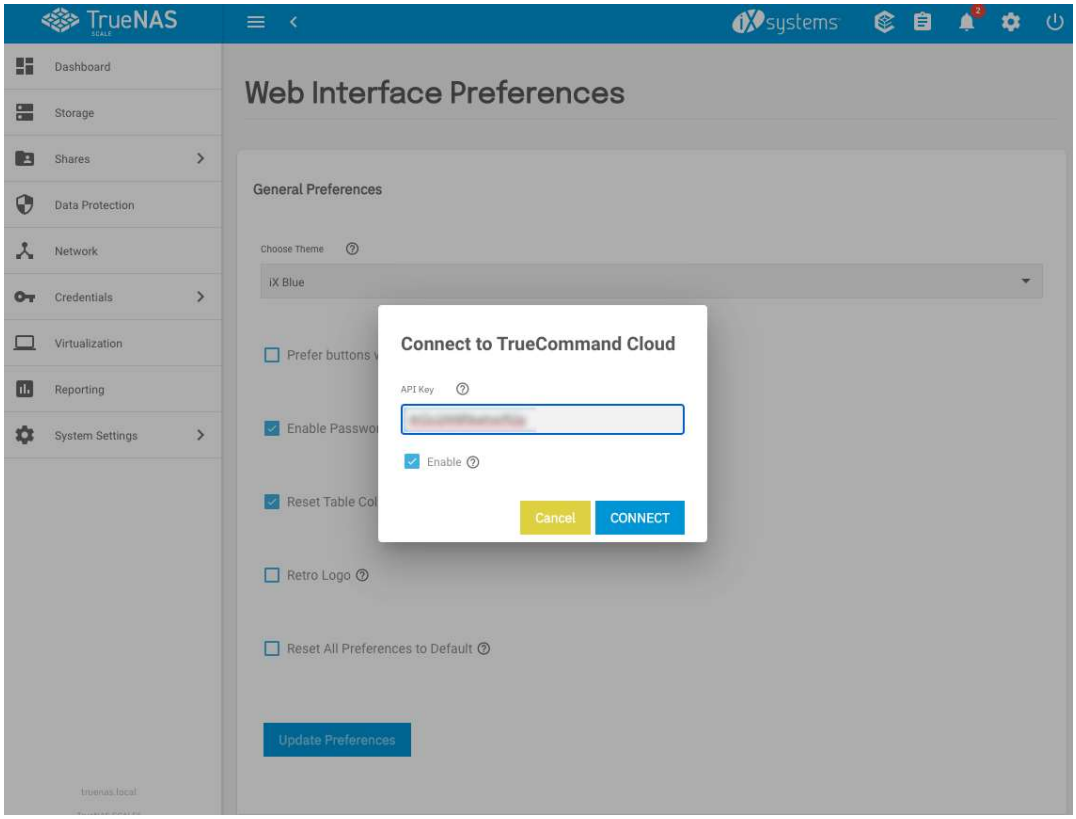
Log into the ixSystems cloud account and click *Manage*. Under **Service Details**, copy the *TrueCommand API Key*.



Connecting from the TrueNAS UI

Log into a TrueNAS system and click the TrueCommand icon in the upper right.

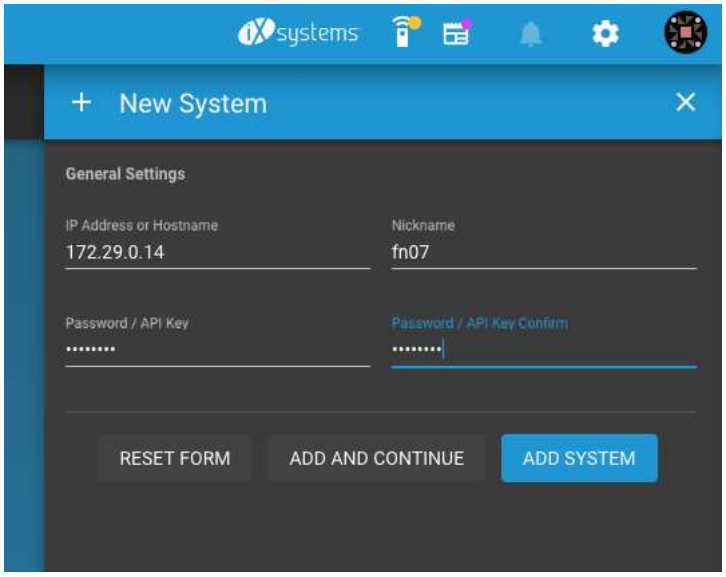
Paste the TrueCommand API Key copied from the iXsystems Account Portal into the TrueNAS dialog window.



Approve the Connection Request

When the True Command logo starts moving, check the TrueCommand Cloud email address for a verification message. The email contains a link to the Portal to confirm the connection and activate the TrueNAS system.

Click on the **New System** alert, fill in the information from the TrueNAS system, and click *Add System*.



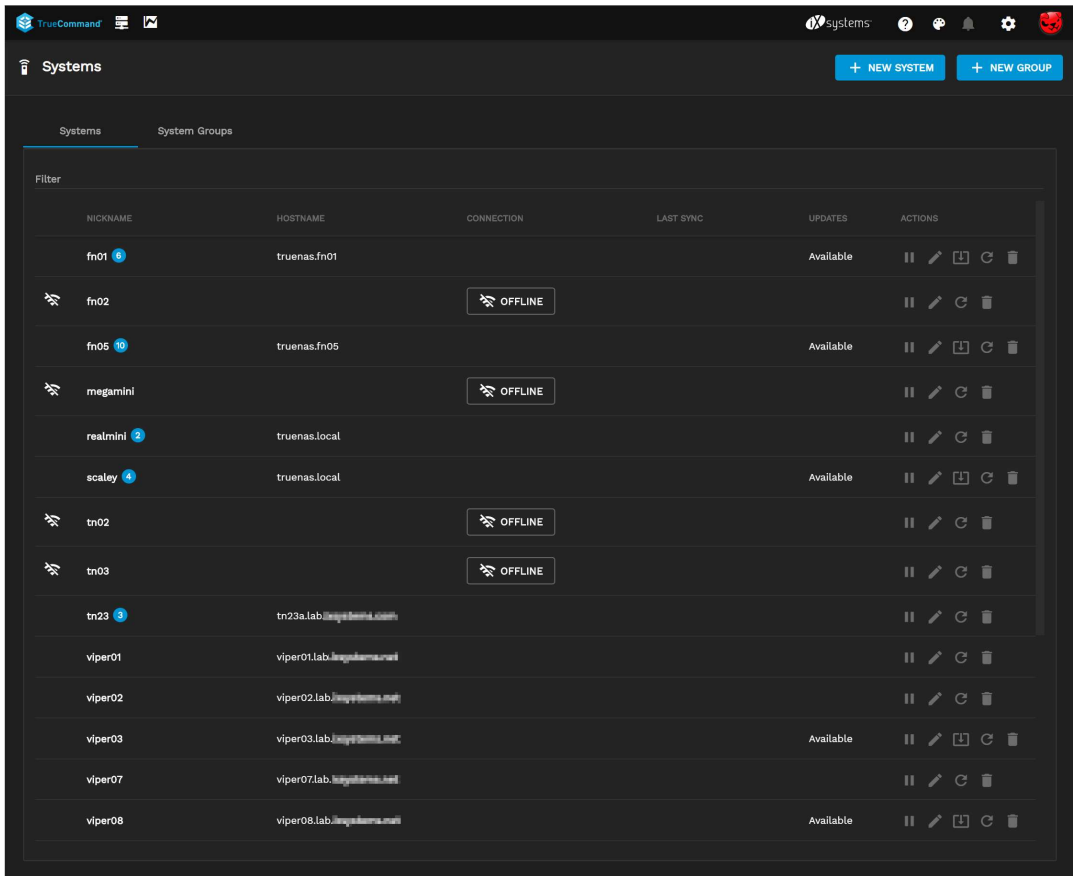
It can take 10 to 15 minutes for the TrueNAS instance to fully sync up with TrueCommand Cloud. When all systems are connected to TrueCommand Cloud, refer to the TrueCommand Administration articles for more instructions about setting up configuration backups, alerts, reports, and role-based access control.

Manual Connections

To connect a system to TrueCommand, open the **Configure** menu and click *Systems*. This menu is organized into two tabs: **Systems** and **System Groups**. These tabs contain all the options to connect and organize systems in TrueCommand. All added systems are listed in the **Systems** tab with the current connection status.

To connect a new system, click + *NEW SYSTEM*.

Enter the system IP address or DNS hostname, nickname, and password. If a mistake is made, the contents of the fields can be reset by clicking *RESET FORM*.



4 - Administration

Initial configuration and general administration articles.

TrueCommand includes an easy to use interface for administrative configurations.
Access to some of these areas may require a TrueCommand administrator account.

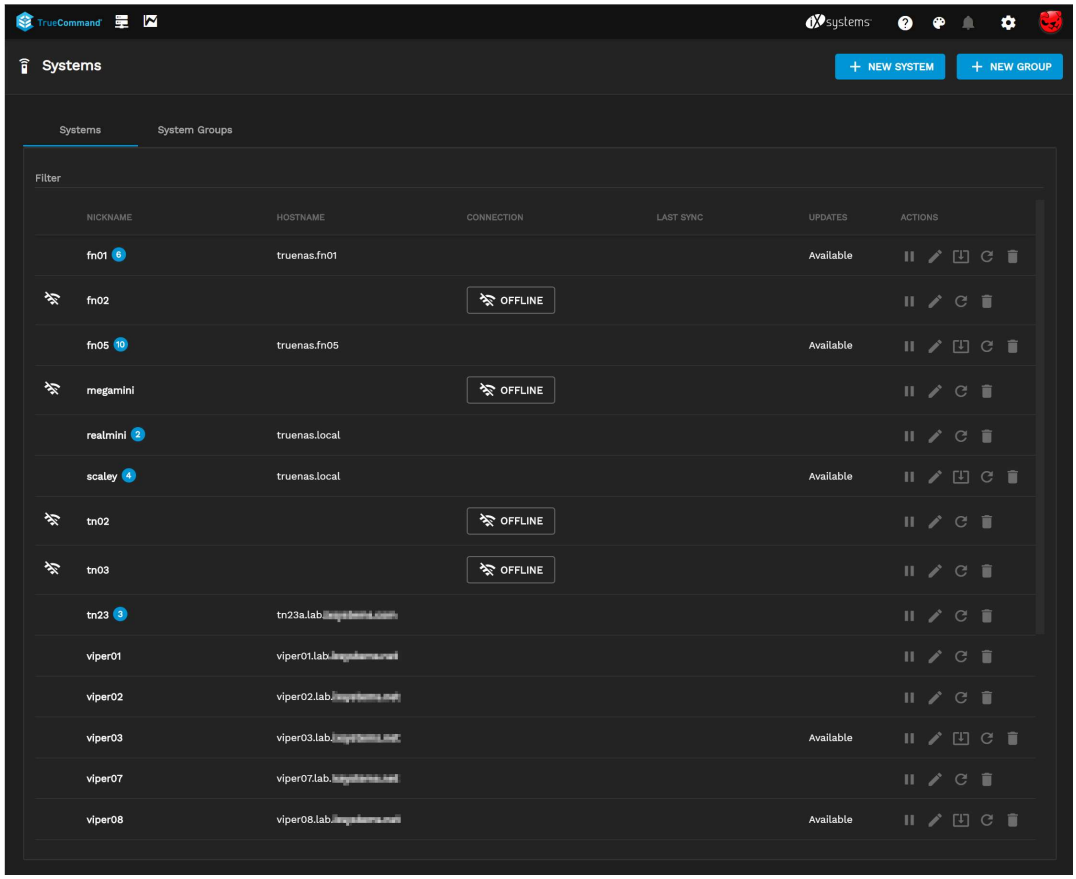
- NAS Fleet Administration
  - NAS Configuration
  - Creating NAS groups
  - Alerts for NAS systems
  - Reports of various metrics
- TrueCommand Instance Administration
  - TrueCommand Configuration Options
  - TrueCommand system Audit Logs
  - User and Team Management
  - UI Theme settings

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the **<** symbol to expand the menu to show the topics under this section.

4.1 - Systems

Connecting Systems to TrueCommand

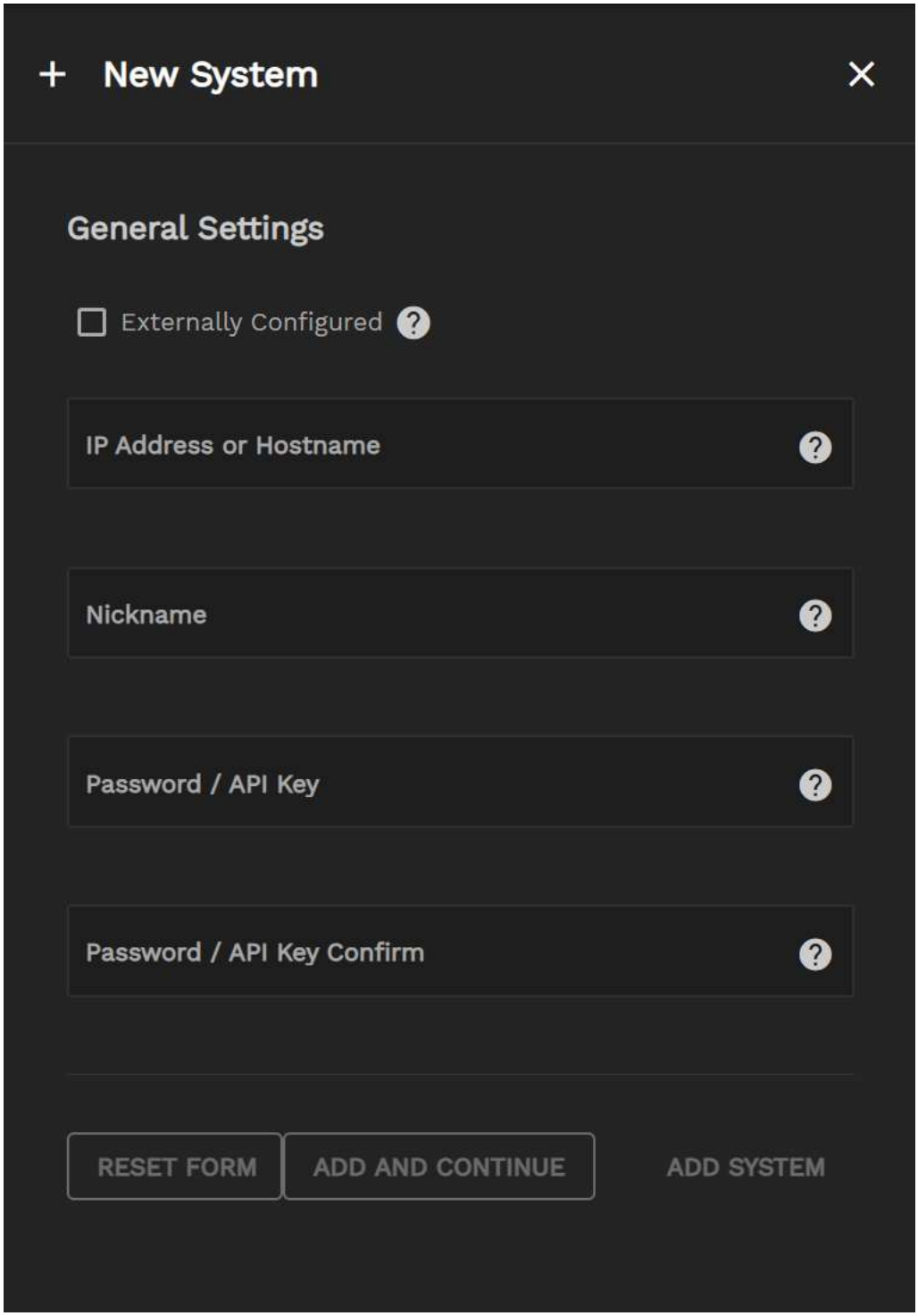
To connect a system to TrueCommand, open the **Configure** menu and click *Systems*. This menu is organized into two tabs: **Systems** and **System Groups**. The **Systems** and **System Groups** tabs contain all the options to connect and organize systems in TrueCommand. All added systems are listed in the **Systems** tab with the current connection status.



Adding a System Manually

To connect a new system, click **+ NEW SYSTEM**.

Enter the system IP address or DNS hostname, the nickname, and the password. If you make a mistake, you can reset the form by clicking *RESET FORM*.



Adjusting Systems

Each system has its own control area with what options are available.

- Pause Data Polling :
- Start Data Polling :
- Edit System :
- Update System :
- Reconnect System :
- Delete System :

Pause

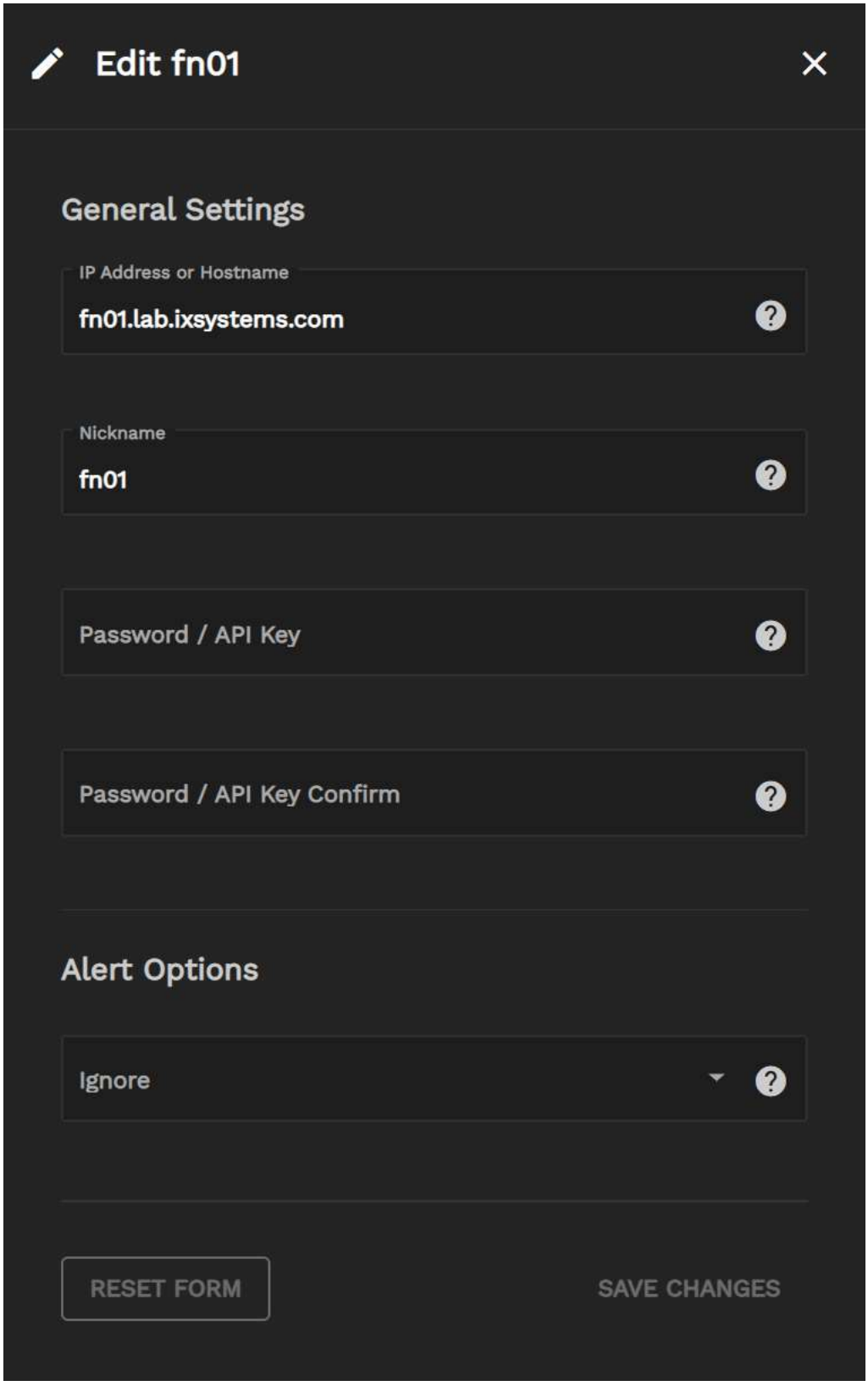
If the pause button is visible, TrueCommand is actively polling data from the NAS. Clicking this button will stop data collection until it is manually restarted.

Start

If the play button ▶ is visible, TrueCommand is not collecting any data from the NAS. To start data polling, click the play button.

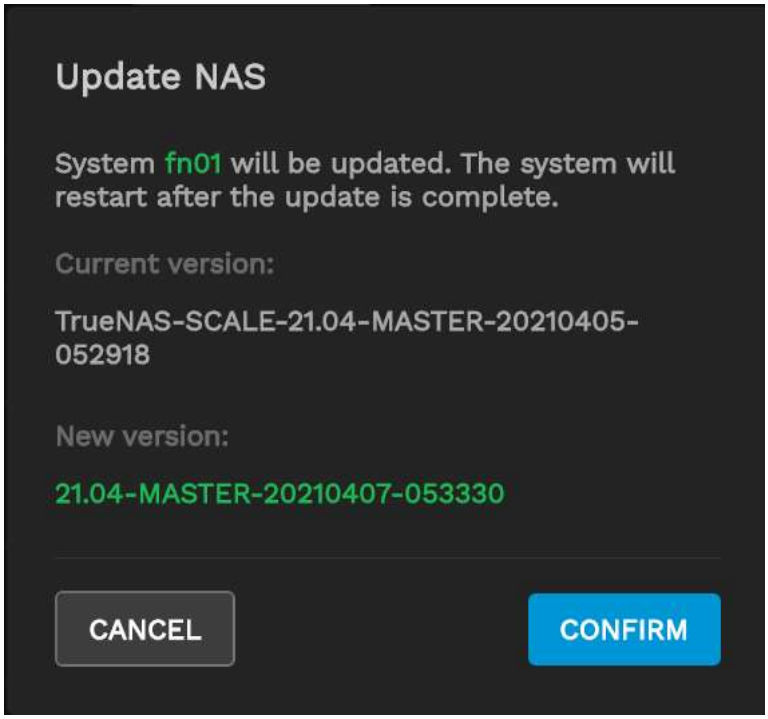
Edit

Clicking the edit button ✎ opens a side bar menu. Adjustments can be made to the system in this meny. Click **Save Changes** to update the system to the new values entered. Clicking **Reset Form** will reset the form to the previous saved settings for the NAS.



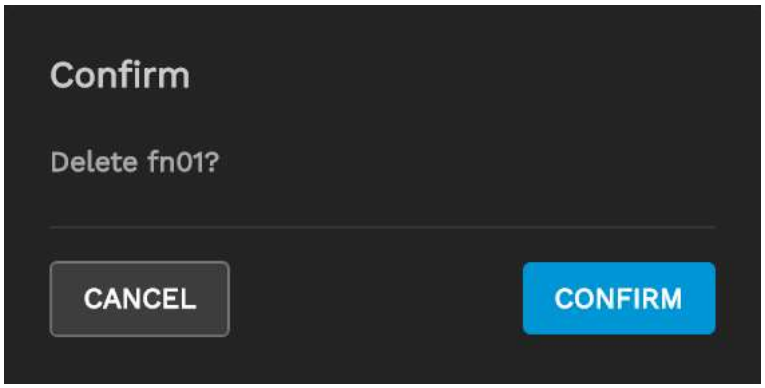
Update

If updates are available on the system, the Update column will say *Available* and the update button will be visible. Clicking the update button will open a popup window requiring you to confirm your desire to update the system.



Reconnect
If a system has lost its connection to TrueCommand either through maintainence or being powered off, click the reconnect button to trigger TrueCommand to reconnect with the NAS. Reconnecting may take several minutes. If data polling was paused before the system was disconnected, data polling will remain paused. Data polling must be manually restarted with the play button.
Delete

Clicking the button will initiate a popup confirmation box to delete a system.

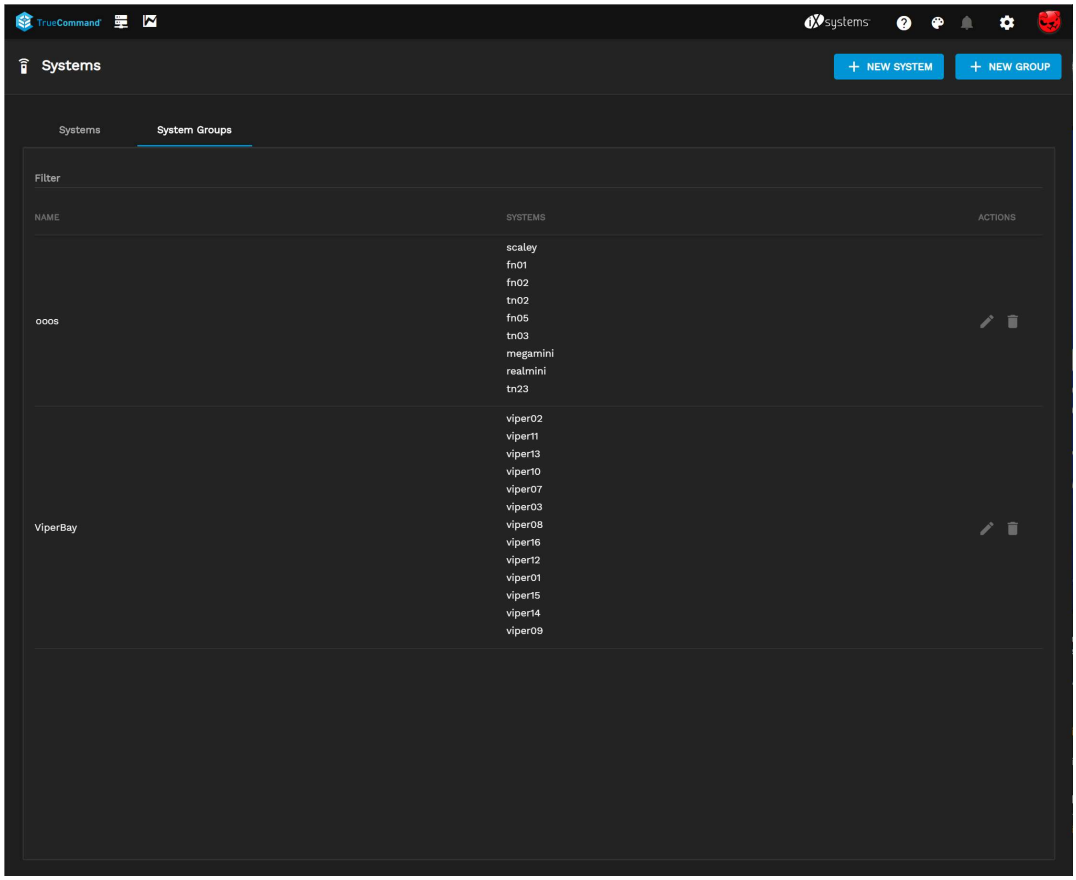


> Deleting a system will purge all collected data from the database.

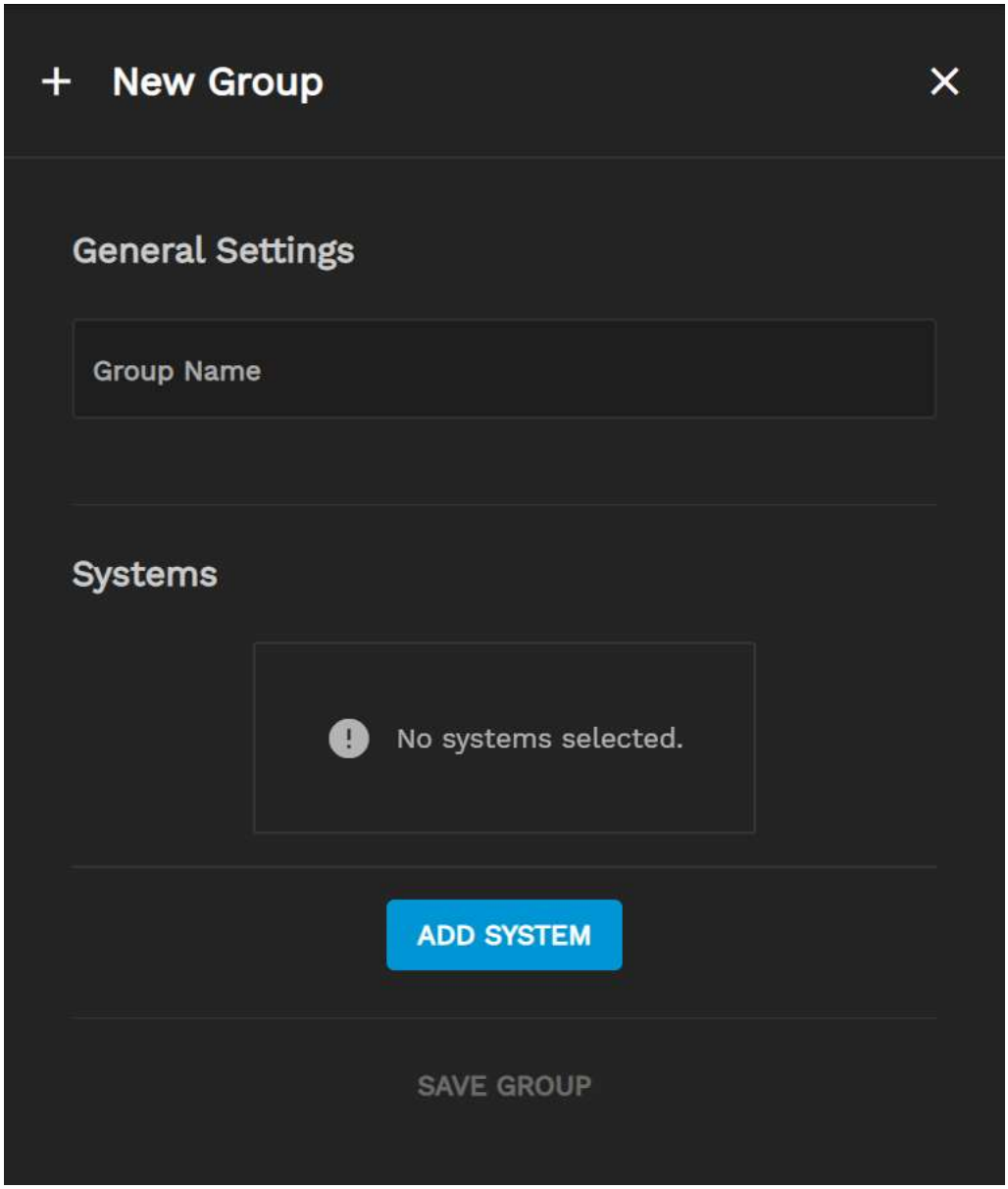
Organizing Systems into Groups

Groups are collections of systems that are organized by TrueCommand administrators. Grouping systems allows you to efficiently manage system permissions and reporting.

Open the **System Groups** tab to view the list of created groups and the systems they contain.



Create a Group by clicking **Configure** ⚙ **> Systems > + NEW GROUP.** Enter a name for the new group and click *ADD SYSTEM* to add a system to the group. When you've added all the desired systems to the group, click *CREATE GROUP*.



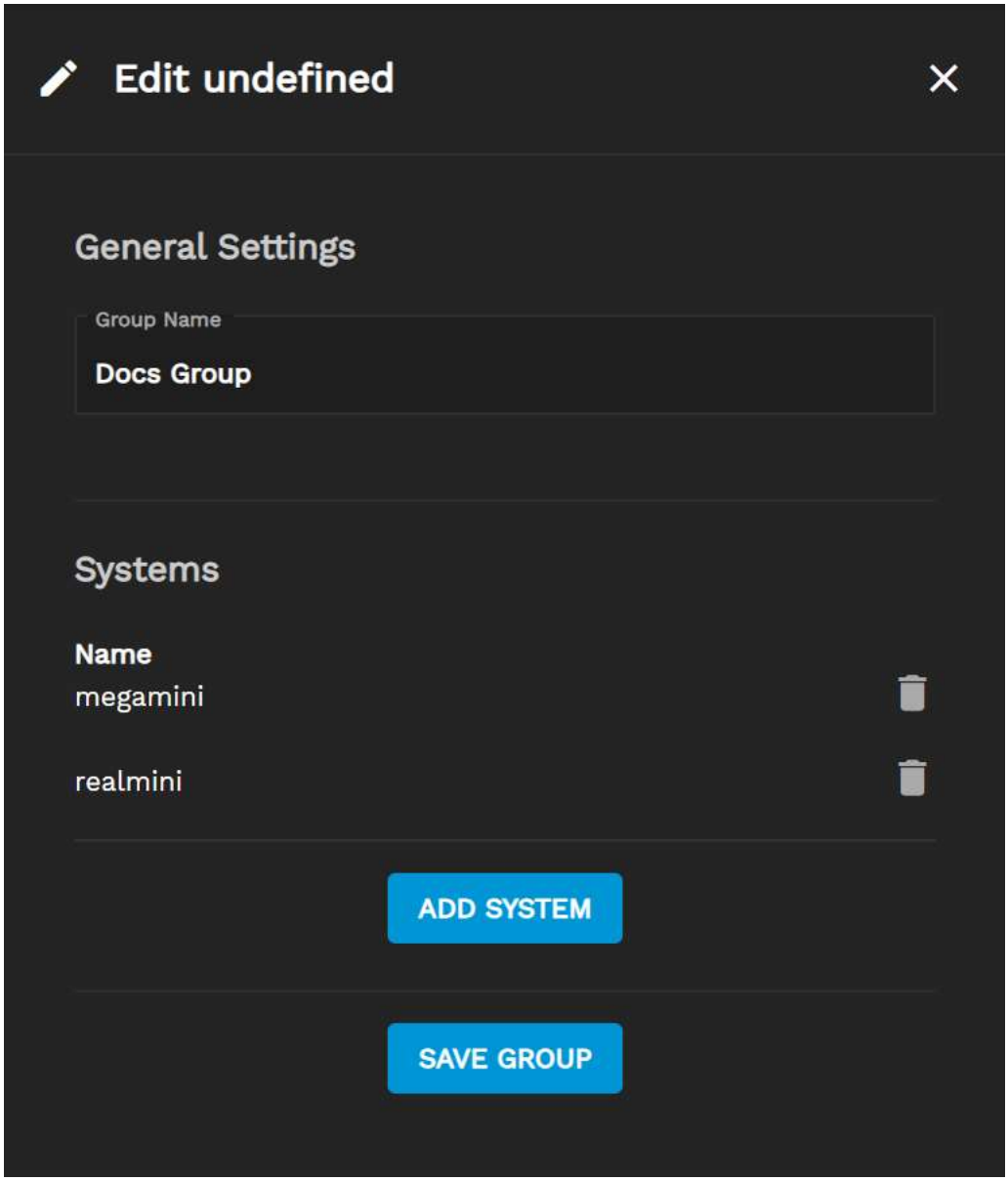
Adjusting Groups

Each group has its own control area with what options are available.

- Edit System :
- Delete System :

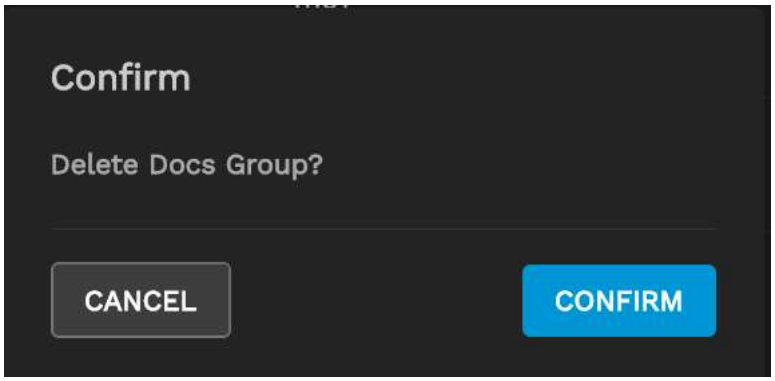
Edit

Clicking the edit button opens a side bar menu. Adjustments can be made to the Group in this manner. Systems can be added or removed from the group by using the **Add System** button or the Remove button. Click **Save Changes** when finished with your changes to update the Group to the new group settings.



Delete

Clicking the button will initiate a popup confirmation box to delete a group.



4.2 - Users

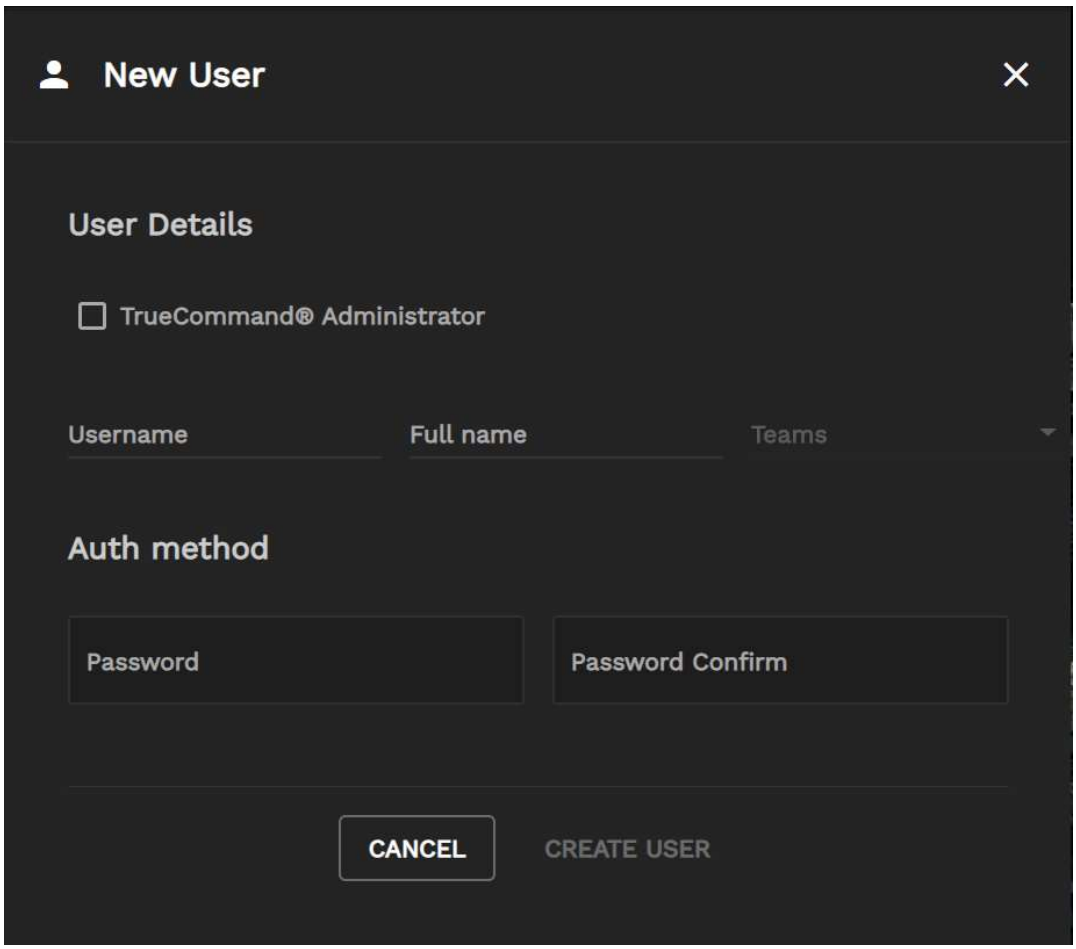
TrueCommand has a robust user management system designed to allow TrueCommand administrators to personalize the TrueCommand experience for each user account. You can create user accounts in the TrueCommand interface. Alternatively, LDAP can automatically create new user accounts when someone logs into TrueCommand with their LDAP credentials.

User accounts also organize into “Teams” for simultaneous management of large numbers or related user accounts.

Adding Local User Accounts

To create a new user account, open the **Configure** menu and click *Users* > + *NEW USER*. Enter a descriptive user name and an authentication method for the user.

TrueCommand uses the *DEFAULT* authentication method to create unique credentials for logging in to the web interface. The administrator has to provide these credentials to the intended user.



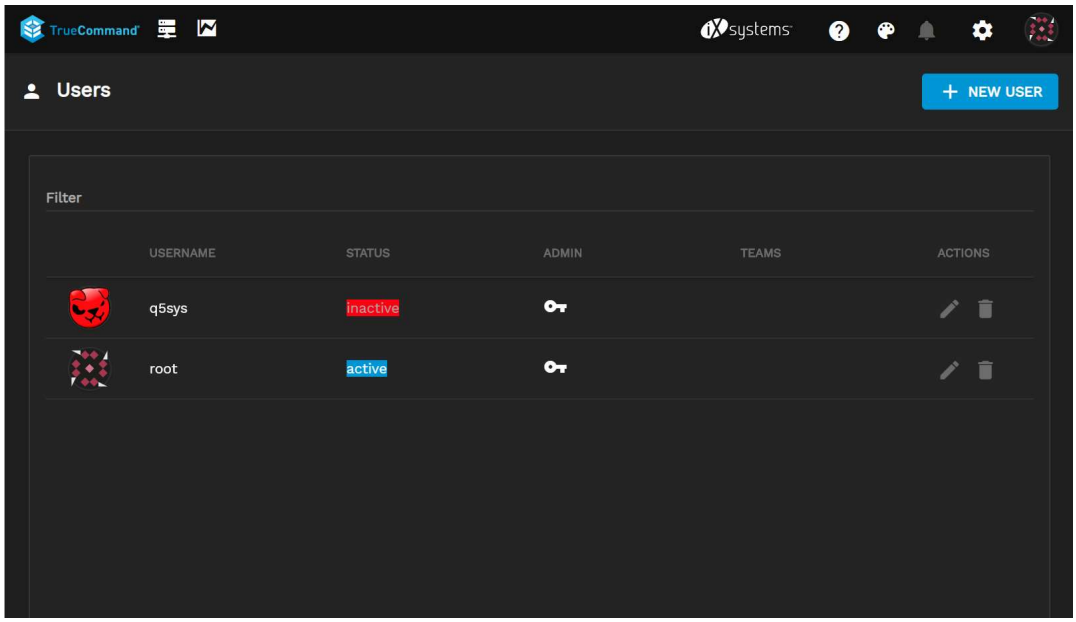
You can assign users to existing *Teams* by selecting a team from the drop-down to add the user to that team. You can assign users to multiple teams.

If the user needs to be an Administrator, check the *TrueCommand Administrator* box.

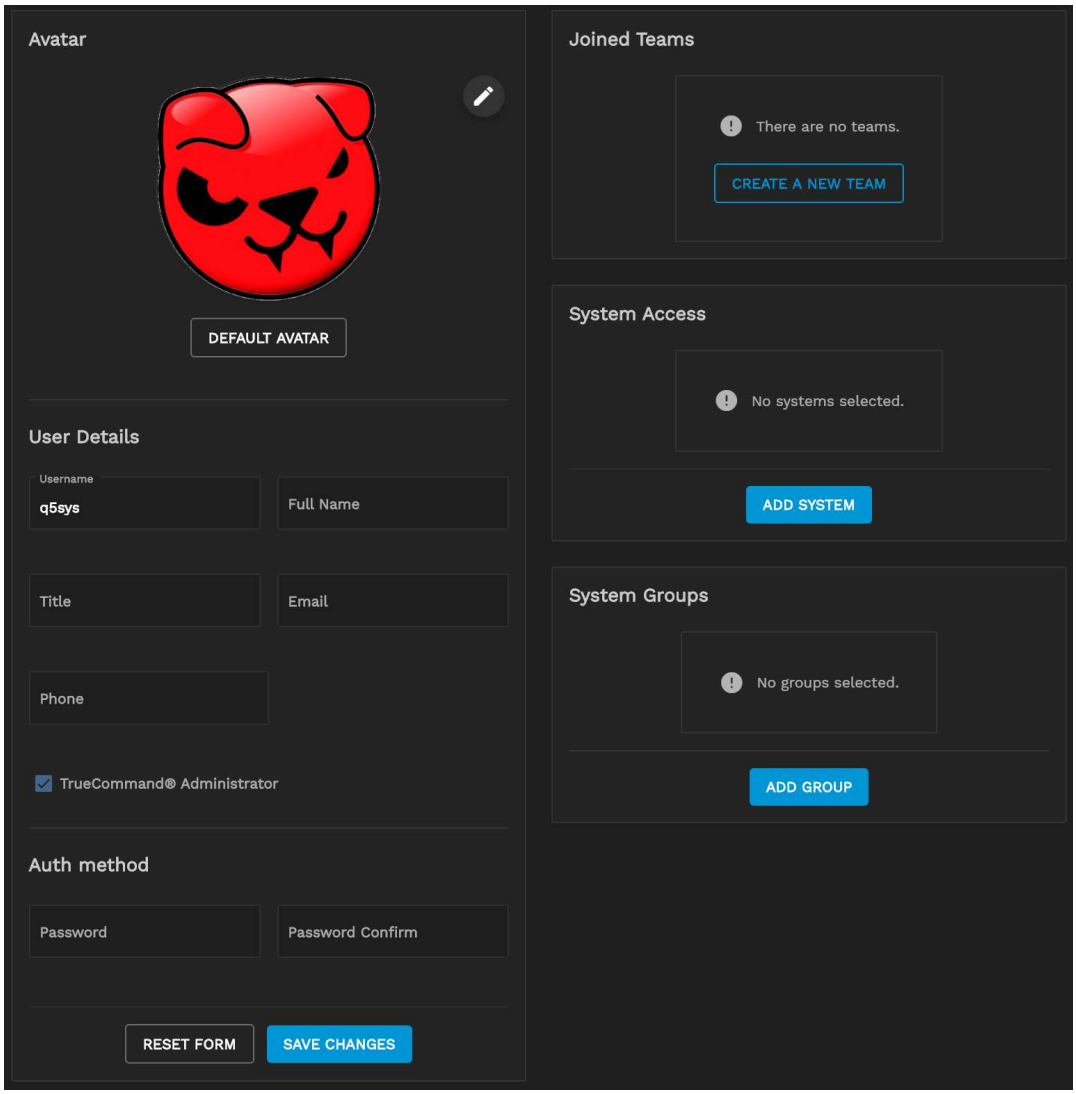
When the form is completed, click **Create User**.

Configuring User Accounts

To configure account details and permissions, open the *Configure* menu and click **Users**.



To edit a user click the Edit button .



There are several different elements that you can configure for a user, including the user's avatar, personal details, Team membership, and System permissions.

User Details

You can add personal details about the user in this form. You may also designate the account as TrueCommand administrator or change the account password. Saving changes to a user's password requires entering the current password for that user. To go back to the original contents of the fields, click RESET FORM.

Joined Teams

The **CREATE A NEW TEAM** button appears if no TrueCommand teams exist. When teams are present, the **JOIN TEAM** button appears. Click **JOIN TEAM** to add the user to a team. You can add users to multiple teams. TrueCommand applies team permissions to any user added to a team, but setting a specific permission for the user can override a related team permission. Team Configuration can be accomplished in the Team Page.

System Permissions

To limit the access that non-administrative accounts have to the connected systems, configure the **System Access** and/or **System Groups** sections. This requires system connections and/or system groups have already been configured in TrueCommand.

Click **ADD SYSTEM** and select a system from the drop-down to give the user access to that system. To restrict the user to only viewing details about the system, set the *read* permission. To remove a user's access to a particular system, click minus on the desired system.

When system groups are available, an *ADD GROUP* button appears. Click **ADD GROUP** and select a group from the drop-down to give the user access to all the systems in that group. To assign user's type of access to the group, choose *read* or *read/write* permissions. To remove a user's access to a particular system group, click - *(minus)* on the desired group.

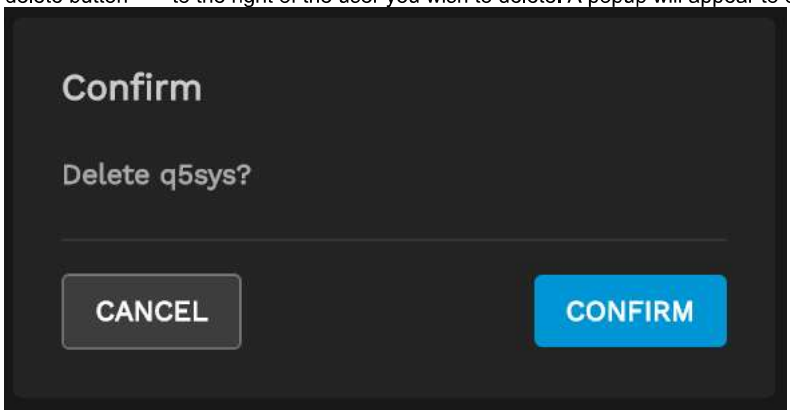
Resetting a User Password from the Command Line

The Docker version of TrueCommand allows you to reset user passwords from the command line. Open the shell on the system running the TrueCommand Container and use the following command, replacing the values in brackets with their appropriate values.

```
docker exec -it [docker instance ID] resetpw [username]
```

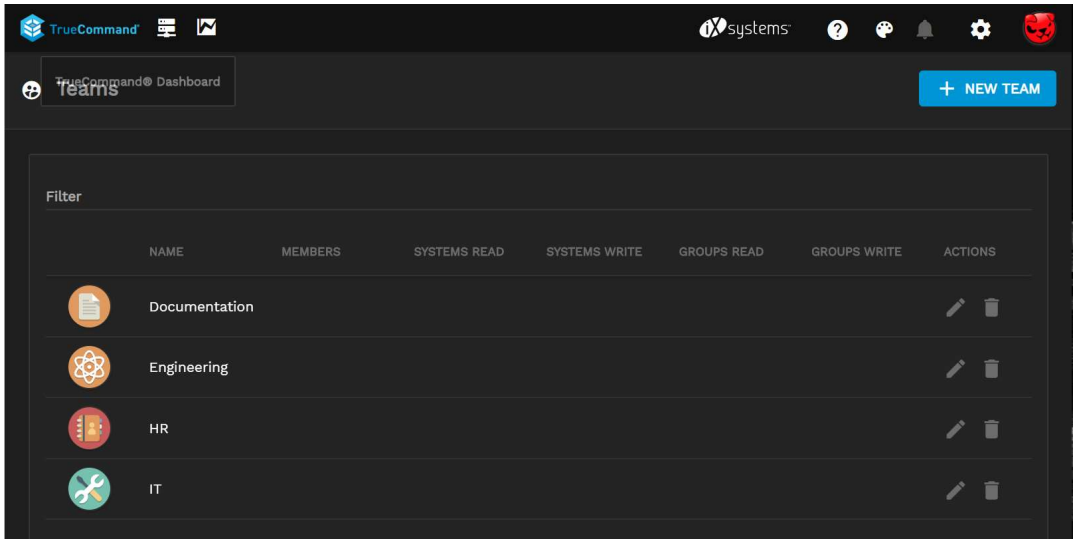
Deleting User Accounts

To delete an account details and permissions, open the *Configure* menu and click **Users**. When the users page loads, click the delete button to the right of the user you wish to delete. A popup will appear to confirm deletion of the user.

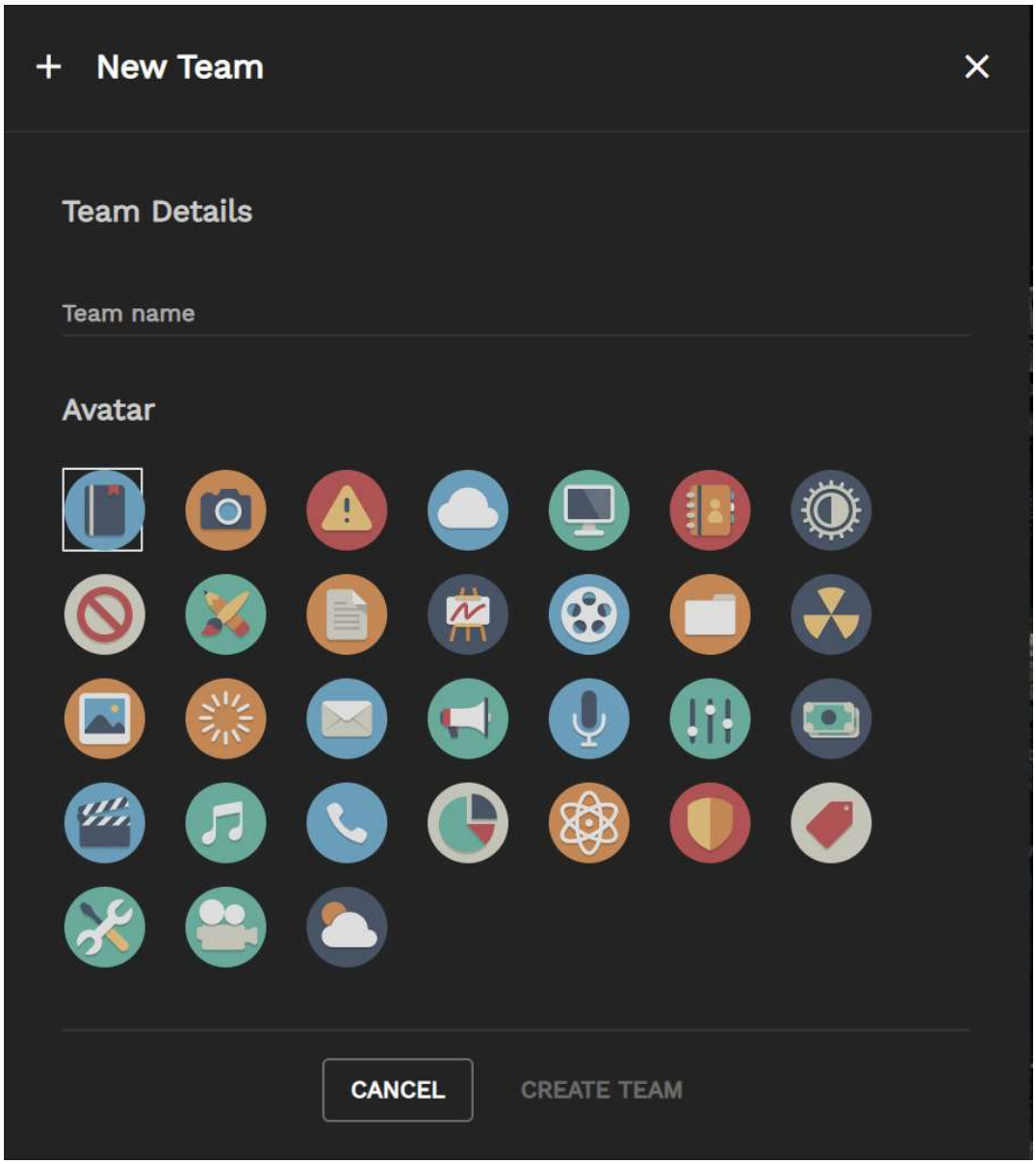


Organizing Users into Teams

To create a team, open the **Configure** menu and click **TEAMS**.



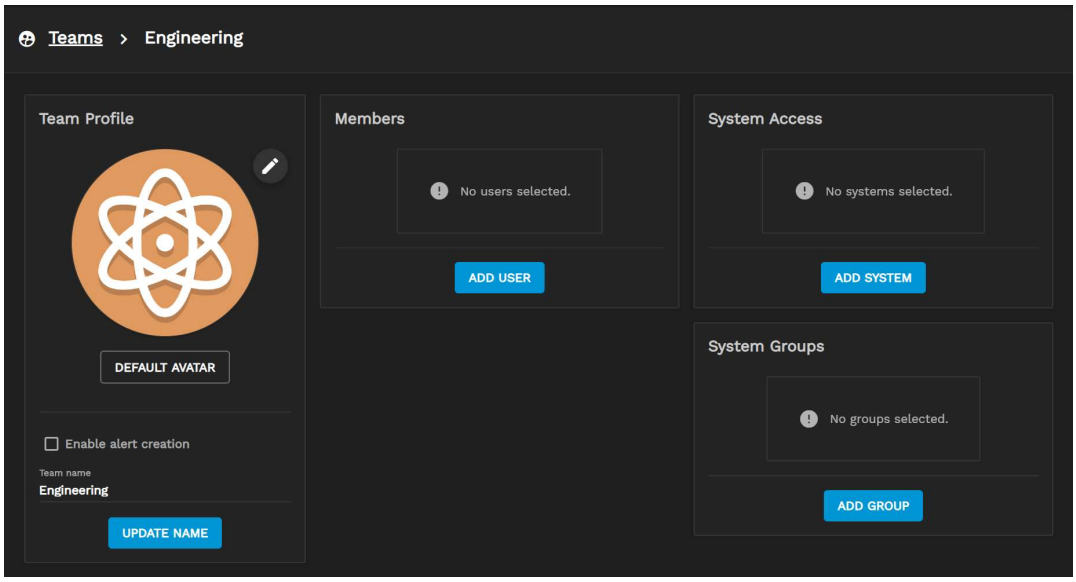
Clicking **NEW TEAM** will open a popout menu.



Enter a name and select an avatar for the new team. You can edit the permissions for a team after creating it.

Configuring Teams

To configure a team, open the **Configure** menu and click **TEAMS**. To adjust the team members or permissions, click the Edit button .



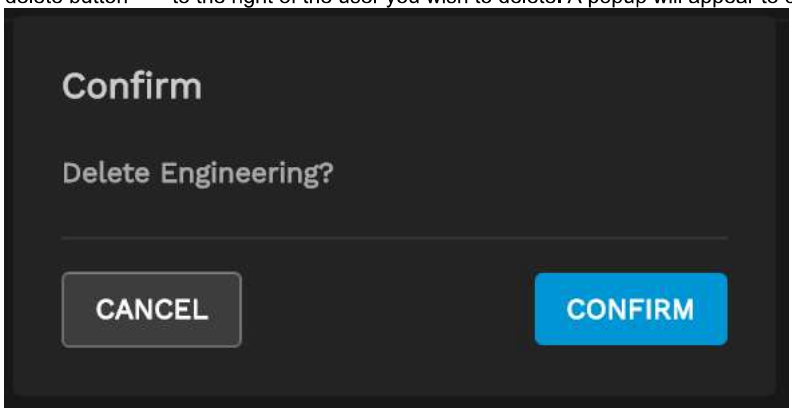
You can adjust the team profile with a new avatar, change the team name, or grant team members permission to create new TrueCommand Alert Rules.

The **Members** section shows which user accounts are included in the team. To add users to the team, click *ADD USER* and choose them from the drop-down. To remove users from the team, click - *(minus)* on the desired user.

System permissions are configured exactly the same way as described above for individual user accounts. Note that individual user account permissions can override team permissions.

Deleting Teams

To delete an account details and permissions, open the *Configure* menu and click **Teams**. When the users page loads, click the delete button to the right of the user you wish to delete. A popup will appear to confirm deletion of the Team.

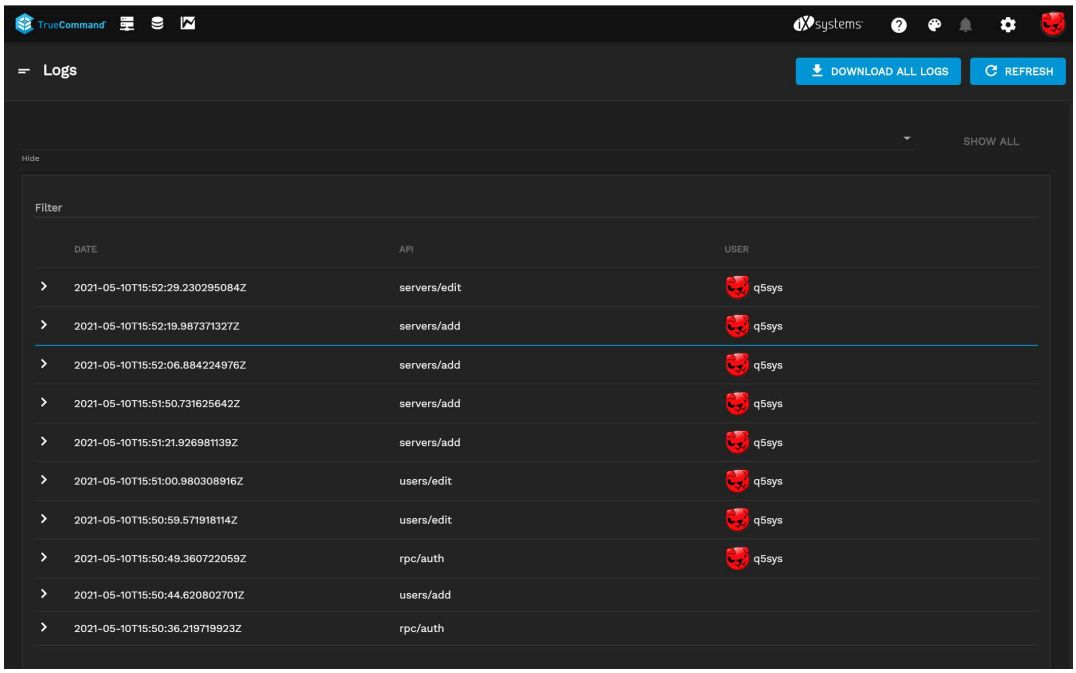


> Deleting a team does not remove users or systems assigned to that team.

4.3 - System Log

TrueCommand records all user account activity in a system log. For example, if a user deletes a system from TrueCommand, the log records which user deleted it along with other information associated with the deleted system.

To view the system log, open the **Configure** menu and click *Logs*.



TrueCommand shows all system log entries by default. To hide specific categories of log entry, make selections in the *Hide* drop down. You can display all system logs again by clicking *SHOW ALL*. You can also filter logs can also by entering strings in the *Filter* field.

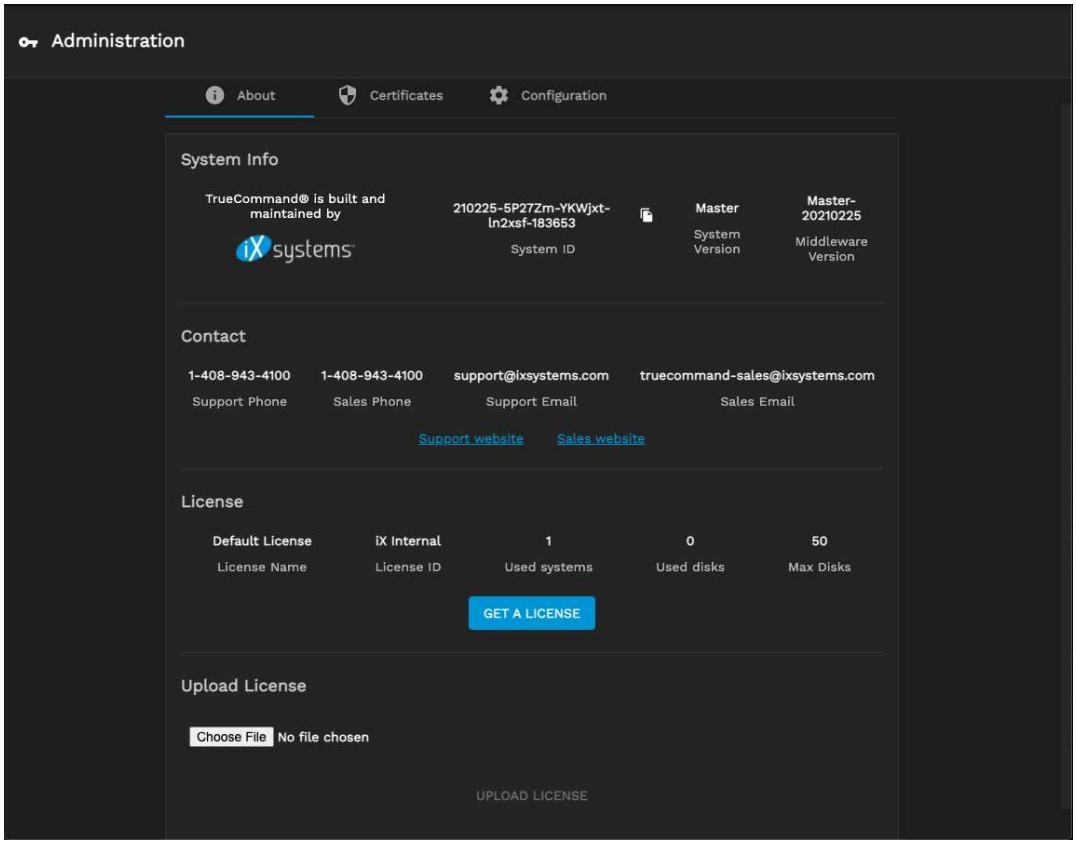
Click an entry in the log to show detailed information about the event. Clicking *DOWNLOAD ALL LOGS* downloads a .json file that contains all system log entries.

4.4 - Settings

The **Administration** page shows additional system details and offers a variety of TrueCommand configuration options. This page is available to users with administrator permissions by opening the **Configure** menu and clicking *Administration*. The page is organized into **About**, **Certificates**, and **Configuration** tabs.

About

The **About** tab contains the current TrueCommand system ID and version, license details, and contact information for iXsystems.



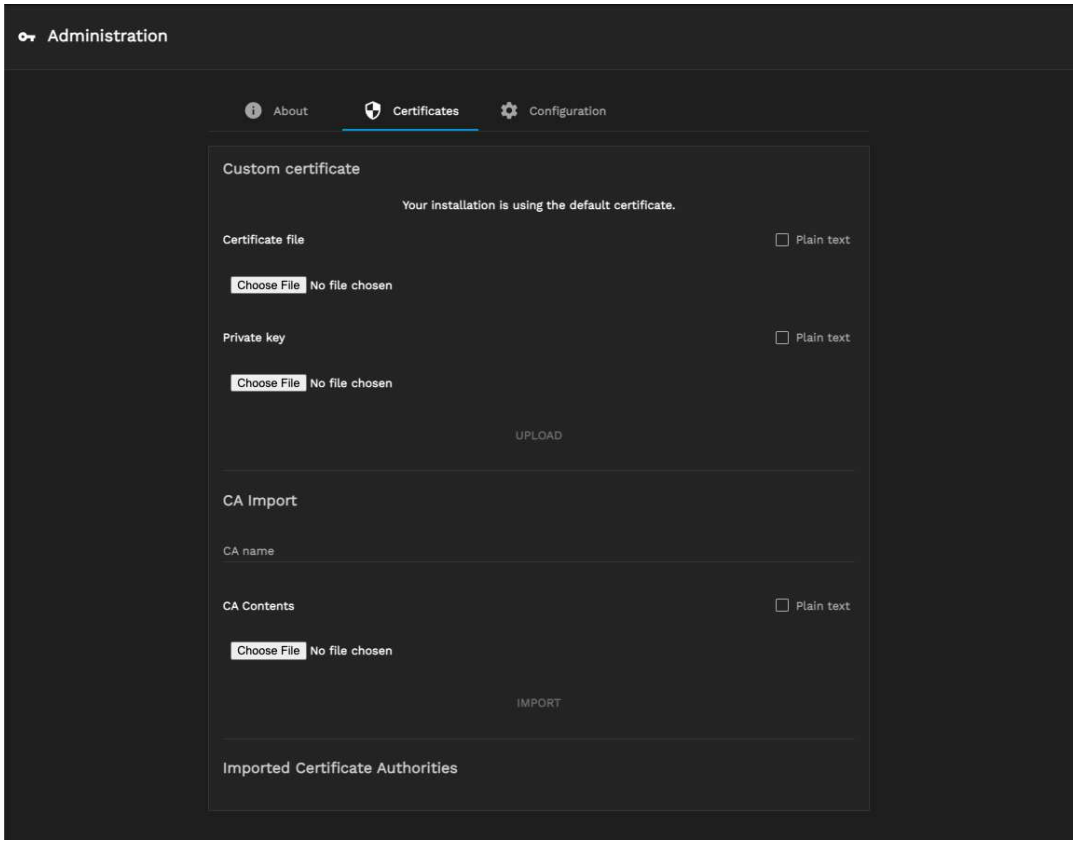
Updating the License

You can expand TrueCommand to monitor more disks by upgrading or purchasing a license from iXsystems. Clicking *GET A LICENSE* opens a new browser tab to purchase a TrueCommand license. You can also contact iXsystems to upgrade the current license.

After you purchase or upgrade the license, you must upload the new license to TrueCommand. Click *Browse…* to open a file browser on your local system. Select the new license file to upload and click *UPLOAD LICENSE* to apply the new license to TrueCommand.

Certificates

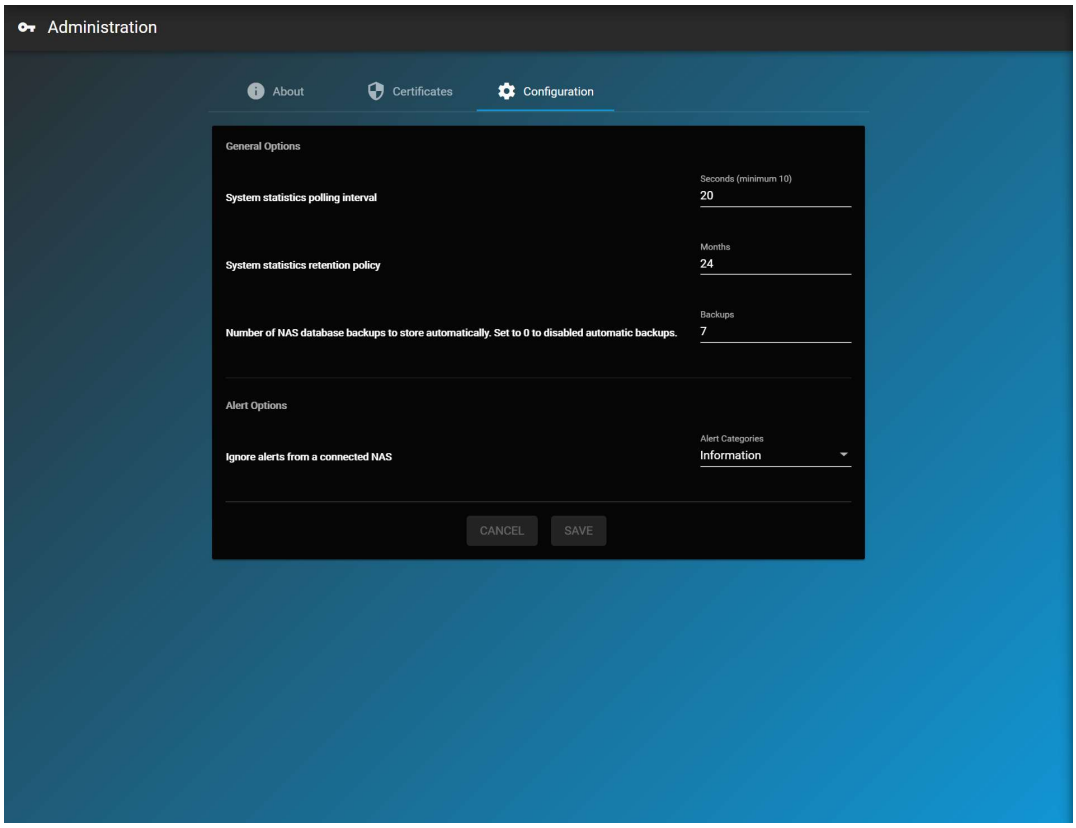
The **Certificates** tab shows the certificates and Certificate Authorities (CAs) TrueCommand uses and has options to upload or import a certificate or CA.



Clicking *Browse…* opens a dialog to upload a file from the local system. Selecting *Plain text* allows you to copy and paste the file raw text instead of uploading a file.

Configuration

The Configuration tab contains options to configure various features of TrueCommand.



Changing any options requires clicking *SAVE* to save the new system configuration. To reset fields back to their previous values, click *CANCEL*.

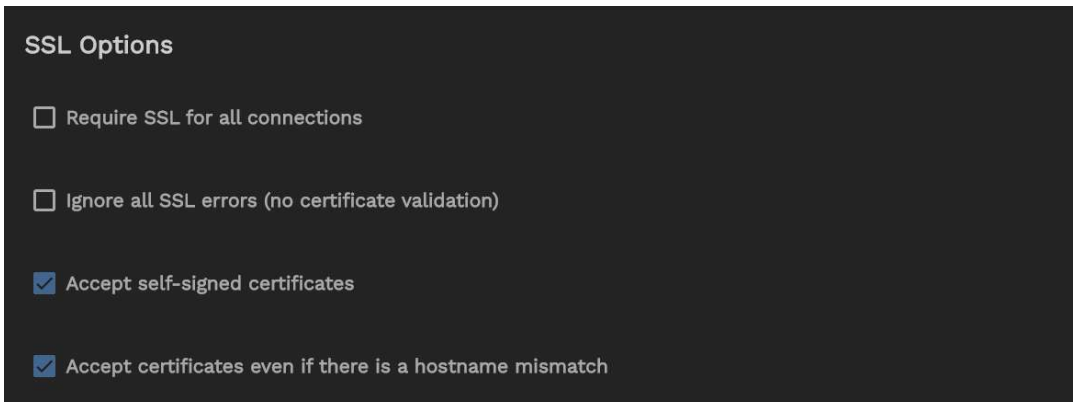
General options include how frequently TrueCommand measures systems statistics, how long to store system statistics, and the number of database backups from an iXsystems NAS to store.

SSL options

> This feature is only available for local installations or containerized TrueCommand deployments.

By default, TrueCommand attempts an SSL connection, then a non-SSL connection if the first attempt fails. You can disable non-SSL connection attempts by setting *Require SSL for all connections*. This is useful when a monitored system does not allow SSL-secured access or when the monitored system is using a custom port.

There are additional options to configure how TrueCommand handles certificates. By default, TrueCommand accepts self-signed certificates and certificate hostname mismatches. This allows the first-time login to TrueCommand and accepting certificates from systems that use a hostname, but are registered in TrueCommand with an IP address (or vice-versa).



Alert Options

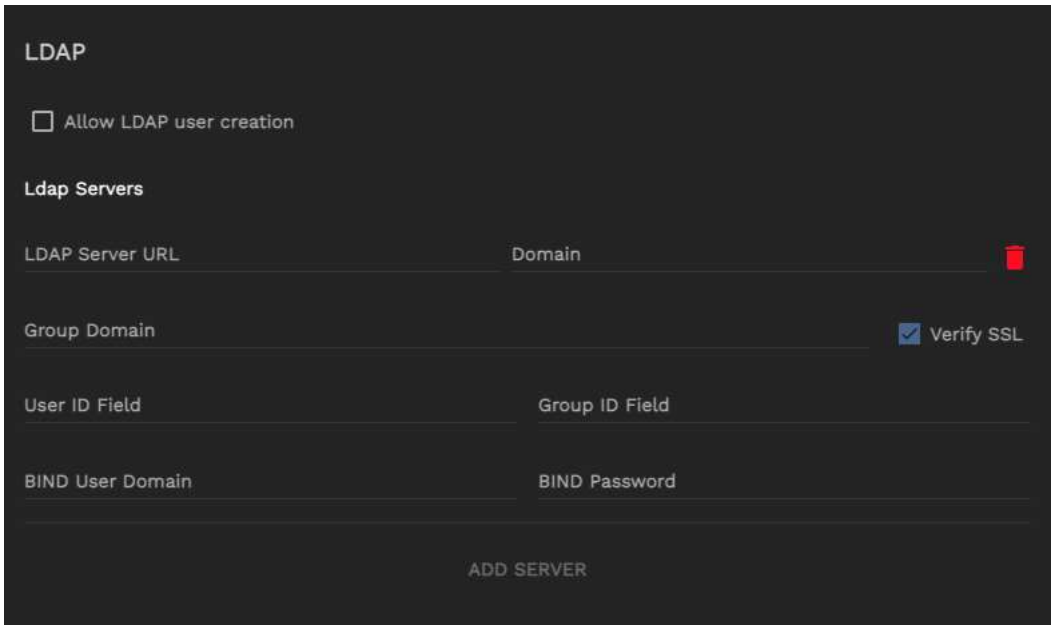
You can adjust the alert levels that TrueCommand shows from a connected NAS to tune the system messages shown according to your use case. Choose an alert category to ignore. Multiple categories can be selected.

LDAP

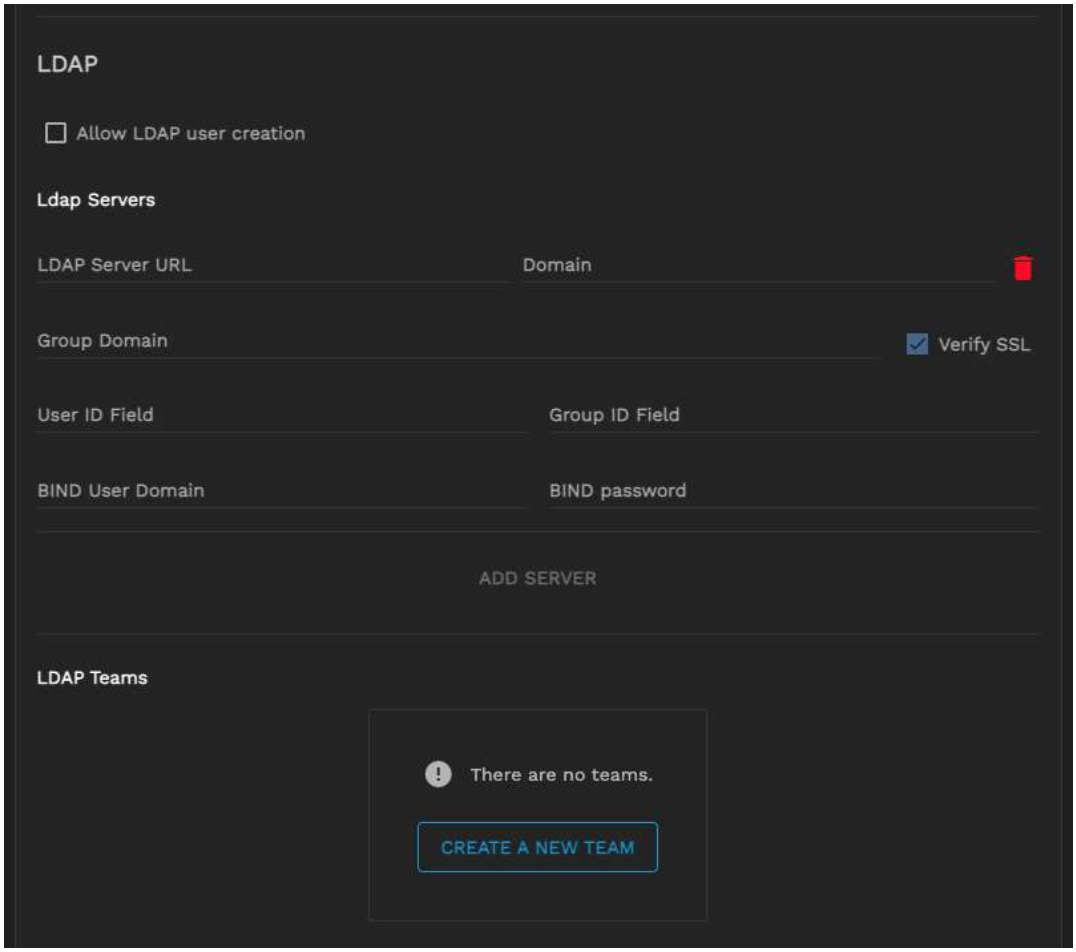
TrueCommand supports using LDAP to better integrate within an established network environment. *LDAP/AD* allows using single sign-on credentials from the Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). This means a user can log in with an LDAP or AD account without creating a separate TrueCommand login.

The LDAP server IP address or DNS hostname and Domain are required to use LDAP/AD. The LDAP or AD Username (optional) is required when the TrueCommand user name does not match the LDAP or AD credentials.

Click on the **(Gear) > Administration**.
Open the *Configuration* Tab to access the LDAP configuration section.



To configure LDAP, add an LDAP server IP address or DNS hostname, fill in the *Domain*, and click *ADD SERVER*. Multiple LDAP servers and Domains can be added.



Field	Value
LDAP Server URL (string, Required)	IP or DNS name of the LDAP server, with port number on the end. Example: “ldap.mycorp.com:636” (SSL port is typically 636 for AD/LDAP)
Domain (string, Required)	Base domain settings of the user. Example: “dc=mycorp,dc=com” for a typical username@mycorp.com user account
Group Domain (string)	The alternative domain setting to use when searching for groups. The Default value is the same as *Domain*
Verify SSL (bool)	Require strict SSL certificate verification. The default value is false. Disable this option if the hostname of the system is different than the one listed on the SSL certificate, an IP is used for the connection instead of the DNS hostname, or if a self-signed certificate is used by the LDAP server.
User ID Field (string)	Domain fieldname to use for user-matching. The default value is “uid” (user ID). Another field commonly-used is “cn” (common name)
Group ID Field (string)	The domain fieldname to use when searching for a group name. The default value is “cn” (common name).
BIND User Domain (string)	The full domain setting for a pre-authenticated bind to the server. Example: “uid=binduser,cn=read-only-bind,dc=mycorp,dc=com” For an unauthenticated bind set this field to just a name (example: “truecommand-bind”). This is sometimes used for logging purposes on the LDAP, but otherwise is not validated.
Bind Password (string)	The password to use for the bind user. For an unauthenticated bind, leave this field blank while setting the *BIND User Domain* to a non-empty value.

LDAP connection options

TrueCommand supports two common methods of validating LDAP user credentials:

Direct Bind

The Direct Bind method uses the *Domain* and *User ID Field* to create a static domain string which is then used to authenticate the user.

Example:

- Domain: “dc=mycorp,dc=com”
- User ID Field: “uid”

When user “bobby.singer” attempts to login, TrueCommand will establish an SSL-secure connection to the LDAP server and then attempt to bind with the static domain “uid=bobby.singer,dc=mycorp,dc=com” and the user-provided password. If successful, then the user authentication has been verified and Bobby Singer is allowed access to TrueCommand.

Indirect Bind

The Indirect Bind authentication method is much more dynamic and searches for the proper user domain settings rather than making assumptions about the format. With TrueCommand, Indirect Bind configures a “bind user” (typically a read-only, minimal-permissions user account) with a known domain/password to perform the initial bind to the LDAP server. Once logged in, TrueCommand searches for the user domain currently requesting to login. It then attempts a second bind with the user domain and provided password.

Example:

- Domain: “dc=mycorp,dc=com”
- User ID Field: “uid”
- BIND User Domain: “uid=binduser,cn=read-only-bind,dc=mycorp,dc=com”
- BIND Password: “pre-shared-key”

When “bobby.singer” attempts to login, TrueCommand will establish an SSL-secure connection to the LDAP server. TrueCommand will use the *BIND User Domain* and *BIND Password* settings to perform an initial bind using pre-known settings from your LDAP provider. Once bound, TrueCommand will search for the user matching “uid=bobby.singer”, but only within the subdomains that include the “domain” setting (“dc=mycorp,dc=com” in this example). If TrueCommand finds a user, it will use the full user domain string from the search result to initialize a second bind along with the user-provided password. If successful, TrueCommand verifies the user authentication and Bobby Singer is allowed access to TrueCommand.

SSL/TLS Connection Info

WARNING: AD/LDAP authentication *requires* SSL connections.

If the LDAP server uses an SSL certificate generated by a custom certificate authority (CA), then one of two things must occur before TrueCommand can use the LDAP server:

- (Option 1) Users must register the custom certificate authority with TrueCommand via the *Certificates* tab in *Administrator Settings*.
- (Option 2) Users can disable the *Verify SSL* option to accept whatever SSL certificate the server provides. Users may need to choose Option 2 if the LDAP server hostname is different than the one listed on the certificate, or if the server uses a self-signed SSL certificate.

Enabling *Allow LDAP user creation* means TrueCommand creates user accounts when someone logs in to the User Interface with their LDAP credentials. *JOIN TEAM* automatically adds LDAP users to specific TrueCommand teams.

Enabling *Allow LDAP user creation* means TrueCommand creates user accounts when someone logs in to the User Interface with their LDAP credentials. *JOIN TEAM* automatically adds LDAP users to specific TrueCommand teams.

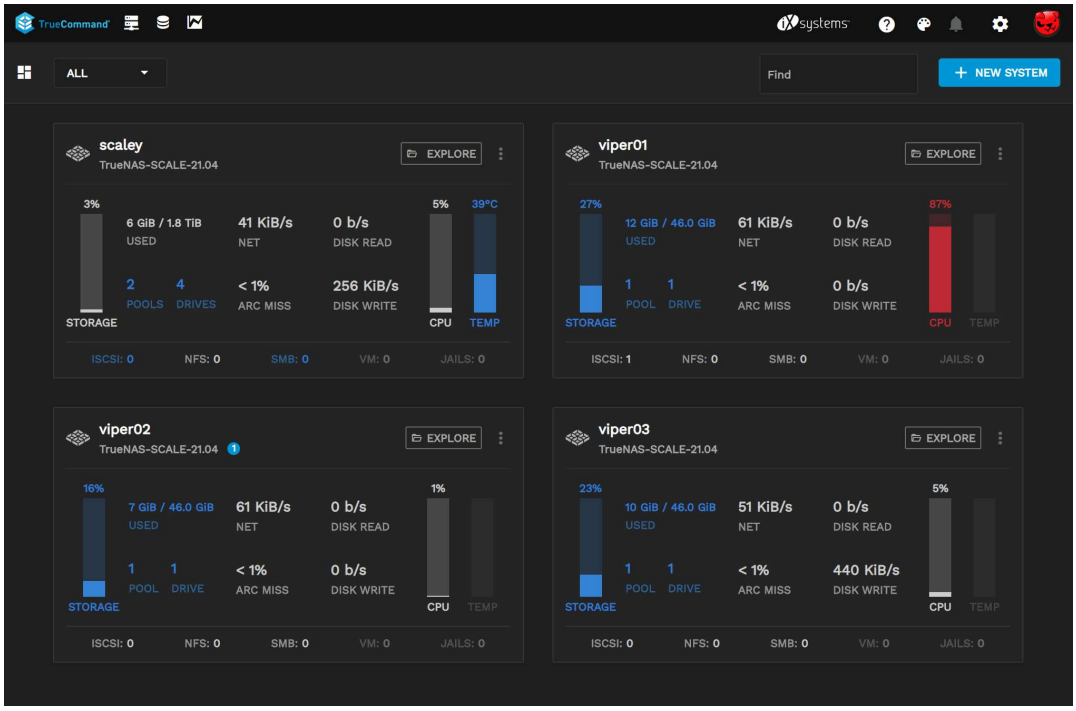
Telemetry

TrueCommand reports some basic usage telemetry back to iXsystems for product improvement analysis. These metrics are completely anonymous.

Click the *PREVIEW* button to see exactly what your system is sending.
Check the *Disable Telemetry* check box and click the *SAVE* button to disable this feature.

5 - System Management

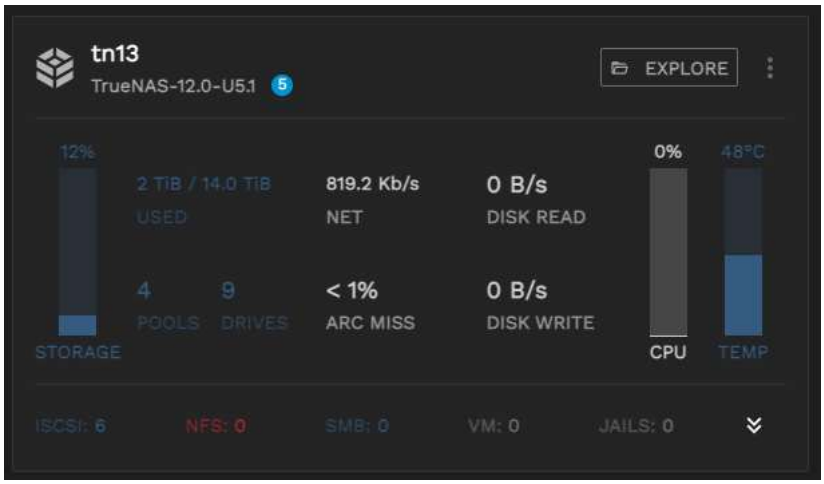
The TrueCommand dashboard gives quick status overviews of the TrueNAS systems it is connected to.



For information on the Top Bar and its options, refer to the Interface Overview article in the Getting Started Documentation.

System Cards

Each system has a unique card to display statistics. When the system has an alert, an *Alerts* bubble appears next to the system version to show how many alerts there are for that specific system. See Alert Management for further information.



Storage lists how many pools and drives are being used by the system. It also shows how much storage is used and available by size and percentage.

ARC MISS shows how often the system is using disks instead of the ARC cache. Anything above 0% means that the system is using RAM. The numbers vary on use case and work load.

There are also several "hot spots" on the card that will open system specific areas for management.

Clicking the system name on the card shows an expanded view of the system with more Single System Management options.

Clicking the *Alerts* bubble after the system version on the card will open an expanded system information screen that lists the current system alerts.

Clicking *DRIVE*, *DISK WRITE*, *DISK READ* displays the disk activity graph.

Clicking *NET* displays the Net Activity graph.

Clicking *CPU* displays the CPU Usage percentages graph.

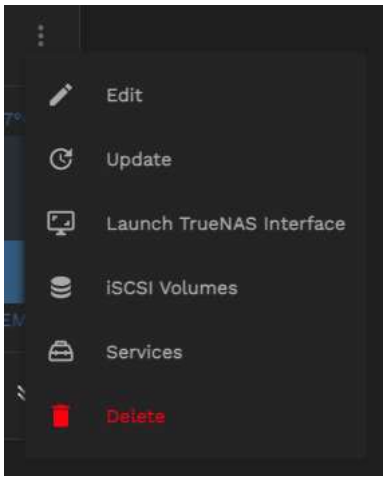
Clicking *TEMP* displays the CPU Temperature percentages graph.

Clicking *ISCSI*, *NFS*, and *SMB* opens a *Services* window that allows users to stop/start Services for the system.

Clicking *VM* opens a *Virtual Machines* window that allows users to start/stop VM's on the system.

Clicking *APPS* (Scale) or *Jails* (TrueNAS 12.x) opens a window that allows users to start/stop APPS/Jails on the system.

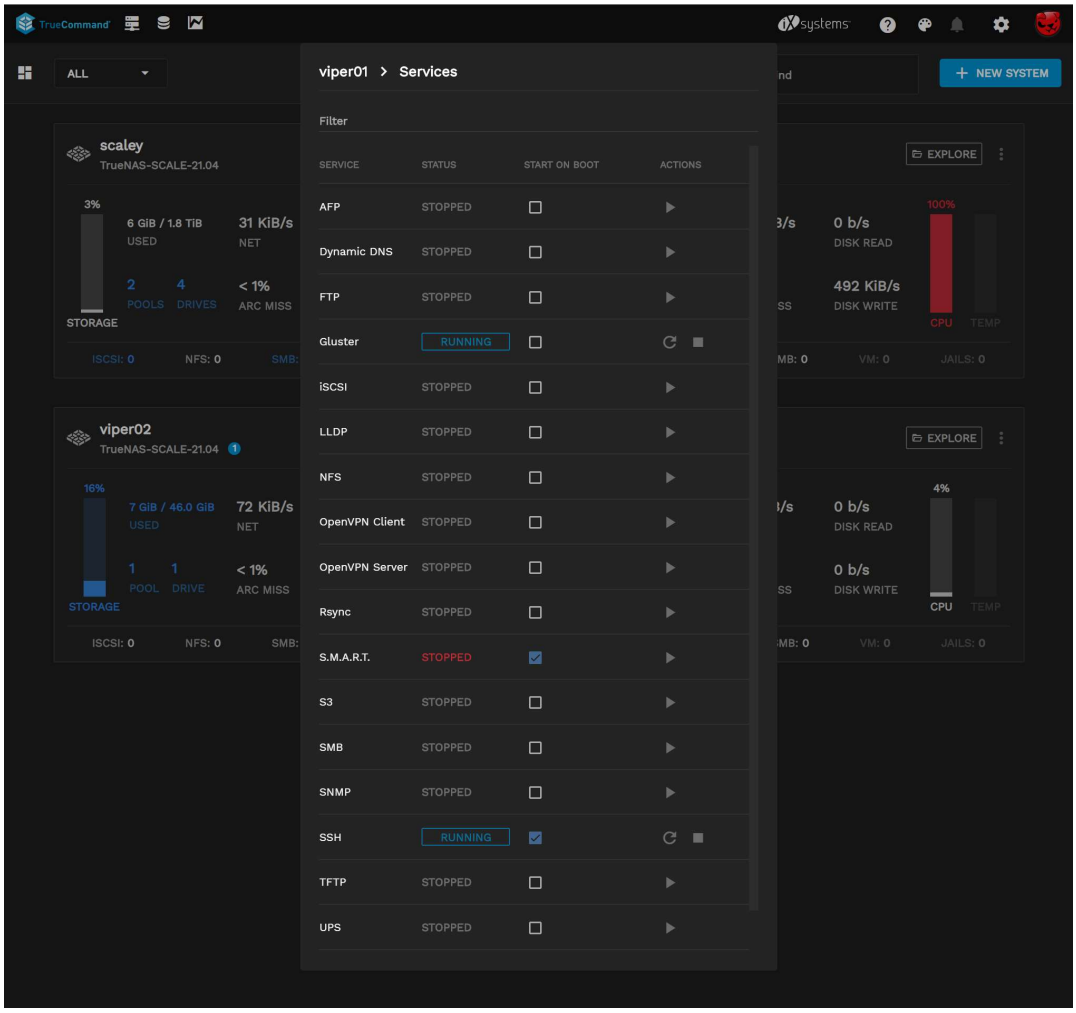
Options Menu



The *Options* menu has several shortcuts to simple tasks.

- **Edit** opens the edit window for the TrueNAS connection details and nickname.
- **Update** updates the TrueNAS system.
- **Launch TrueNAS Interface** opens a new tab for the full TrueNAS Web UI.
- **iSCSI Volumes** opens the specific TrueNAS's iSCSI management page.
- **Services** opens the services page, which allows users to directly control current service status and autostart.
- **Delete** removes the system from TrueCommand. This does not delete any data stored on the TrueNAS system. However, it does delete all system metrics that are saved in TrueCommand's database.

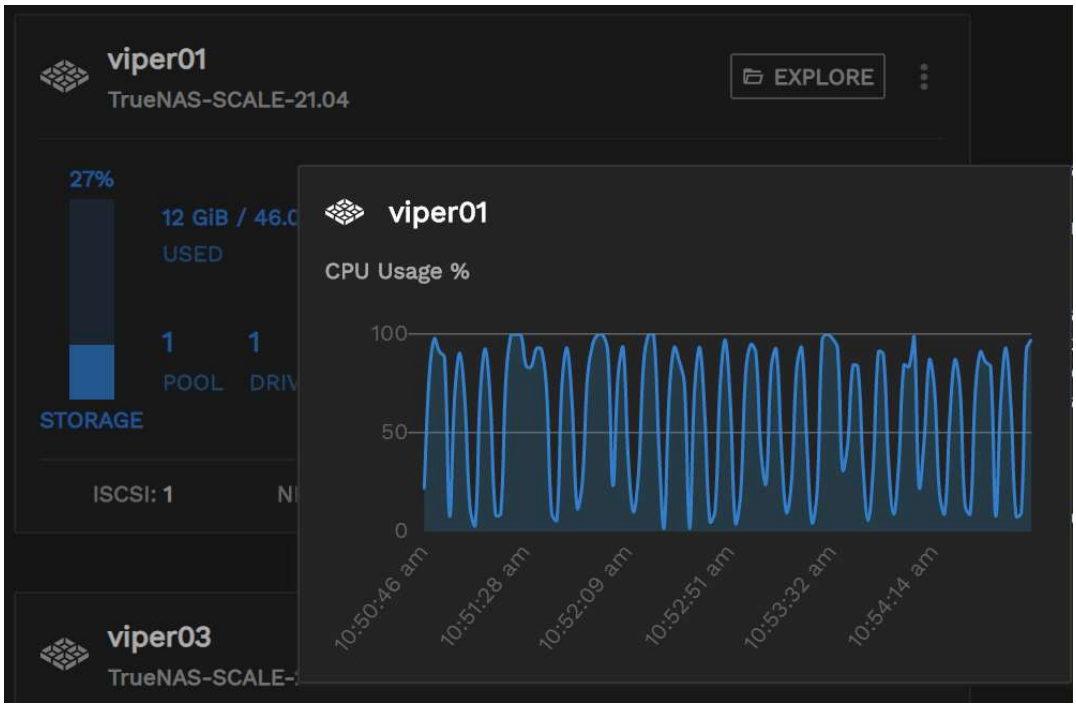
Services



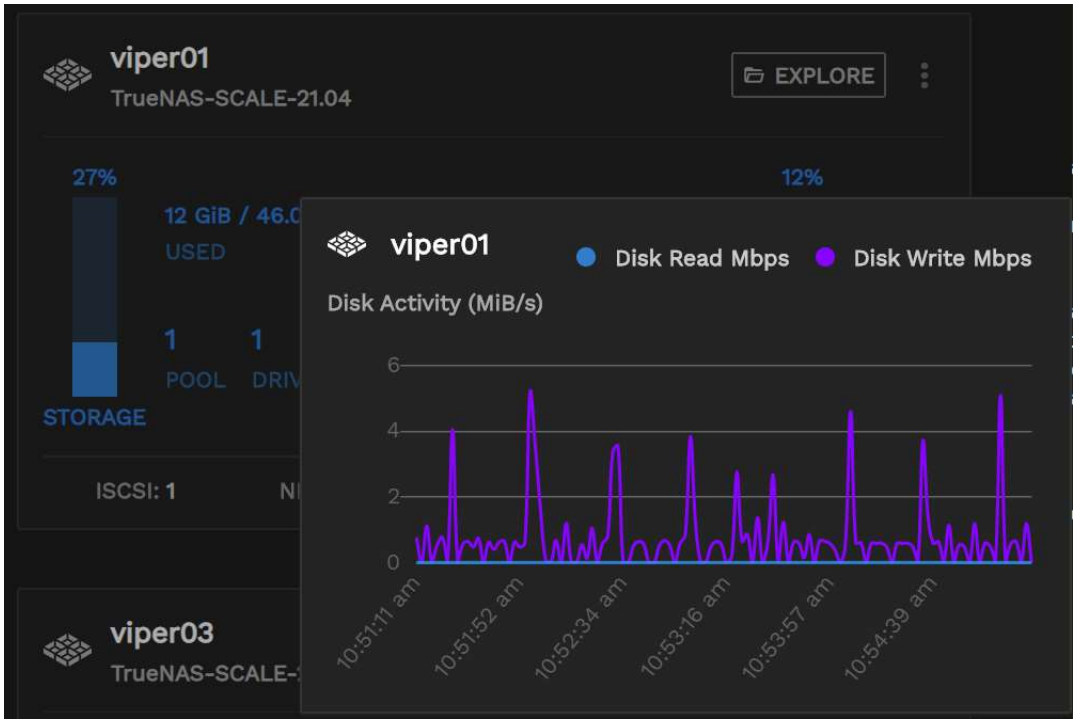
Graphs

Clicking on the values for CPU, Disk, and Network will open small popup windows that display the statistical history for systems.

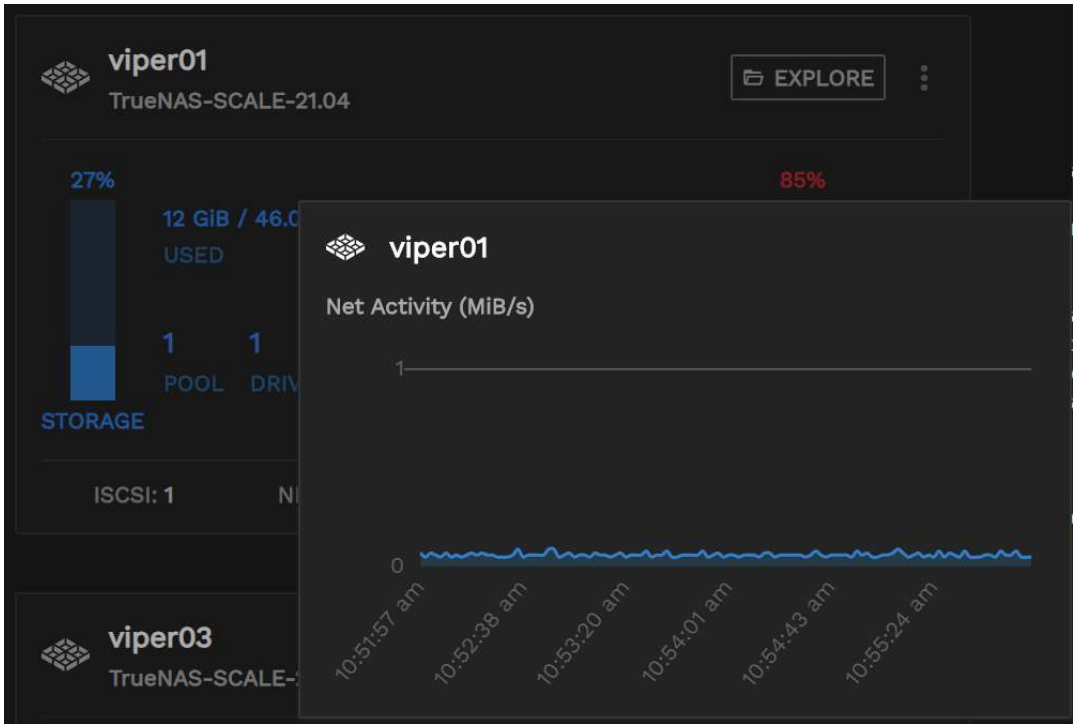
- CPU



- Disk

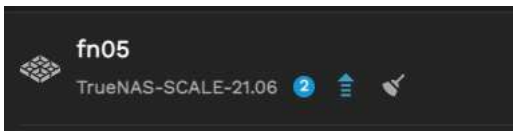


- Network



Activity Indicator Icons

TrueCommand's individual indicators provide a better, "at-a-glance", indication of what the system is up to. The indicators will be visible to the right of the system nickname.



- Update: 
- Replication: 

- Resilver/Scrub : 

5.1 - Single System Management

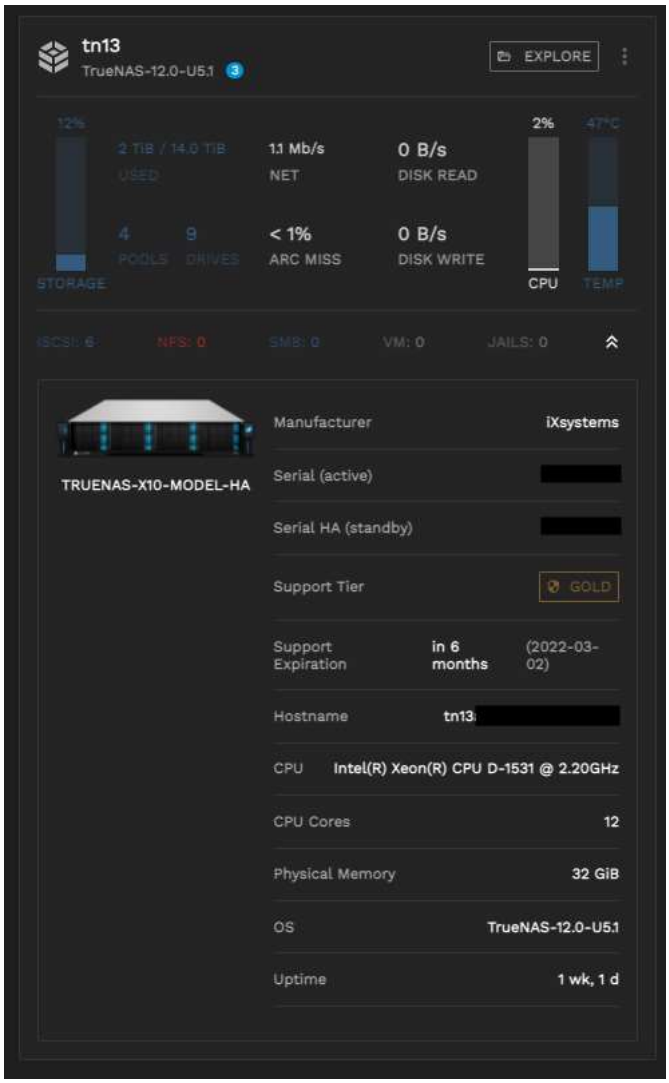
While TrueCommand allows users to manage all of their systems on a single dashboard, it also lets users view single systems at a time.

To manage a single system either click the name of the system in the system card or click the dashboard drop-down menu, hover over *Ungrouped*, and select the system you want to manage.

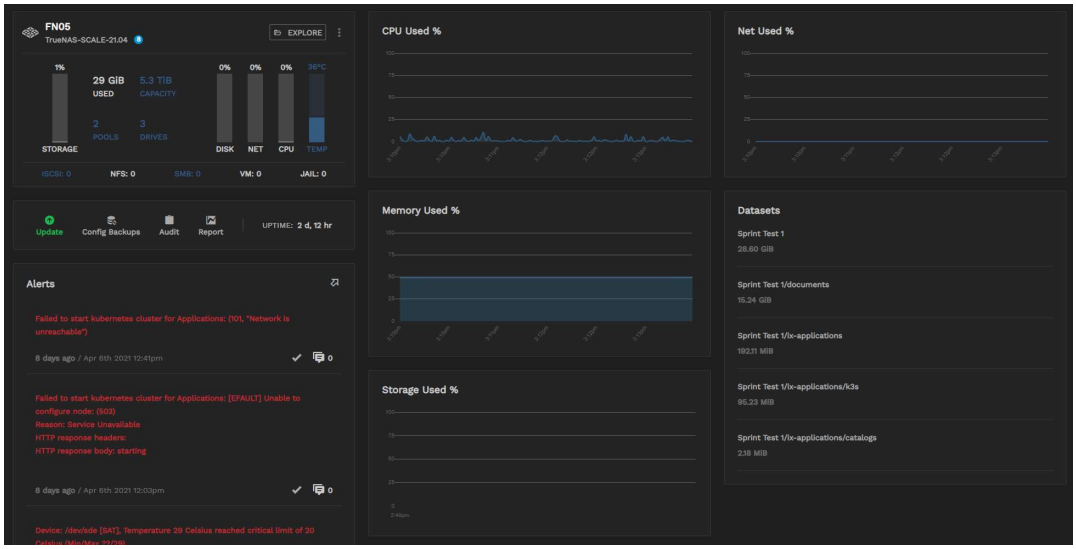
While viewing a single system, users can see various statistics like CPU, Memory, and Storage usage, as well as existing datasets and alerts.

Users can create and manage storage, snapshots, and shares using the File Explorer.

Users can also view the TrueNAS system's Manufacturer, Serial Numbers, Support Tier, Support Expiration date, Hostname, CPU, CPU Cores, Physical Memory, OS, and Uptime by clicking on the double arrows located at the lower right corner of the System Card.

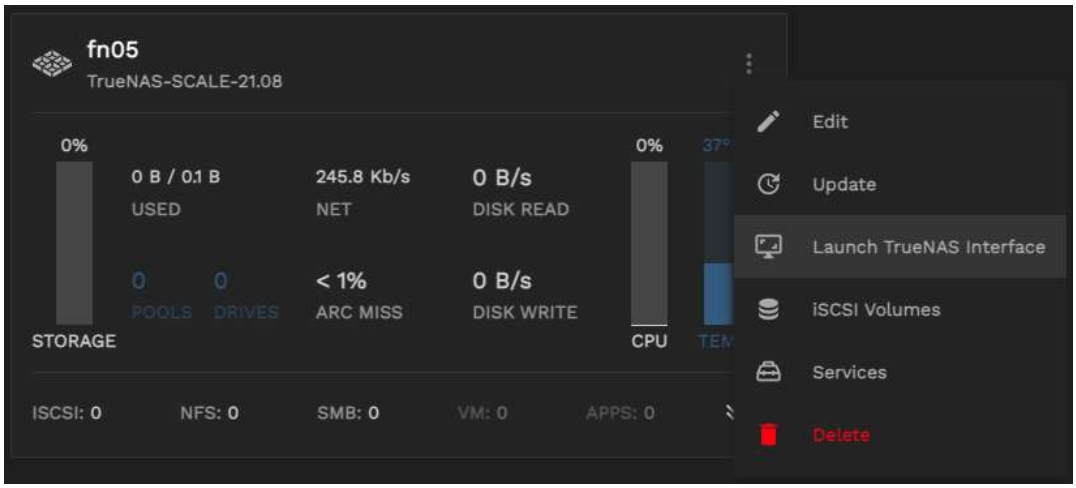


Users with adequate permissions may update the system, configure backups, and generate system audits and reports.


FN05
TrueNAS-SCALE-21.04
EXPLORE
1%
29 GiB
USED
5.3 TiB
CAPACITY
2
POOLS
3
DRIVES
STORAGE
0%
0%
0%
36°C
DISK
NET
CPU
TEMP
iSCSI: 0
NFS: 0
SMB: 0
VM: 0
JAIL: 0
Update
Config Backups
Audit
Report
UPTIME: 2 d, 12 hr
Alerts
Failed to start kubernetes cluster for Applications: (101, "Network is unreachable")
8 days ago / Apr 6th 2021 12:41pm
0
Failed to start kubernetes cluster for Applications: [EFAULT] Unable to configure node: (503)
Reason: Service Unavailable
HTTP response headers:
HTTP response body: starting
8 days ago / Apr 6th 2021 12:03pm
0
Device: /dev/sde [SAT], Temperature 29 Celsius reached critical limit of 20
CPU Used %
Net Used %
Memory Used %
Storage Used %
Datasets
Sprint Test 1
28.60 GiB
Sprint Test 1/documents
15.24 GiB
Sprint Test 1/ix-applications
192.11 MiB
Sprint Test 1/ix-applications/k3s
95.23 MiB
Sprint Test 1/ix-applications/catalogs
2.18 MiB

5.1.1 - System Settings

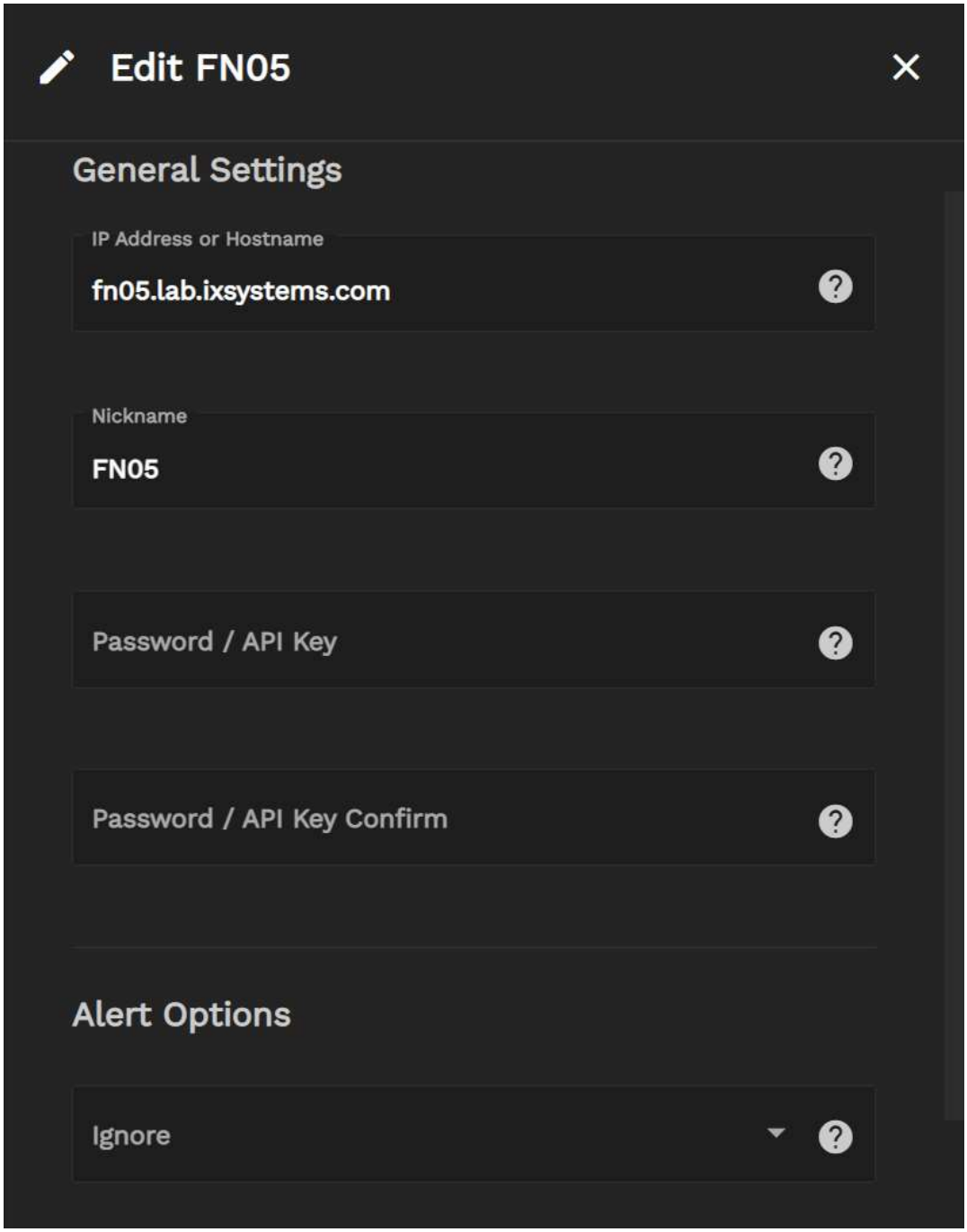
TrueCommand allows users to manage certain settings when managing a single system. To see the system settings menu, click the three-dot menu in a system's window on the TrueCommand dashboard.



Edit

To edit a systems general settings, click the *Edit* button in the system settings menu.

The *General Settings* window lets users edit the system's IP address/hostname, nickname, password/API key, and alert options.



Update

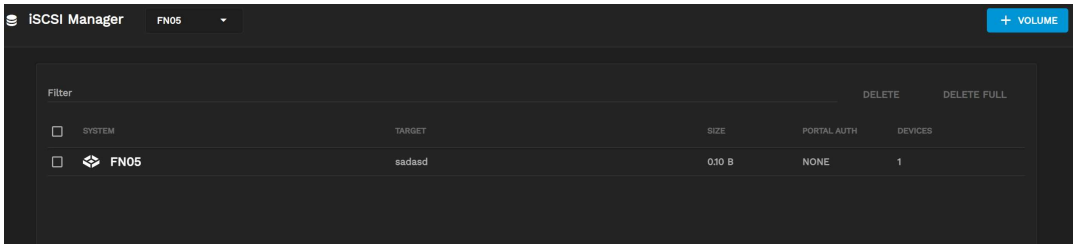
The update button in the system settings menu allows users to update the system to the latest build. During a system update the system card will change to indicate that the system is offline and finishing the update.

Launch TrueNAS Interface

Launch TrueNAS Interface in the system settings menu opens a new browser tab pointed at the system's web interface.

iSCSI Volumes

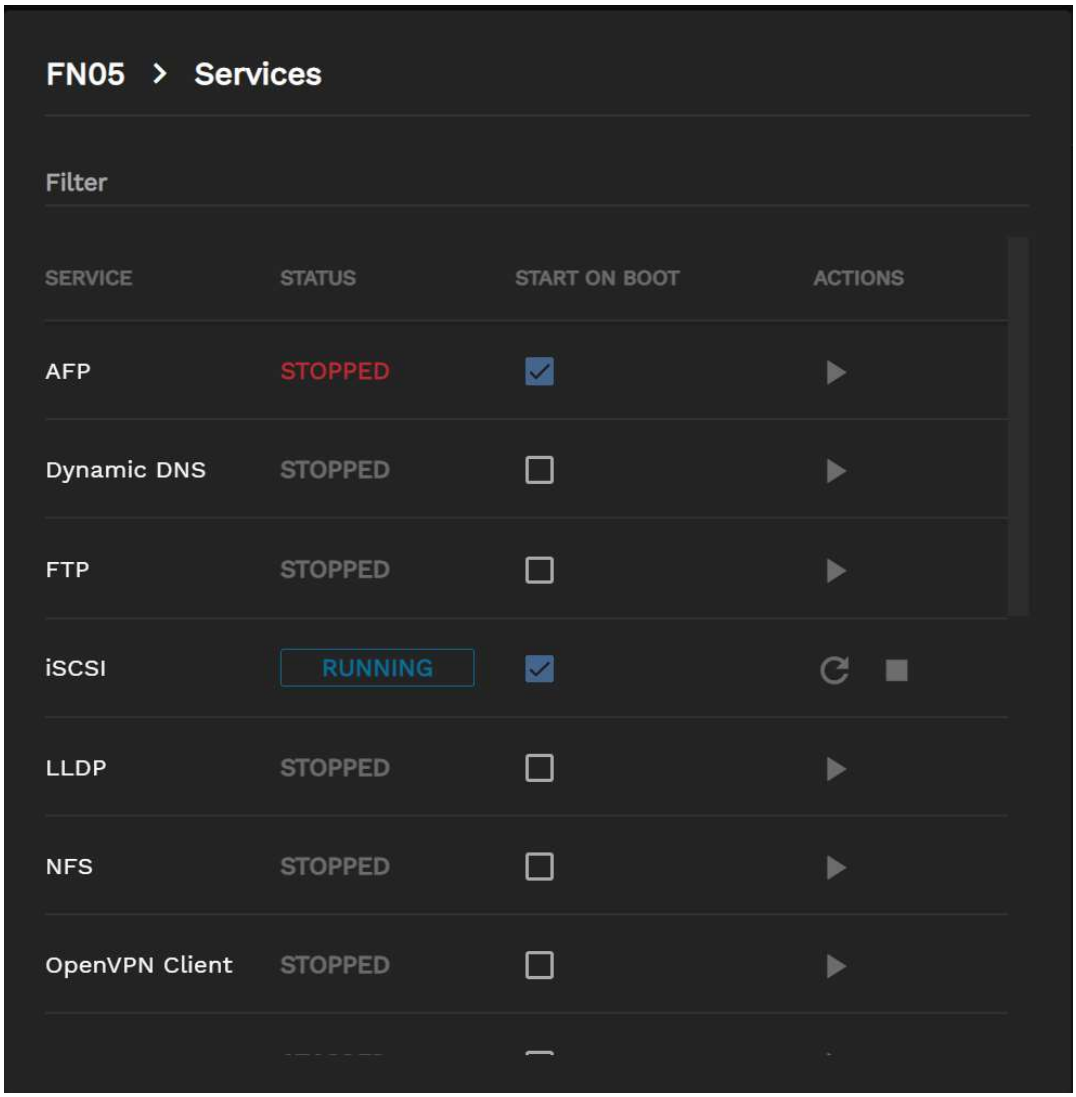
The *iSCSI Volumes* button in the system settings menu allows users to filter, create, and delete one or more iSCSI volumes.



See the full iSCSI Management article for more information.

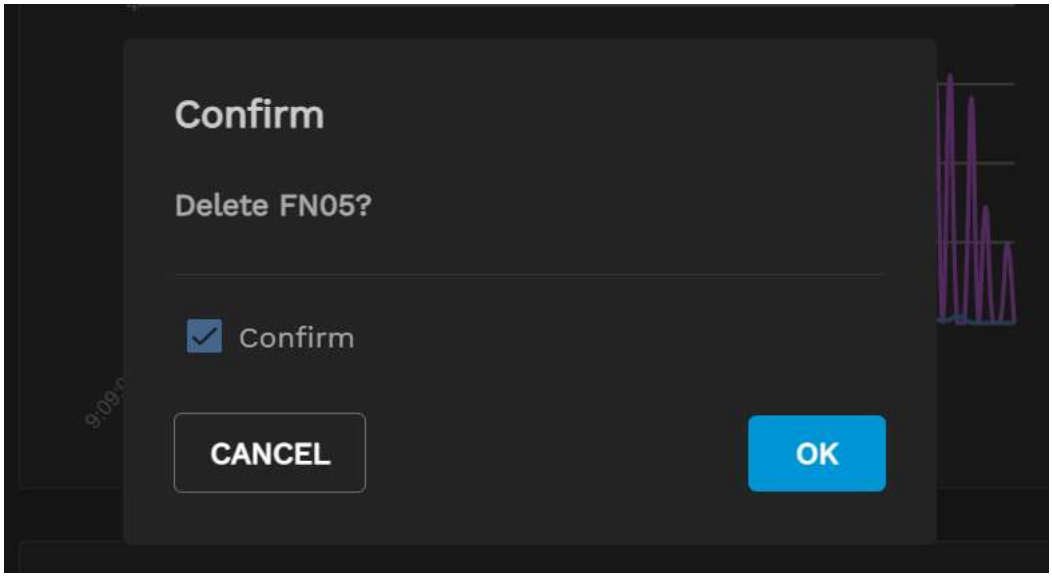
Services

TrueCommand offers limited control over system services. Users can't currently edit service parameters, but can set them to start on boot, as well as start, stop, and restart them.



Delete

TrueCommand offers limited control over system services. Users can't currently edit service parameters, but can set them to start on boot, as well as start, stop, and restart them.

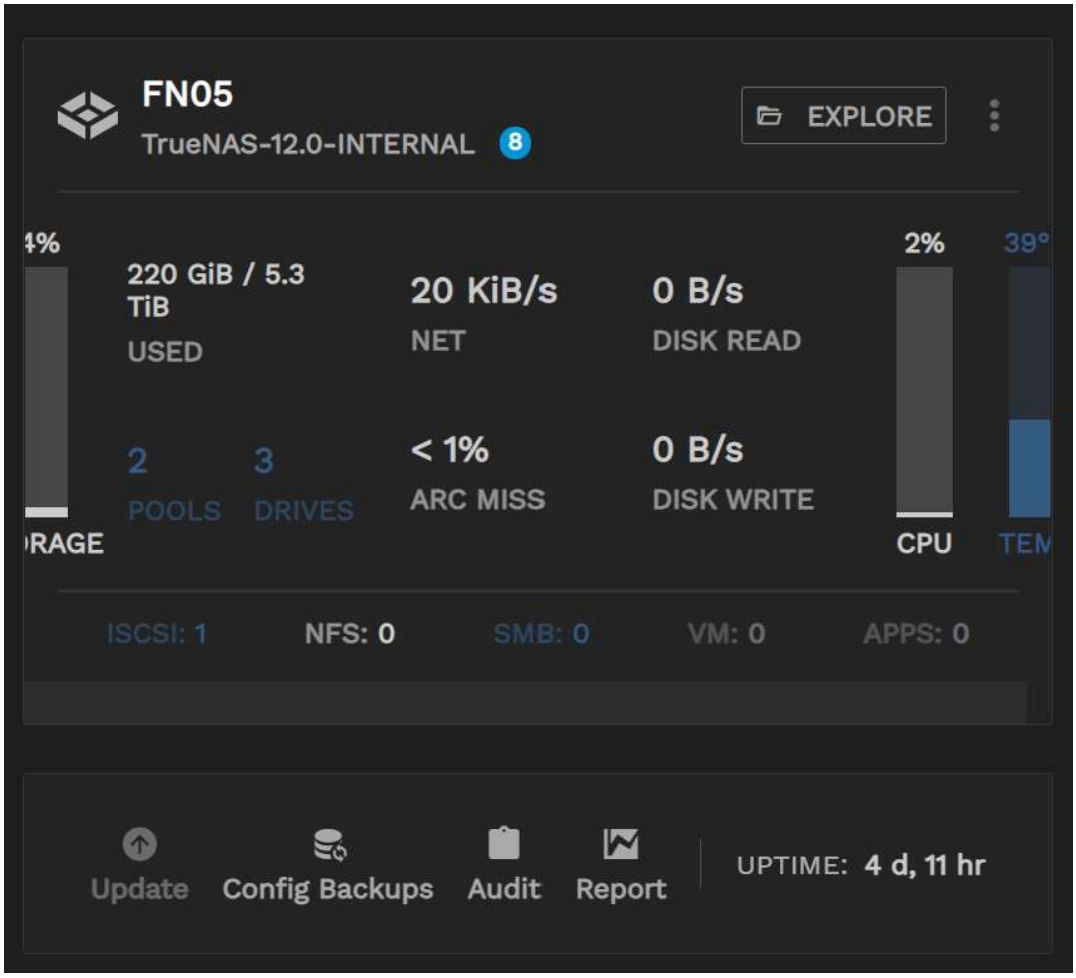

Confirm
Delete FN05?
Confirm
CANCEL
OK

5.1.2 - Config Backups

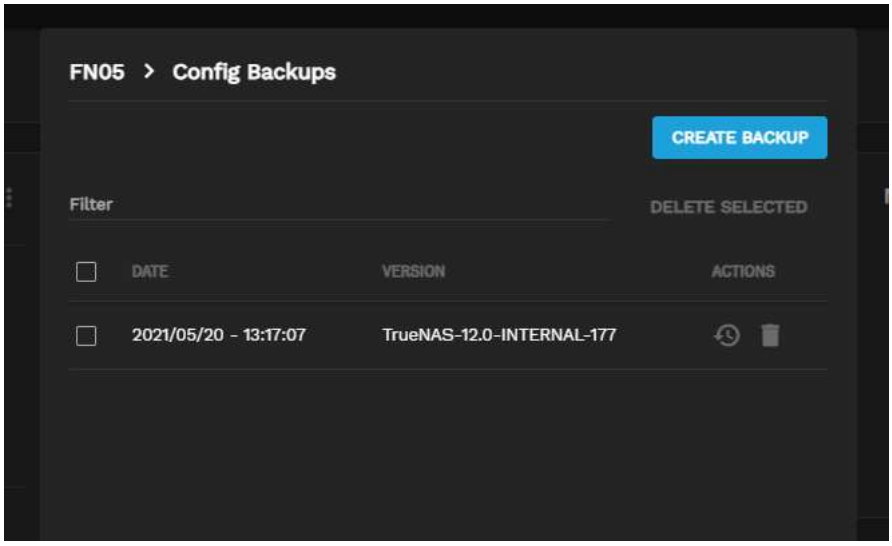
Create a Backup

To create a config backup for a single system, select that system from the dashboard drop-down or click the system's name in the dashboard window.

On the system's management page, click the *Config Backups* button, then click *CREATE BACKUP*.

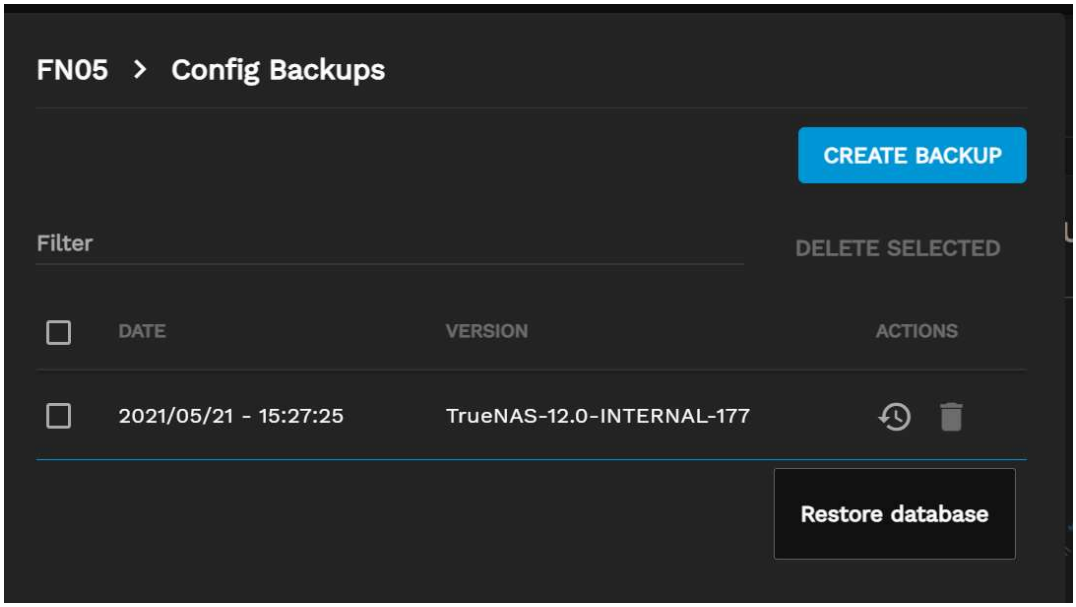


TrueCommand will create a config backup and display the date it was created, as well as what version of truenas the system was using at the time.



Restore a Database

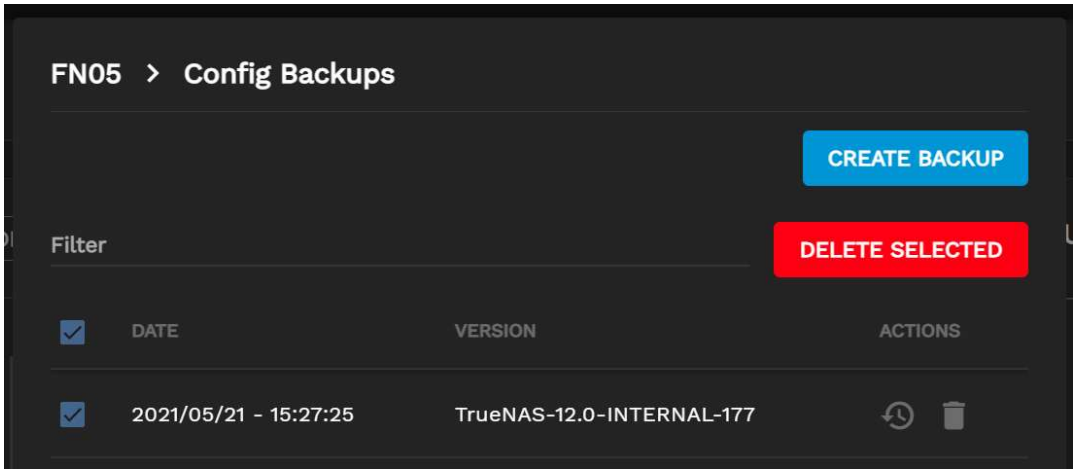
To restore the system to a backed-up config, click the *Config Backups* button on the system's management page, then click the *Restore database* button to the right of the config.



Delete Config Backups

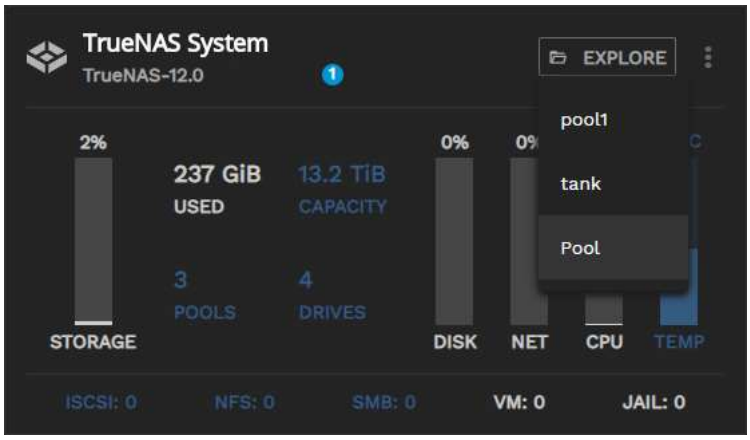
To delete a backup config, click the *Config Backups* button on the system's management page, then click the *Delete backup* button to the right of the config.

To delete multiple backup configs, check the boxes to the left of any configs you want to delete, the click the *DELETE SELECTED* button.


FN05 > Config Backups
CREATE BACKUP
Filter
DELETE SELECTED
DATE
VERSION
ACTIONS
2021/05/21 - 15:27:25
TrueNAS-12.0-INTERNAL-177

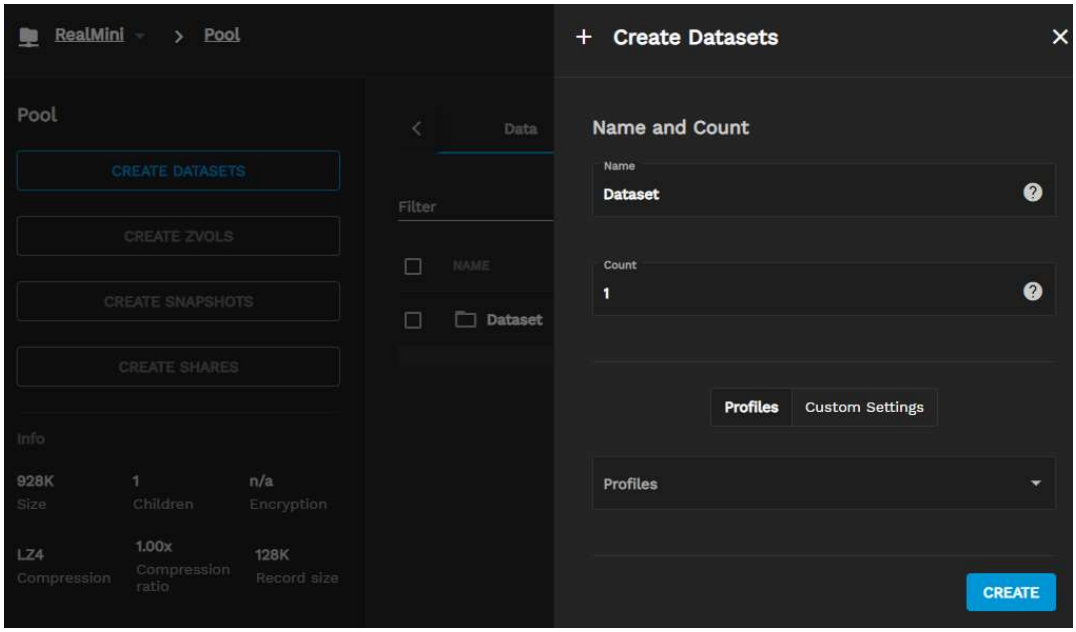
5.1.3 - TrueCommand Storage Management

To view, add, and delete storage from a single system in TrueCommand, click *EXPLORE* in that system's window, then select the pool you want to work with.



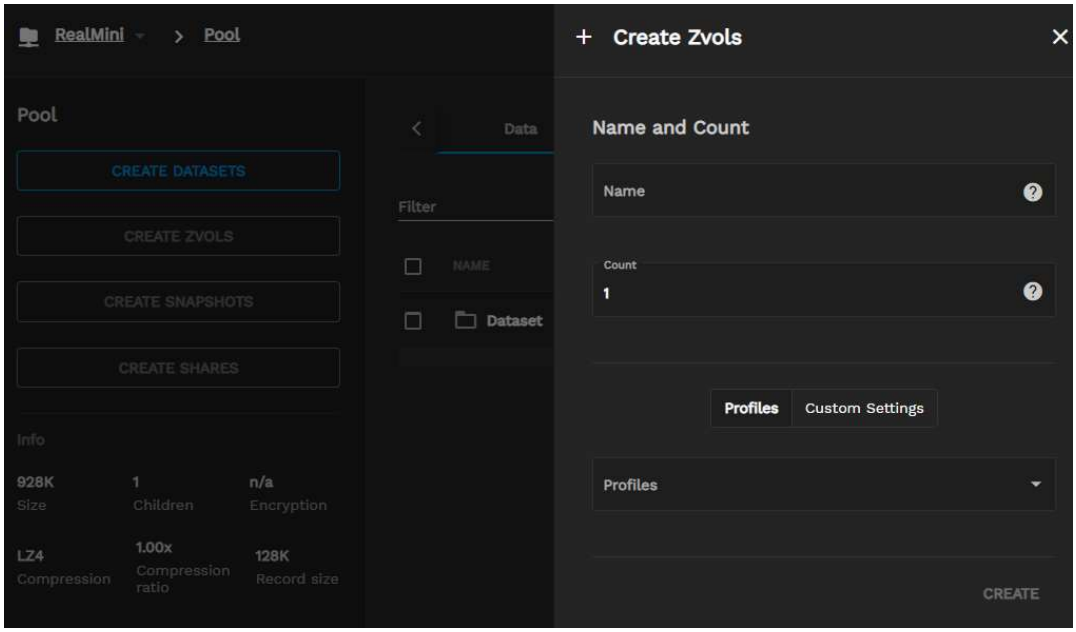
Adding a Dataset

1. In the pool's menu, click *CREATE DATASET*.
2. Name the dataset(s) and set how many you want to create.
3. Select a user-defined configuration profile or apply custom settings to the dataset(s), then click *CREATE*.



Adding a Zvol

1. In the pool's menu, click *CREATE ZVOLS*.
2. Name the zvol(s) and set how many you want to create.
3. Select a user-defined configuration profile or apply custom settings to the dataset(s), then click *CREATE*.



Deleting Storage

1. In the pool's menu, select the *Data* tab.
2. Check the boxes next the each item you want to delete, then click *DELETE*.

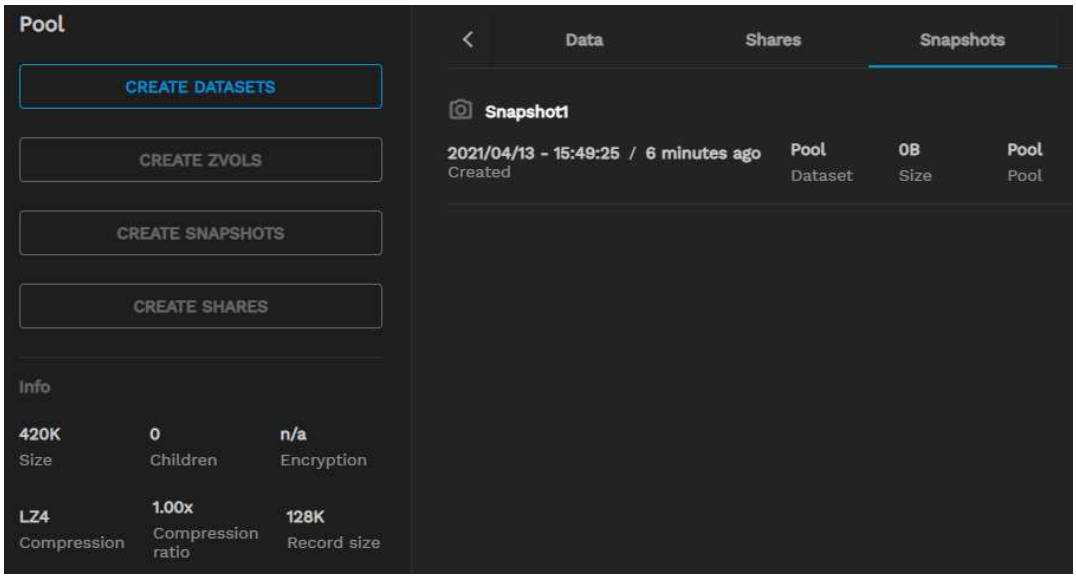
- Alternatively, you can click the three dot menu button next to each item and select either *Delete Dataset Recursively* or *Delete Dataset*.

3. Click *CONFIRM* to delete the item(s).

5.1.4 - TrueCommand Snapshots

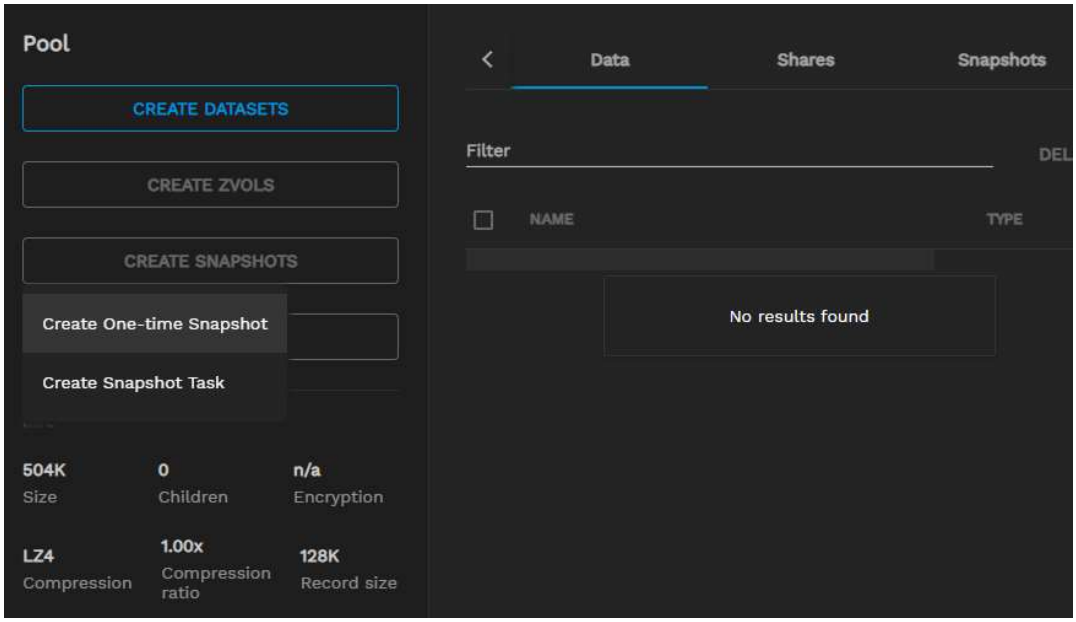
View Snapshots

To view a system's already existing snapshots, click *EXPLORE* in that system's window and select a storage pool. Once the pool loads, select the *Snapshots* tab.



Create Single Snapshots

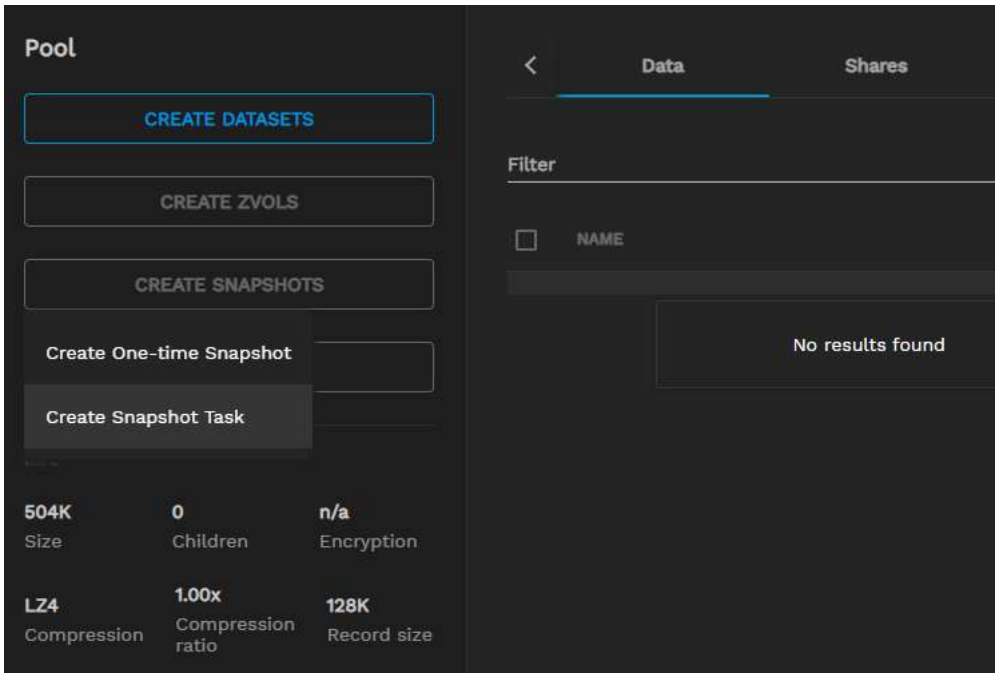
To create single snapshots, select a pool in the system's *EXPLORE* menu and click *CREATE SNAPSHOTS*, then select *Create One-Time Snapshot*.



Name the snapshot and click *CONFIRM*.

Create Recurring Snapshot Tasks

To create recurring snapshot tasks, select a pool in the system's *EXPLORE* menu and click *CREATE SNAPSHOTS*, then select *Create Snapshot Task*.



Set the task's schedule and determine the snapshot lifetime, then click *CONFIRM*.

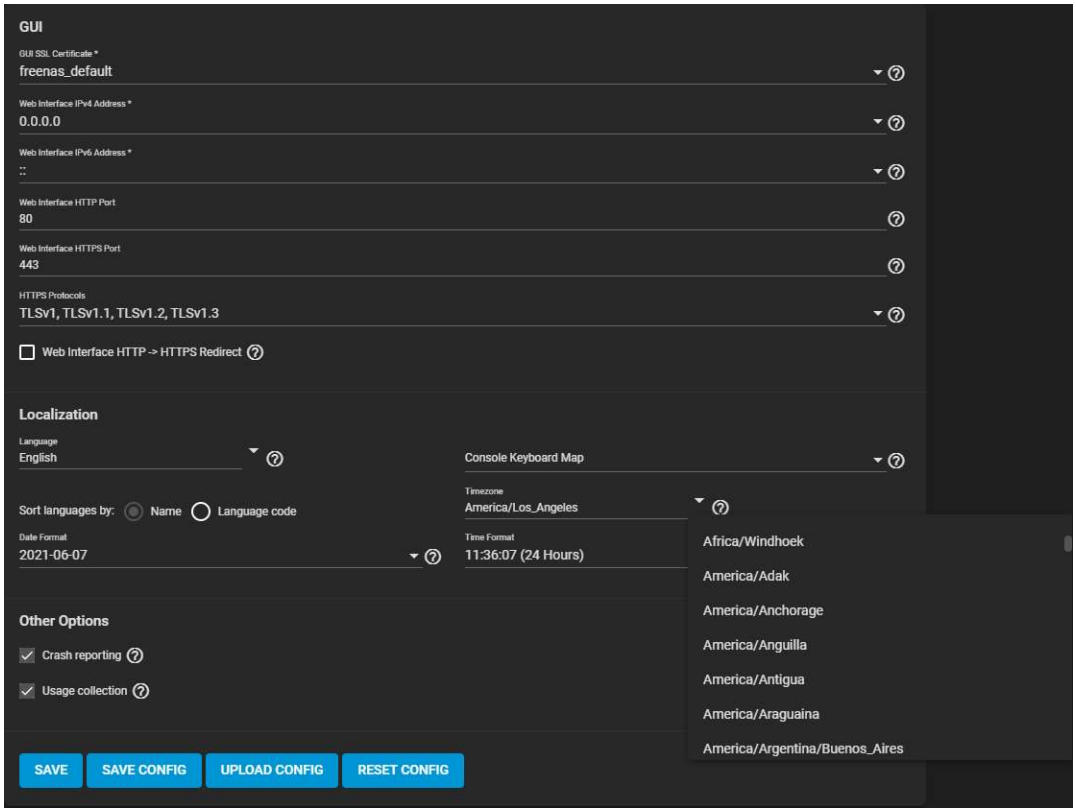
Timezones

When you create snapshot tasks, TrueCommand uses the system the dataset is mounted in to determine what timezone it will use.

For example, if you are in New York and the dataset is mounted to a system with a Los Angeles timezone, a snapshot task set to occur at 12:00 P.M. will actually occur at 3:00 P.M. your time.

To see what timezone a system is in, go to that system's UI and navigate to **System > General** (**System Settings > General** in SCALE).

That system's timezone information is in the *Localization* section. Administrators can change the system's timezone using the drop-down menu.

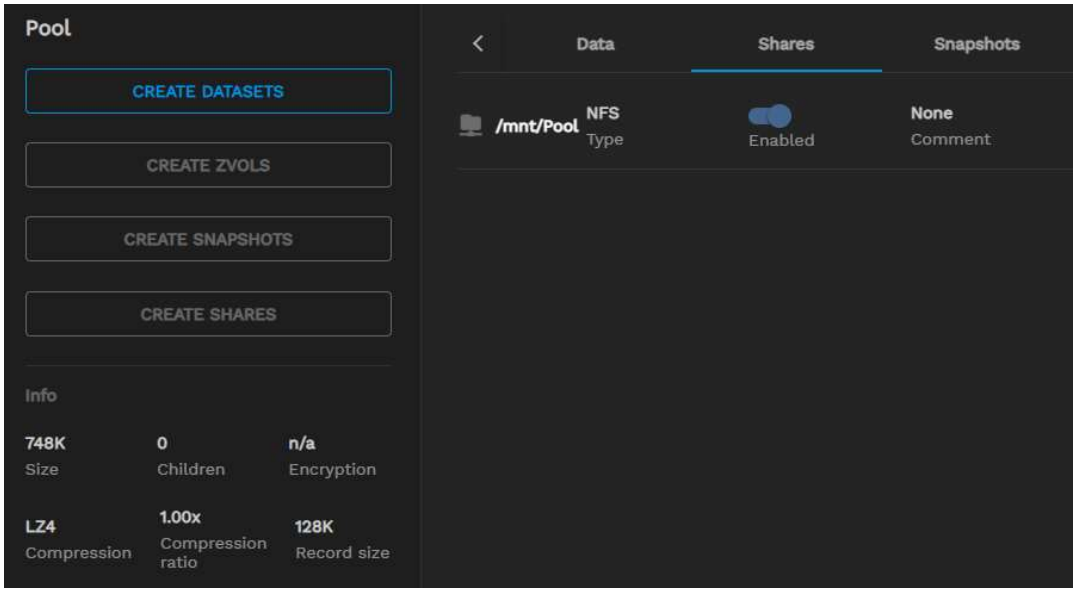

GUI
GUI SSL Certificate *
freenas_default
Web Interface IPv4 Address *
0.0.0.0
Web Interface IPv6 Address *
::
Web Interface HTTP Port
80
Web Interface HTTPS Port
443
HTTPS Protocols
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
Web Interface HTTP -> HTTPS Redirect
Localization
Language
English
Console Keyboard Map
Sort languages by:
Name
Language code
Timezone
America/Los_Angeles
Date Format
2021-06-07
Time Format
11:36:07 (24 Hours)
Other Options
Crash reporting
Usage collection
SAVE
SAVE CONFIG
UPLOAD CONFIG
RESET CONFIG
Africa/Windhoek
America/Adak
America/Anchorage
America/Anguilla
America/Antigua
America/Araguaina
America/Argentina/Buenos_Aires

5.1.5 - TrueCommand Sharing

View Existing Shares

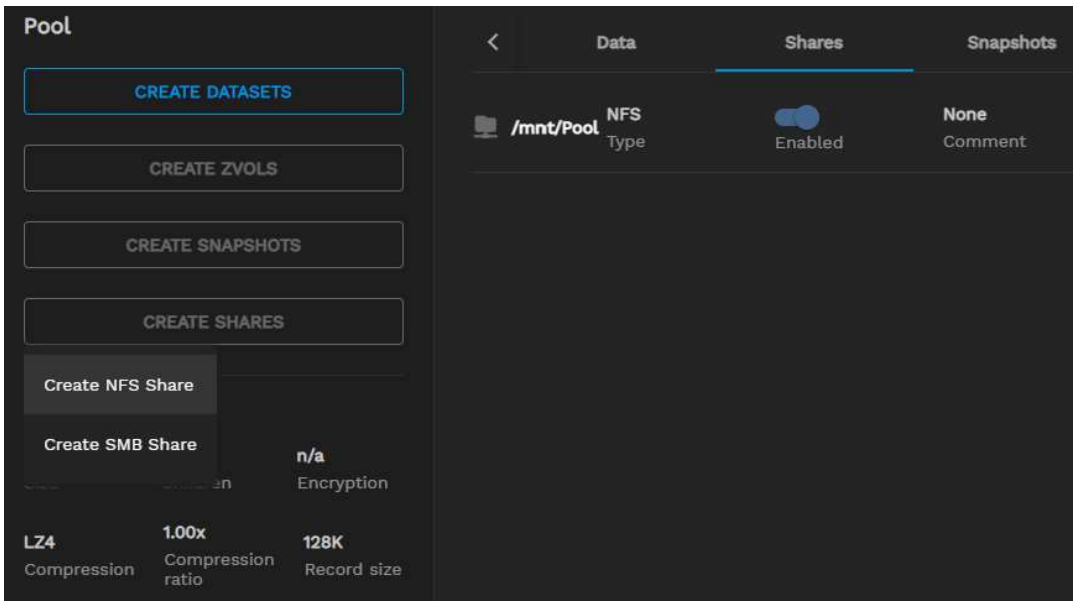
To view a pool's already existing shares, click *EXPLORE* in your system's window, then select the pool.

Once the pool loads, click the *Shares* tab to view its existing shares.



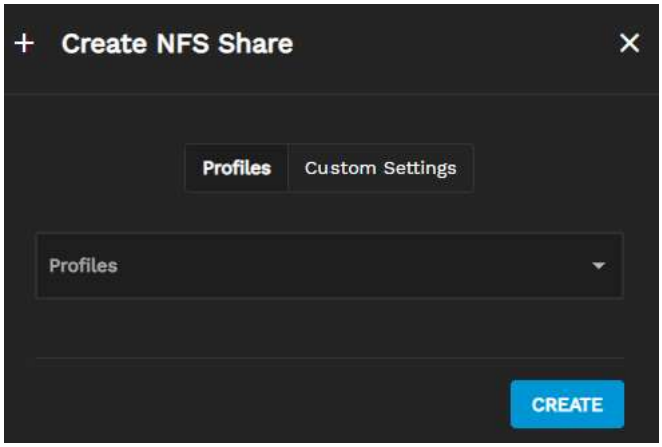
NFS Shares

To add an NFS share to a pool, open the pool using the *EXPLORE* menu in your system's window. Once the pool loads, click *CREATE SHARE* and select *Create NFS Share*.



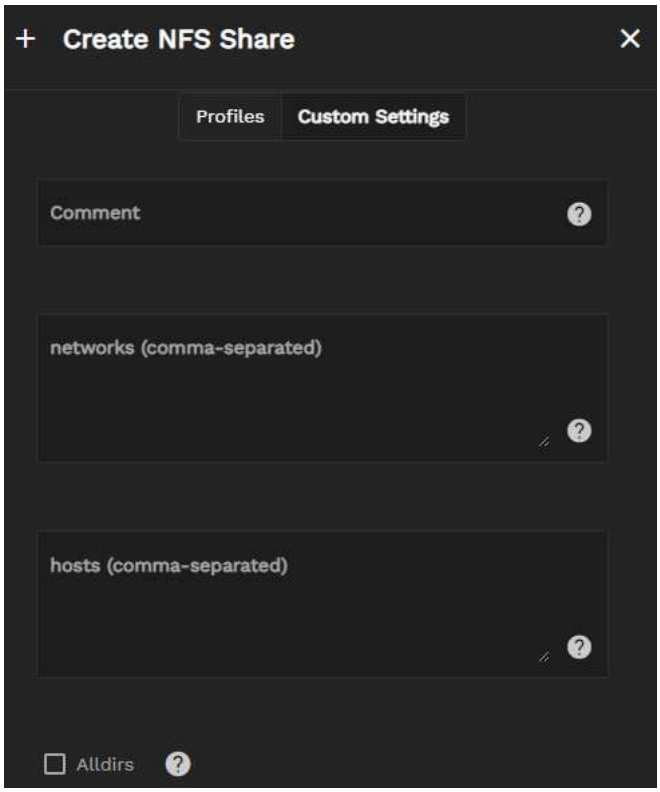
Create NFS Share From a Profile

To create an NFS share from an already existing user-defined configuration, select the *Profiles* tab, then select a profile from the dropdown and click *CREATE*.



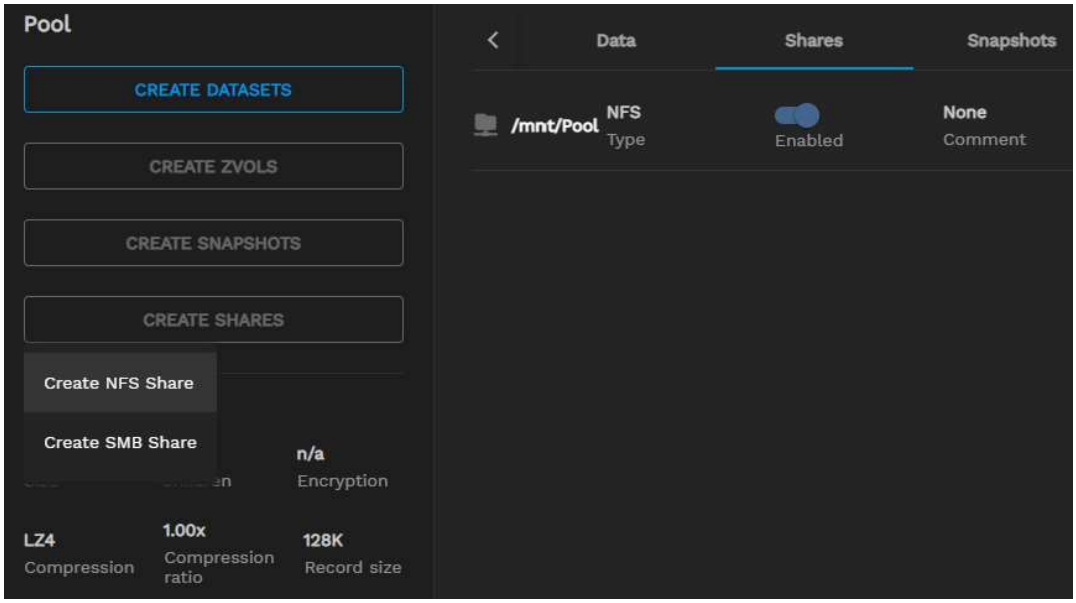
Create a Custom NFS Share

To create an NFS share with custom settings, select the *Custom Settings* tab and fill out the form, then click *SHARE*.



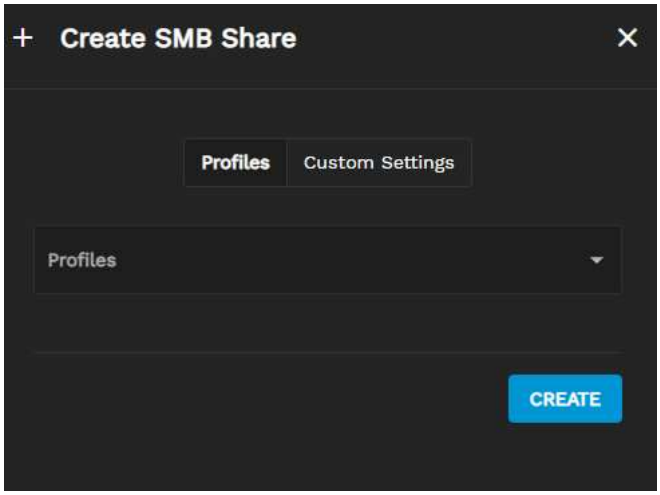
SMB Shares

To add an SMB share to a pool, open the pool using the *EXPLORE* menu in your system's window. Once the pool loads, click *CREATE SHARE* and select *Create SMB Share*.



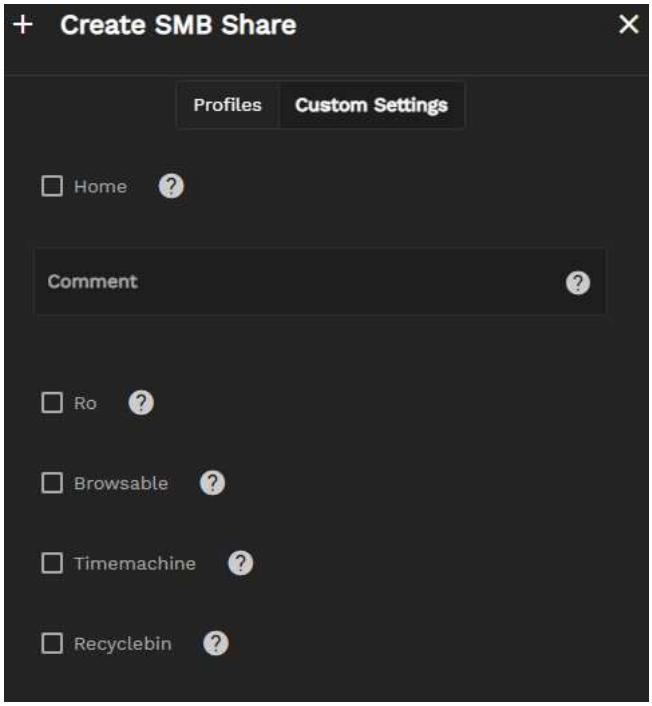
Create SMB Share From a Profile

To create an SMB share from an already existing user-defined configuration, select the *Profiles* tab, then select a profile from the dropdown and click *CREATE*.



Create a Custom SMB Share

To create an SMB share with custom settings, select the *Custom Settings* tab and fill out the form, then click *SHARE*.

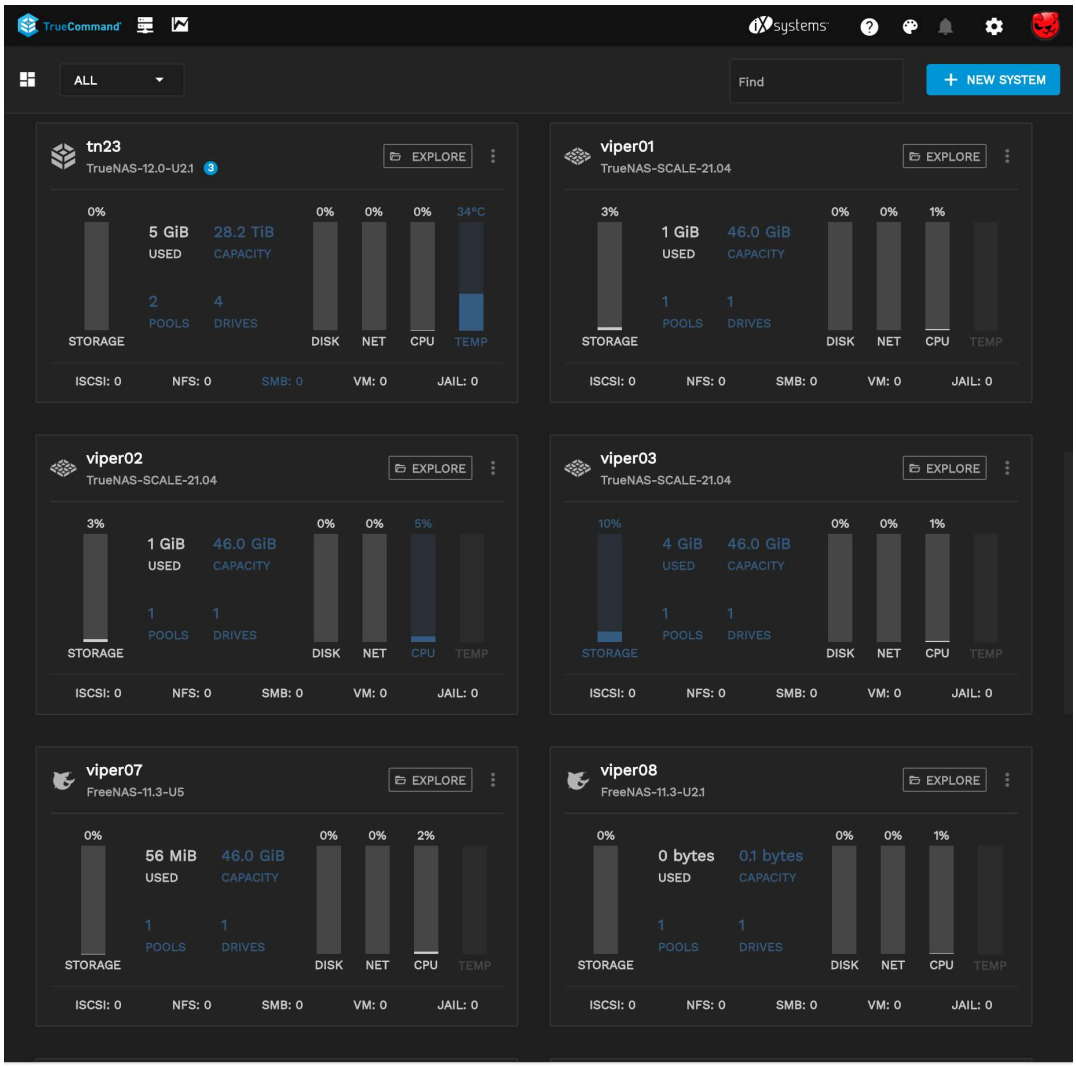

Create SMB Share
Profiles
Custom Settings
Home
Comment
Ro
Browsable
Timemachine
Recyclebin

5.2 - TrueNAS Configuration File Management

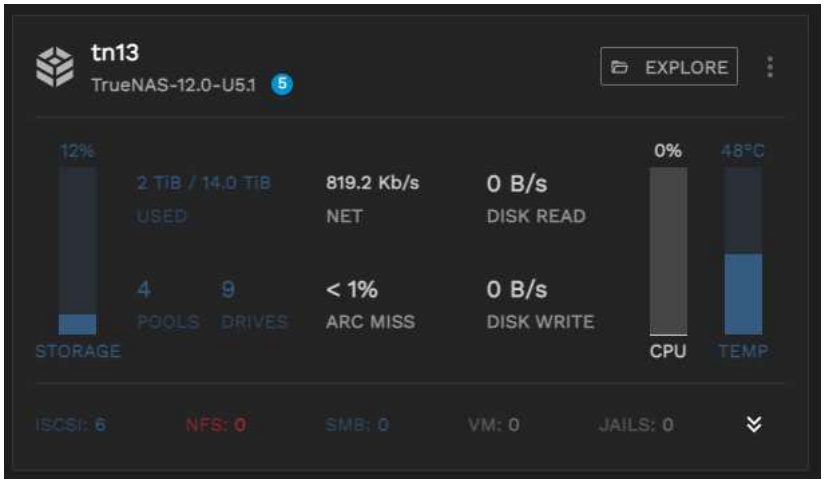
TrueCommand automatically backs up the TrueNAS configuration every 24 hours as well as any time there is a database change or a TrueCommand Audit Log entry. Users can create manual backups as needed.

Viewing Backups

To view the current TrueNAS configuration backups, open the **Dashboard**.



Click on the system name for a TrueNAS server to open the Single System view.

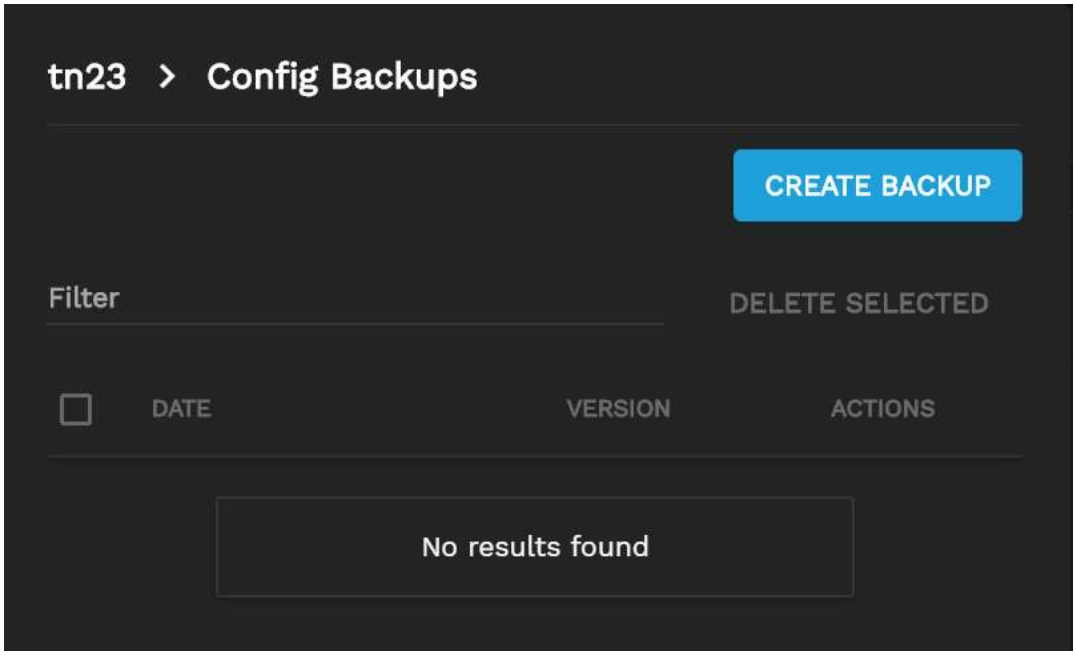


Click the **Config Backups** Button to open the config backup window.

The **Configuration Backup Window** shows a list of backups along with the time and date of their creation.

Create a config backup

To create a new backup, click **Create Backup.**

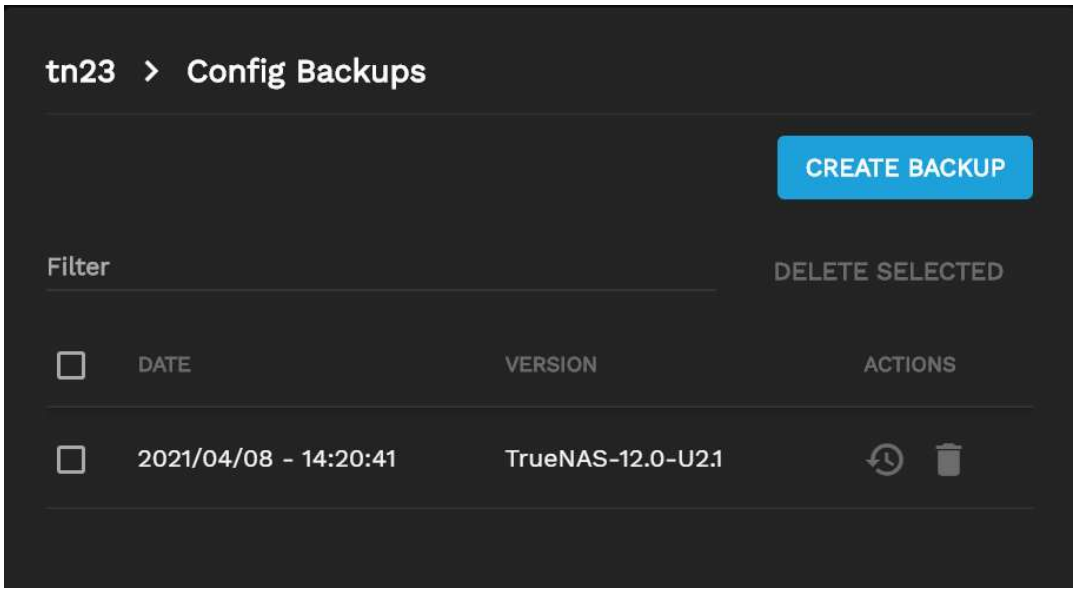


A maximum of one config backup per day can exist.
If a prior config backup for the current day exists, creating a new one will overwrite the previous backup.

> By default, TrueCommand retains seven backups. Local instances of TrueCommand can raise or lower this figure as desired. This can be changed in the Configuration Tab of the Administration Page.

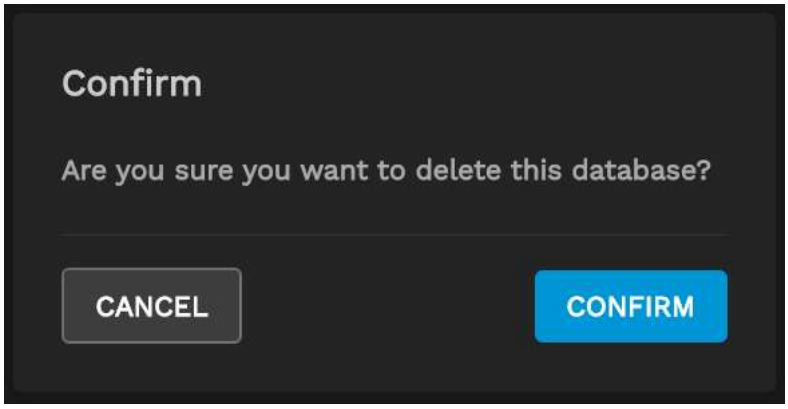
Apply a config backup

To reset a TrueNAS system to a previous configuration, click the icon. Choose the configuration file to use. You must reset the TrueNAS system to apply the configuration changes.



Delete a config backup

To Delete a backup, click the Delete Button delete button or mark the checkbox and click **Delete Backups.**


Confirm
Are you sure you want to delete this database?
CANCEL
CONFIRM

5.3 - Multiple Systems

TrueCommand has several multisystem management capabilities with more in development for future releases.

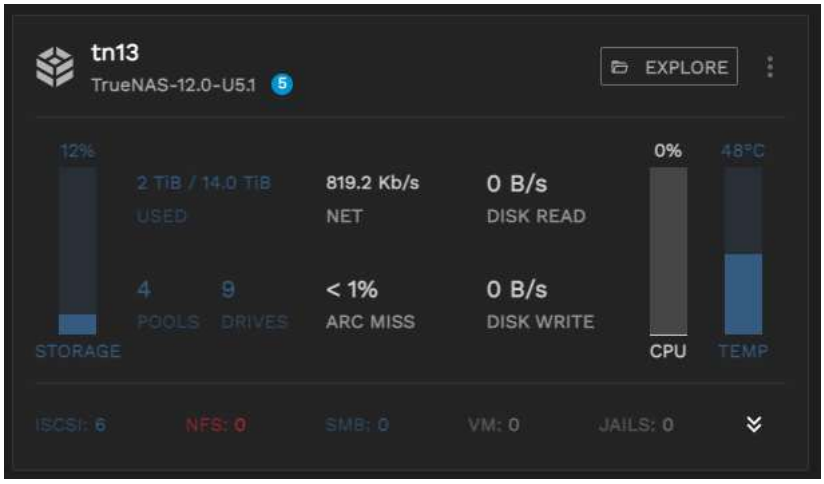
Cluster capability has been added with TrueCommand 2.0, as well as applying TrueNAS configurations to multiuple systems at once.

Config Management

TrueCommand can manage TrueNAS Config files. TrueCommand can also restore a single config file to multiple systems.

To apply a config to multiple systems, first create a config backup from the TrueNAS system you with the settings you wish to apply to other TrueNAS units.

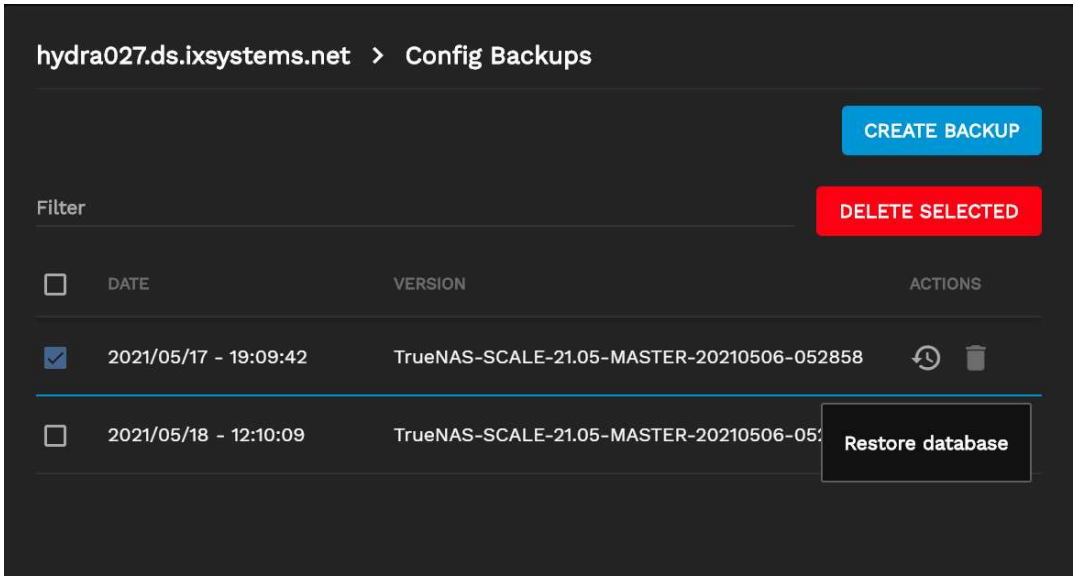
Click on the system name for a TrueNAS server to open the Single System view.



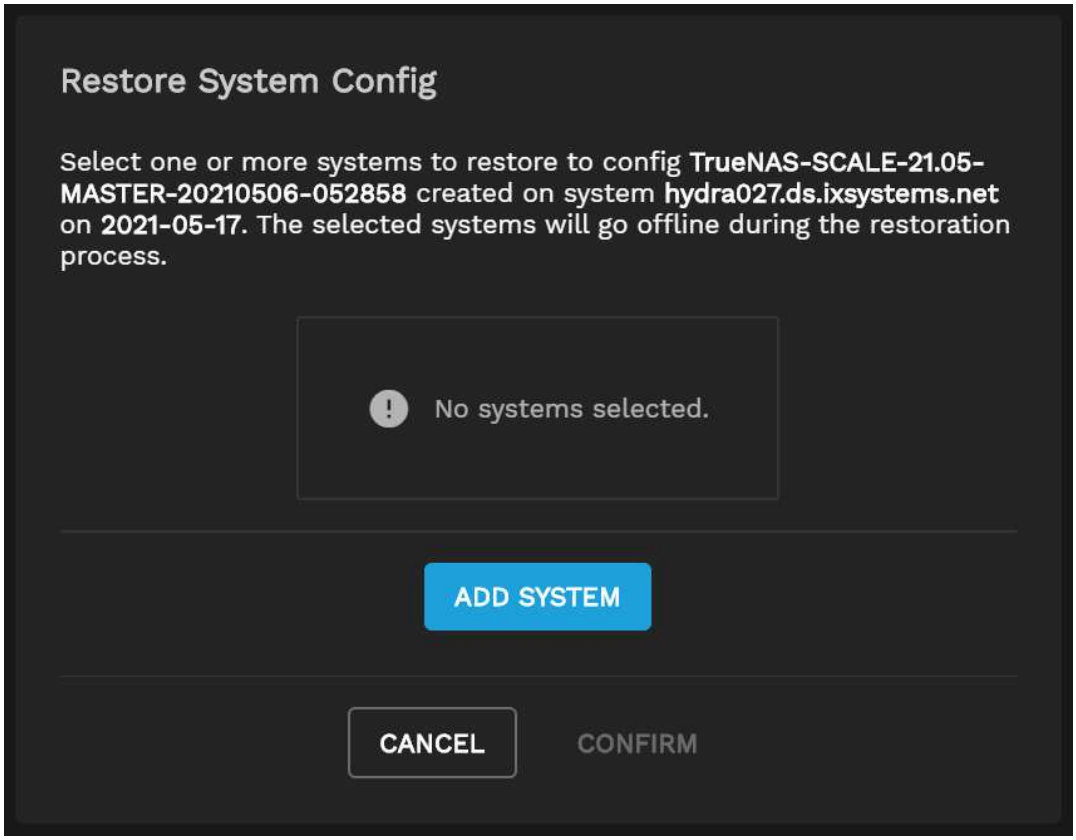
Click **Config Backups** to open the config backup window.

The **Configuration Backup Window** shows a list of backups with the time and date of their creation.

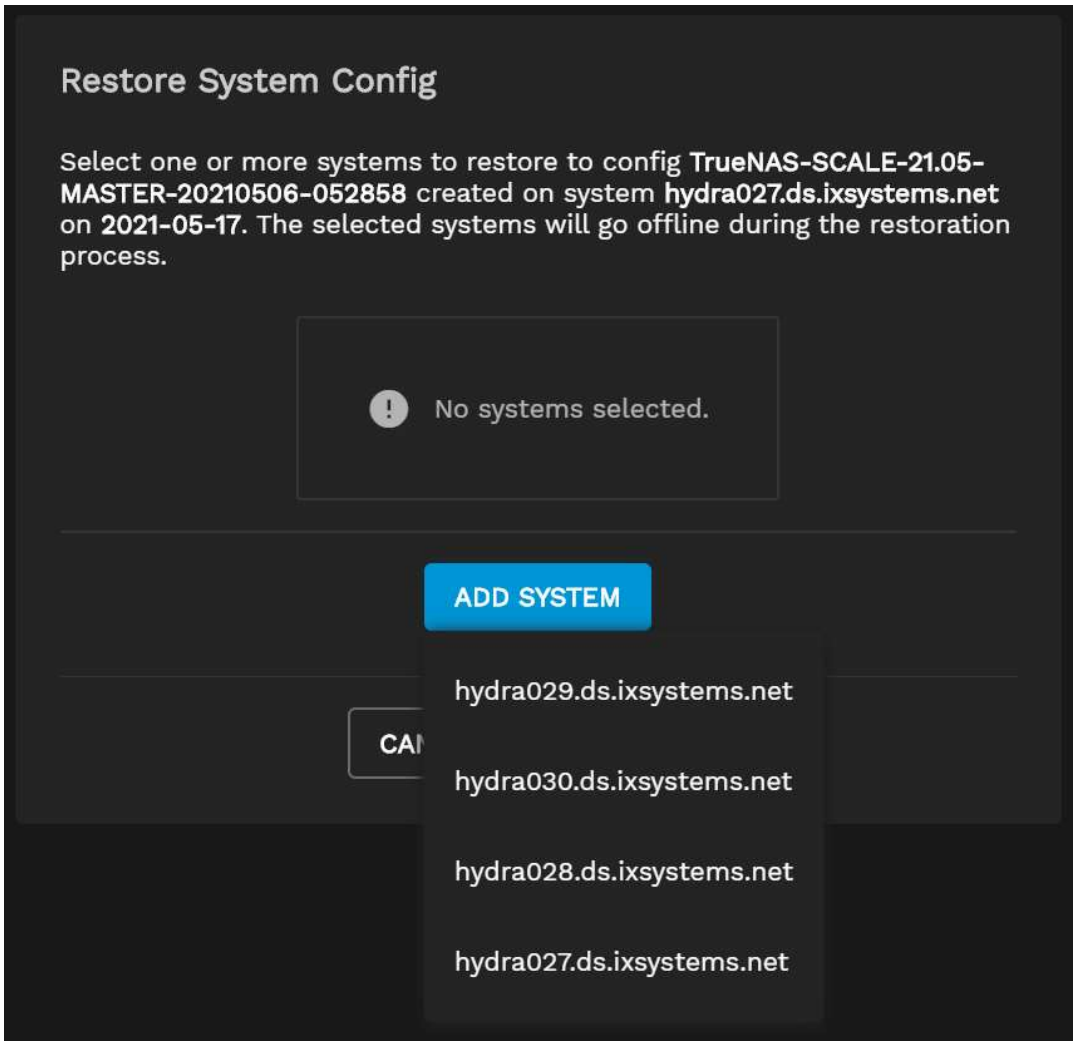
Set the checkbox for the config to restore and click the Restore Icon.



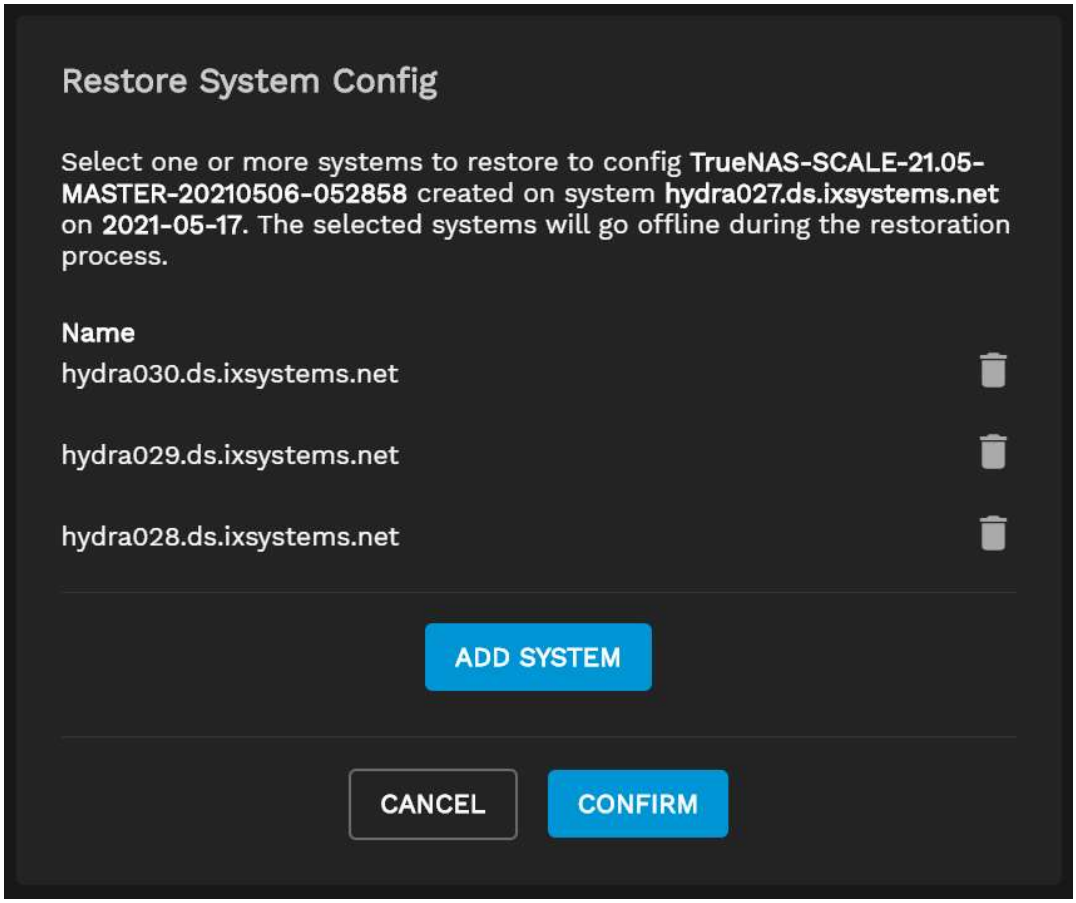
Click **ADD SYSTEM** to select a system that will be restored by the config file.



Additional servers can be added as needed.

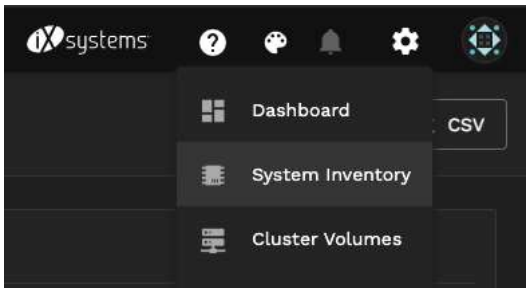


Once the systems have been chosen, click **CONFIRM** to upload the config backup to the selected TrueNAS systems.



System Inventory

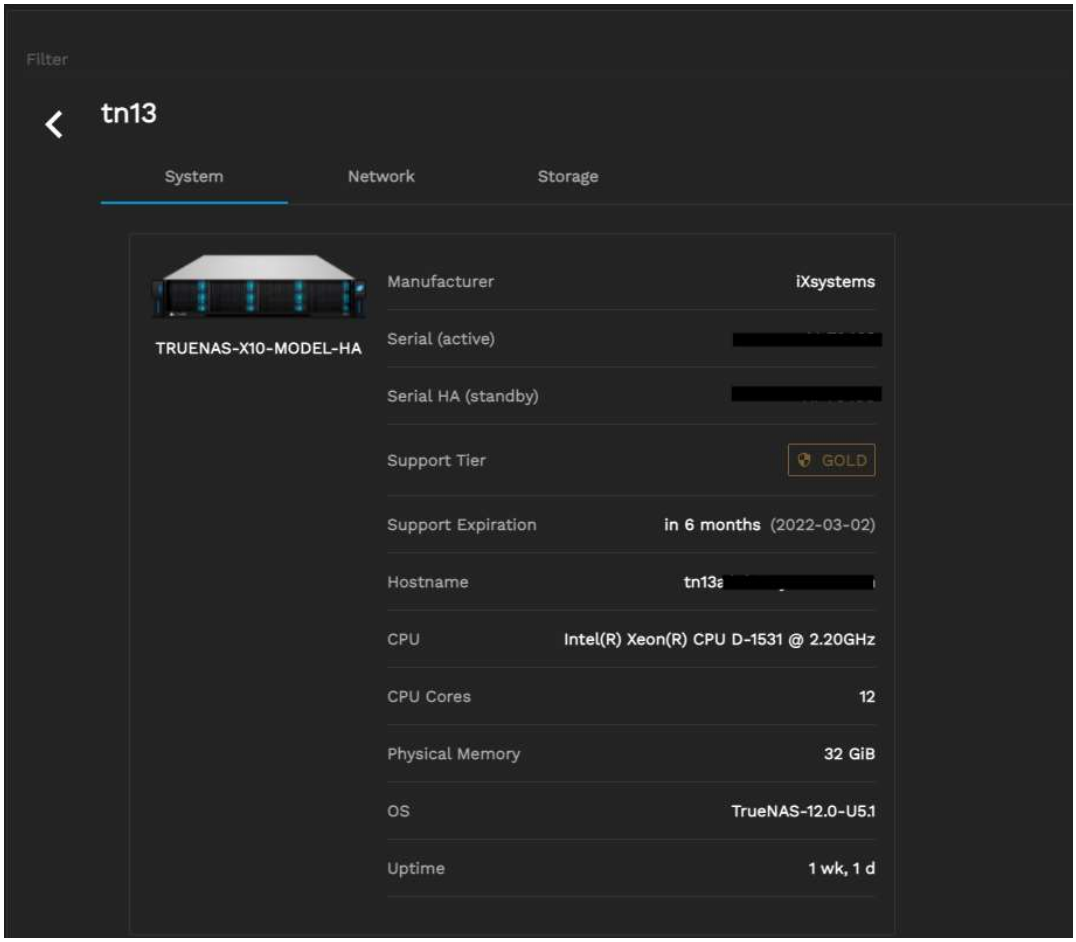
To access the System Inventory page, click the *Gear* icon and Select **System Inventory.**



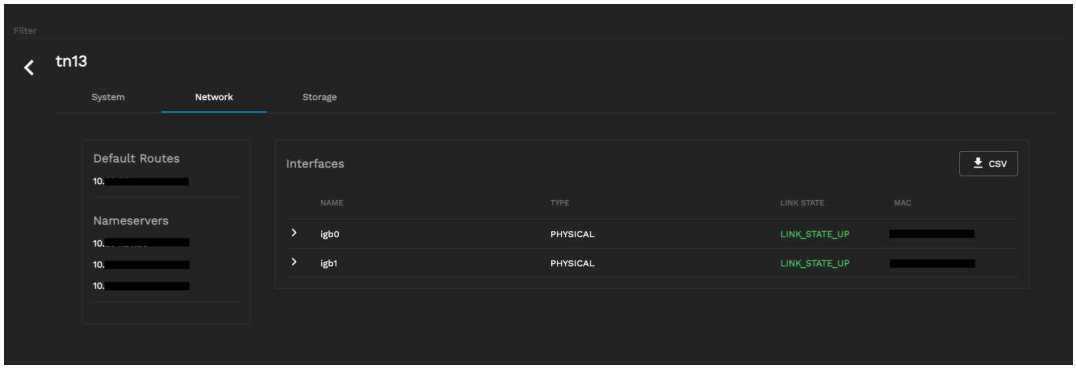
> To download a comma deliminated .CVS file for the current *Inventory* page, click **CVS** in the upper-right area of the screen.

There are three categories of inventory information:

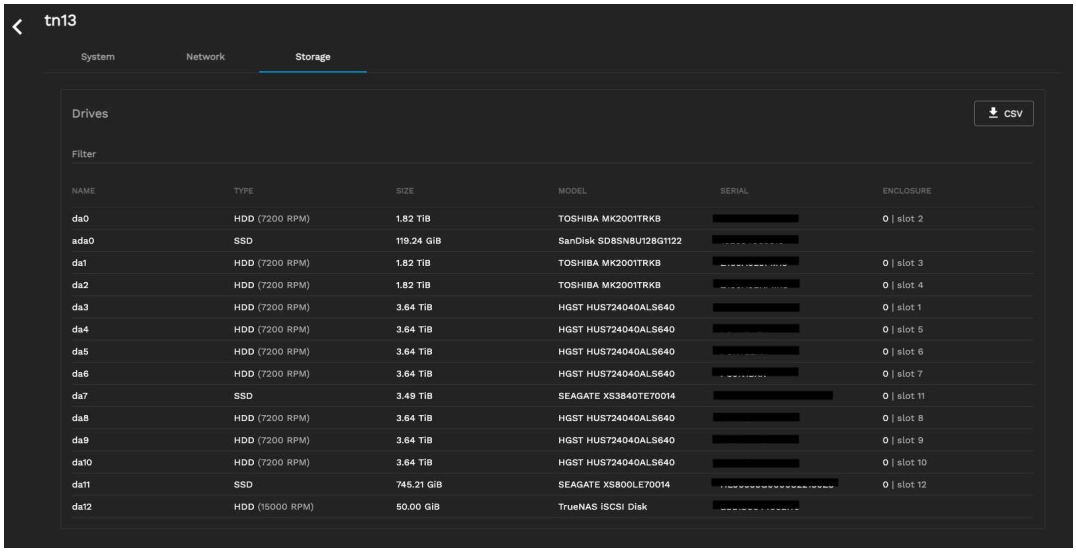
System provides information on the *Manufacturer*, the *Serial* numbers of the controllers, the system's *Support Tier*, the Support Contract's *Expiration* date, the *Hostname* of the active controller, the *CPU*, the number of *CPU Cores*, the amount of *Physical Memory*, what *OS* the system is running, and the *Uptime*.



Network provides information about the *Interface* names, *Type*, *Link State* and *MAC* Address.



Storage provides information about the *Drives* such as *Name*, *Type* of drive, *Size*, *Model*, *Serial* Number, and location in the *Enclosure*.



iSCSI Management

When creating an iSCSI Volume with TrueCommand, the volume can be configured on multiple systems at the same time. Refer to the iSCSI section for more information.

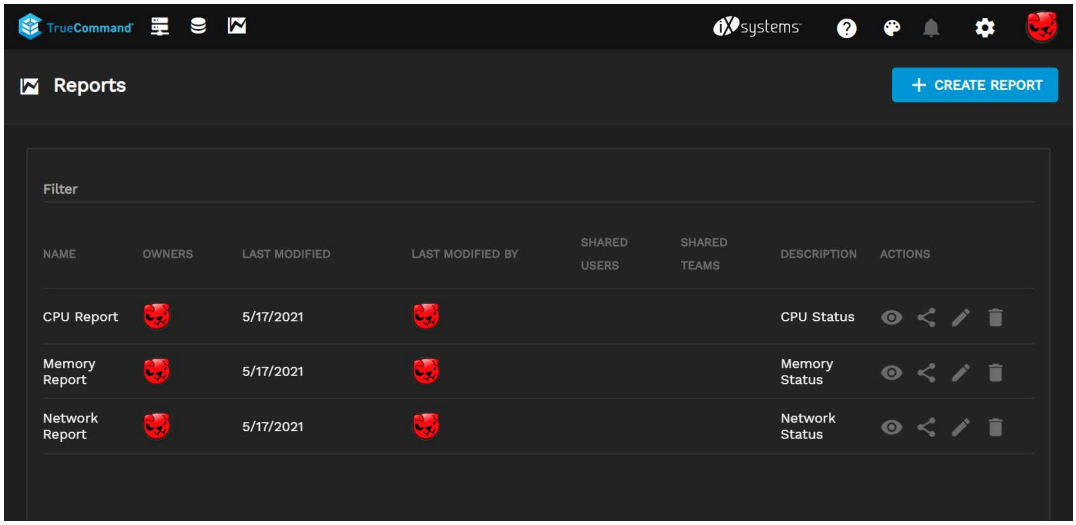
Cluster Managemnet

By definition, clusters span across multiple systems. TrueCommand instances that are connected to three or more TrueNAS SCALE systems can create clustered volumes. Refer to the Clustering section for more information.

6 - Reports

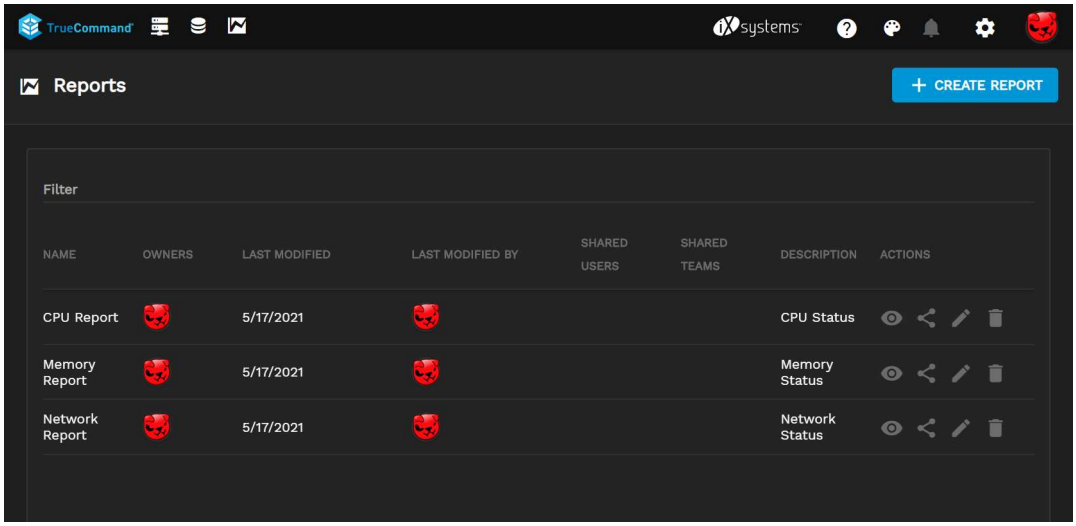
TrueCommand users can create reports and share them with other TrueCommand users. We designed default reports that generate a basic system overview chart. Default reports show details like network traffic, storage, and the chosen system's memory utilization.

Users must have access to the analyzed systems to view their reports.



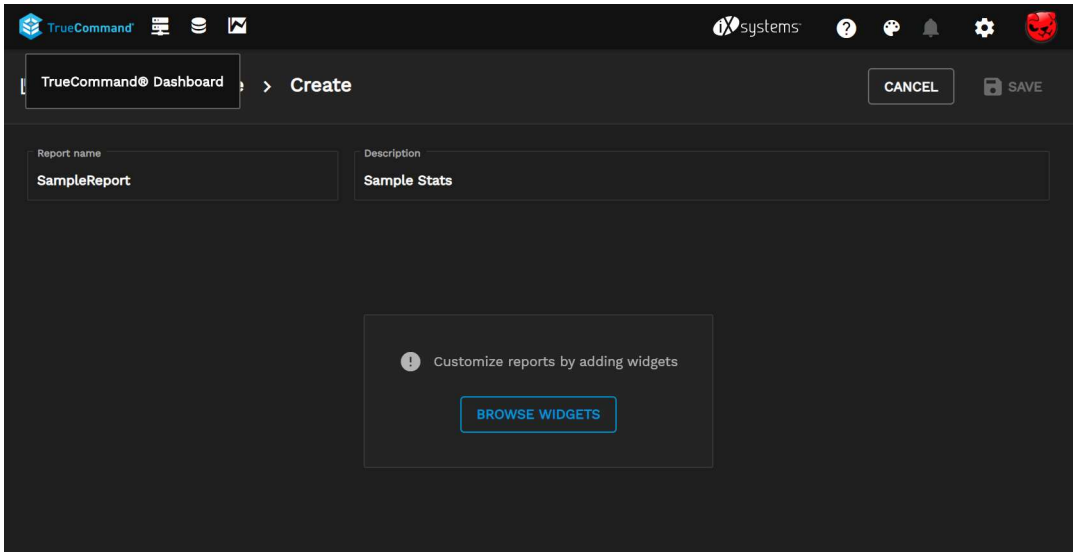
6.1 - Creating a Report

The **Reports** page customizes system metrics charts for data analysis.

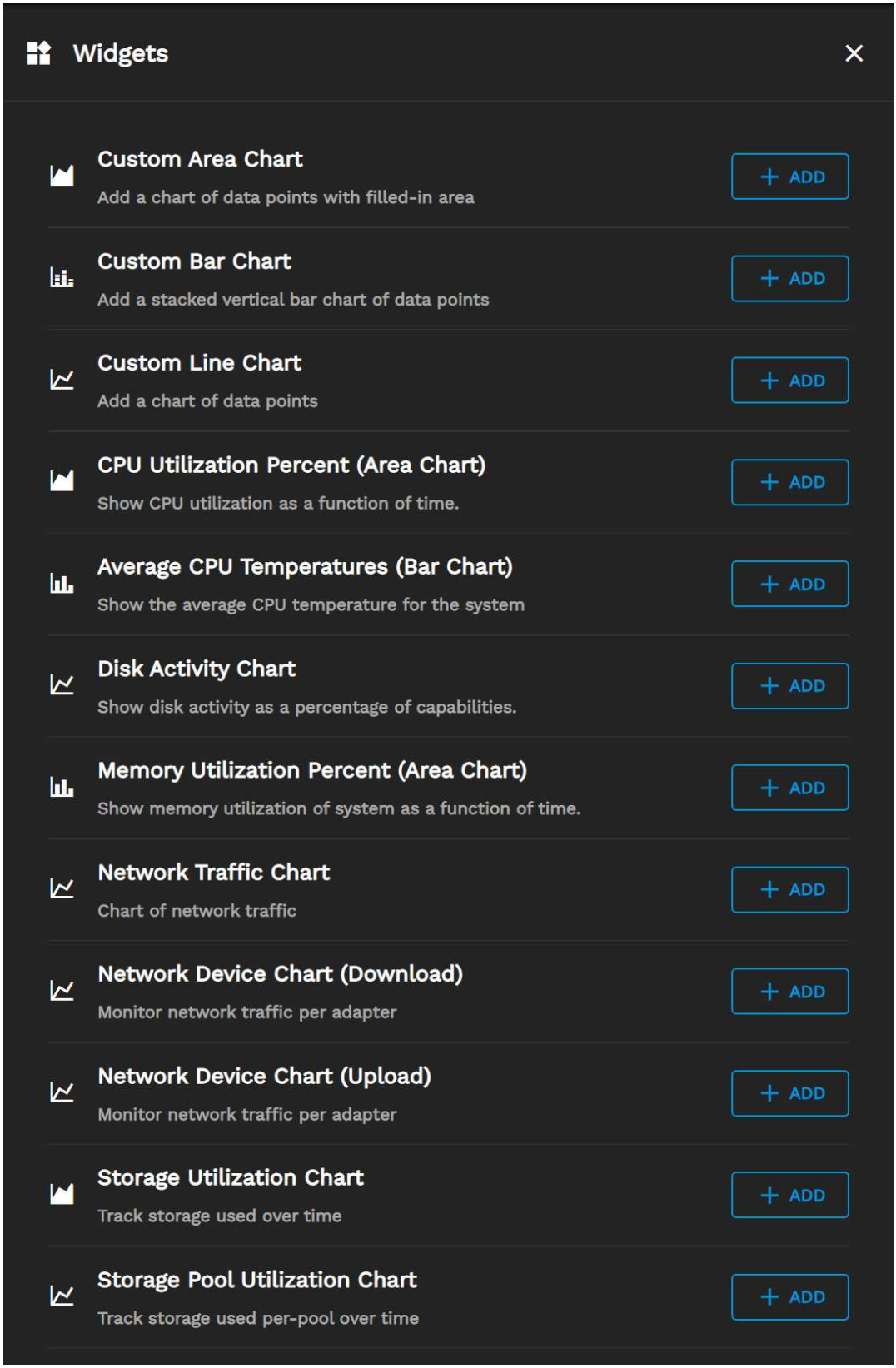


Creating a Report

Click + *CREATE REPORT* to create a customizable report. Enter a report name and an optional description for the report.



Click *BROWSE WIDGETS* or *WIDGET* to add charts to the report.

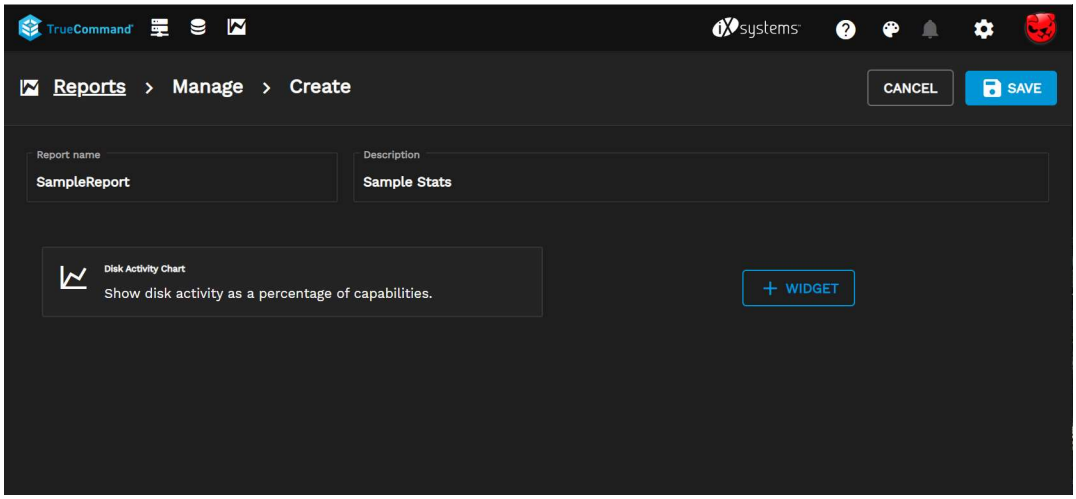


Custom Charts

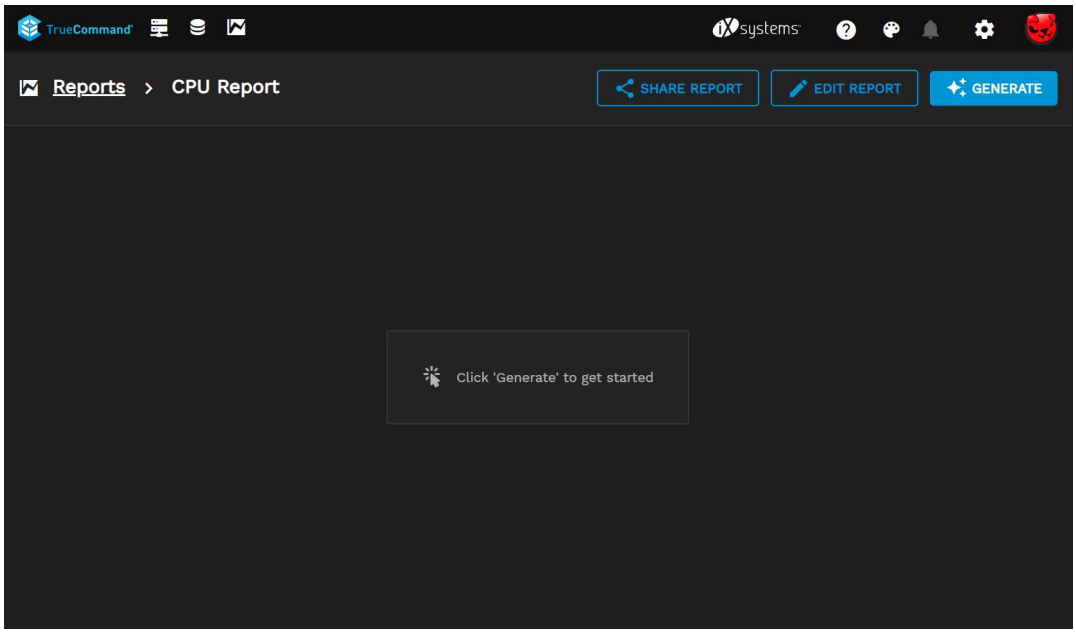
Most charts are already configured to report certain settings. To create a custom chart with custom settings, add a *Custom Area Chart*, *Custom Bar Chart*, or *Custom Line Chart*. Fill in these options when adding a custom chart:

- General settings: Enter a Title, Subtitle (optional), Axis label (optional), Point size, Line size, Y min (optional), and Y max (optional) for the chart. `Stack the values` can be set to bring data points on the chart closer together. This setting is useful for charts that have many different data points at the max Y value.
- Data sources: Add data sources to the chart by expanding a category and selecting appropriate sources. Multiple data sources can be added to one chart.
- Summary: This step shows the all of the chosen values. Click *SAVE* to add the custom chart to the report or *BACK* to go back and change a setting or data source.

After adding charts to the report, click **SAVE** to make this report available for use.

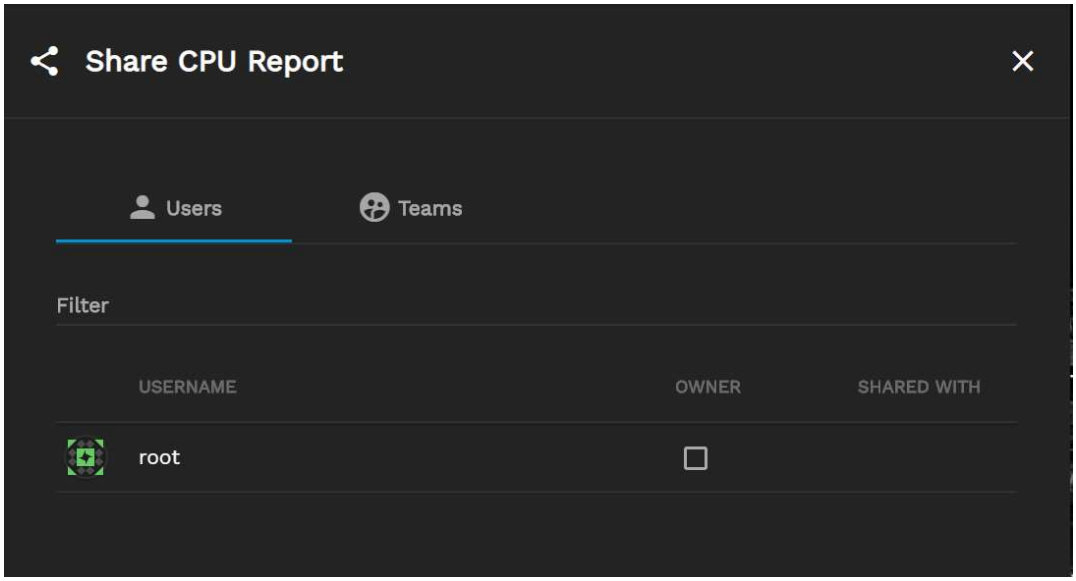


After creating a report, you can click **GENERATE** to generate the report or you can go back to the reports page and make create another report.



Share Report

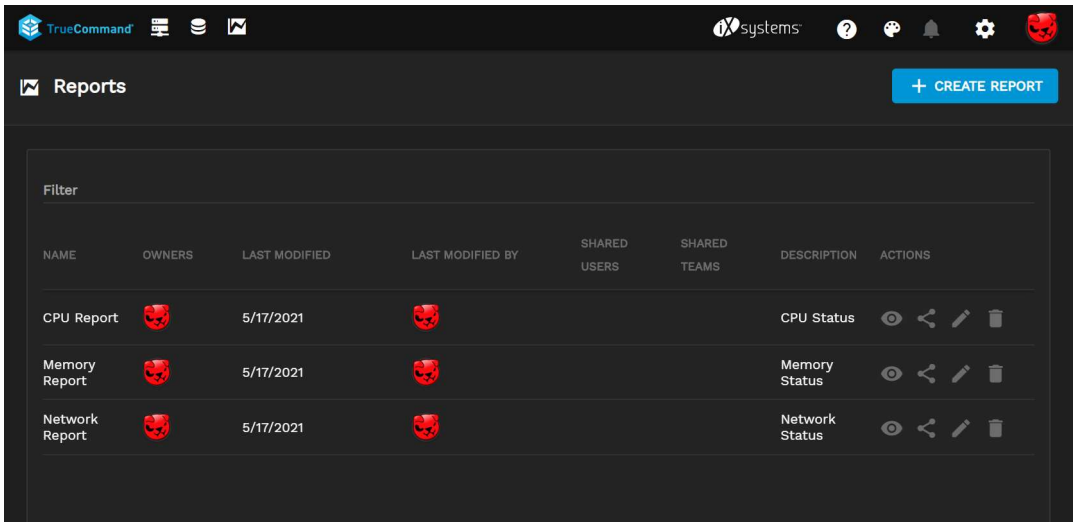
By default, the reports created by a user are available only to that user. To share a report with other users or teams, open the Reports page and click the icon for the chart.



You can share reports with individual users or entire teams.

6.2 - Generating a System Report

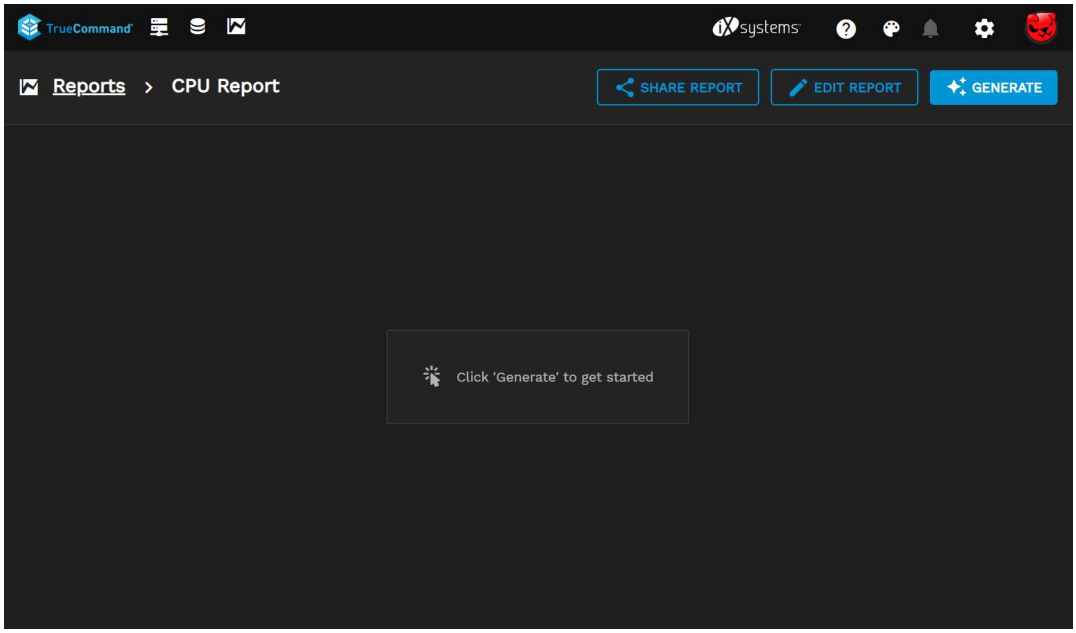
The **Reports** page customizes system metrics charts for data analysis.



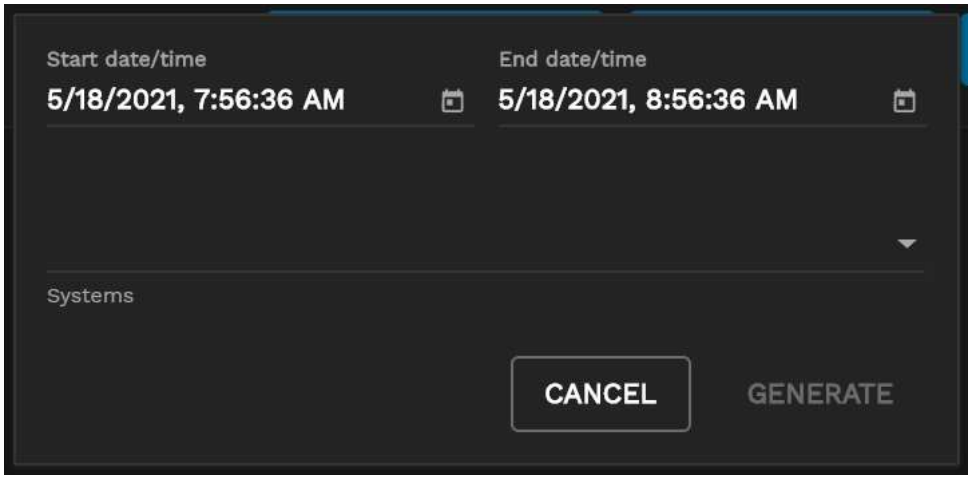
You must create a report before you can run the report.

Generating a report

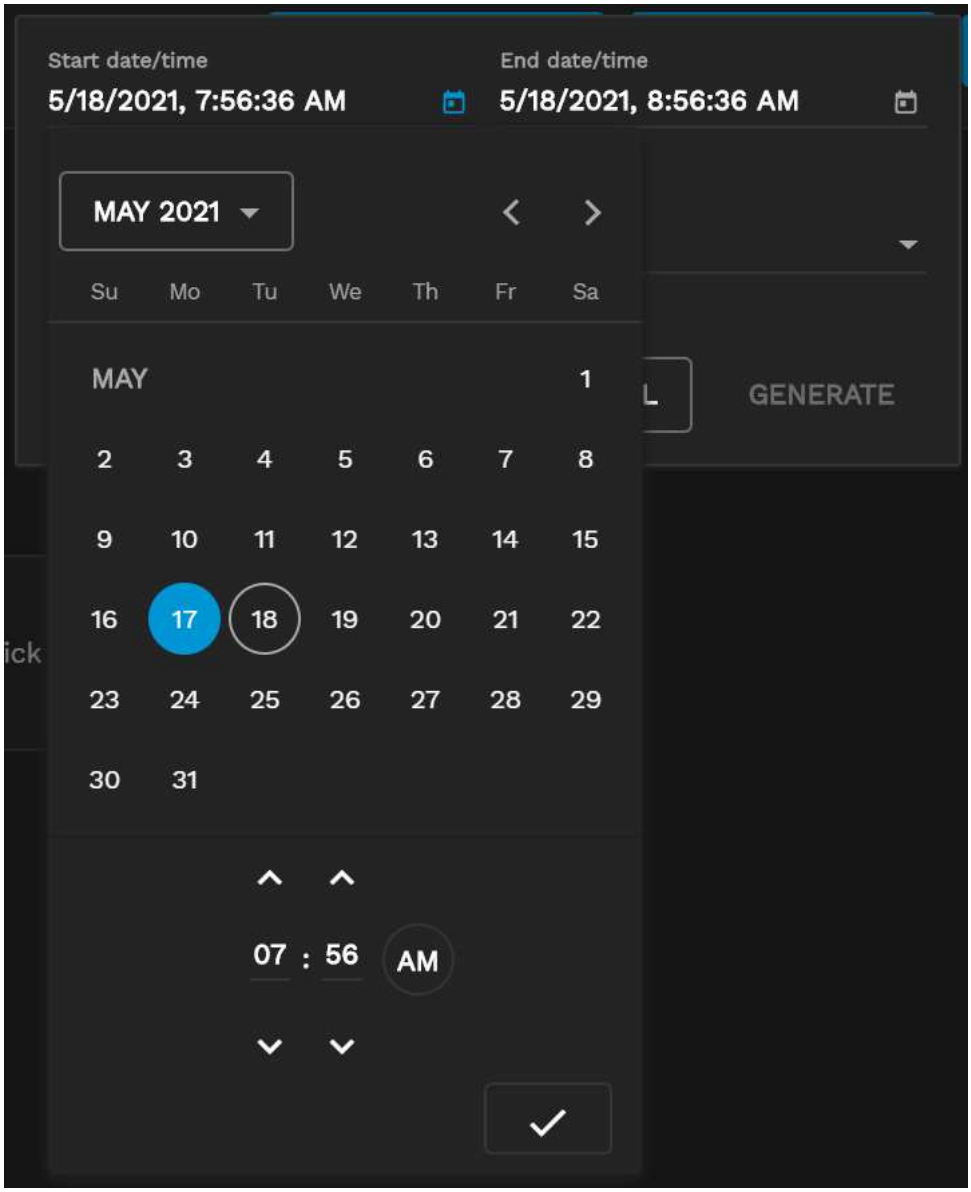
To generate a report click the (eye) icon to launch the Generation Page.



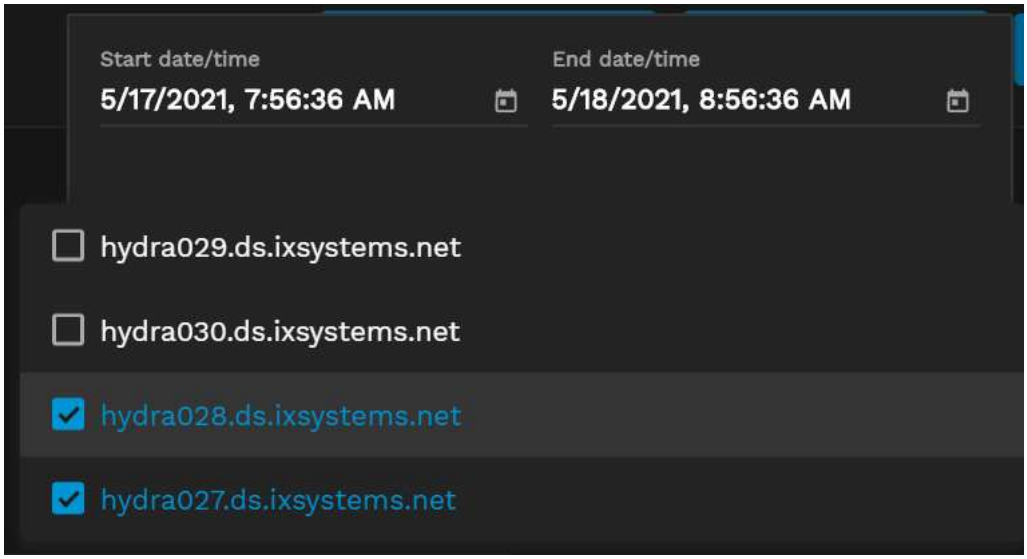
Click **Generate** to open the date and system selection window.



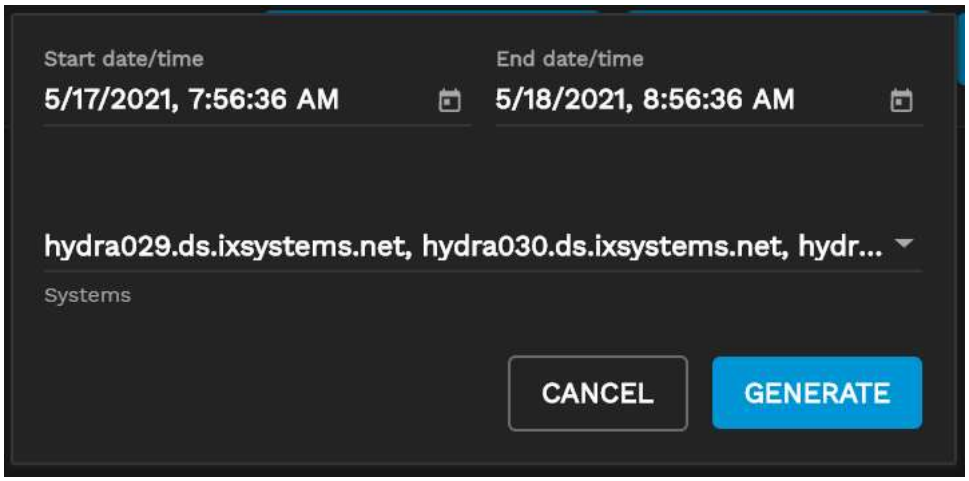
Select the beginning and end dates for the report using the dropdown.



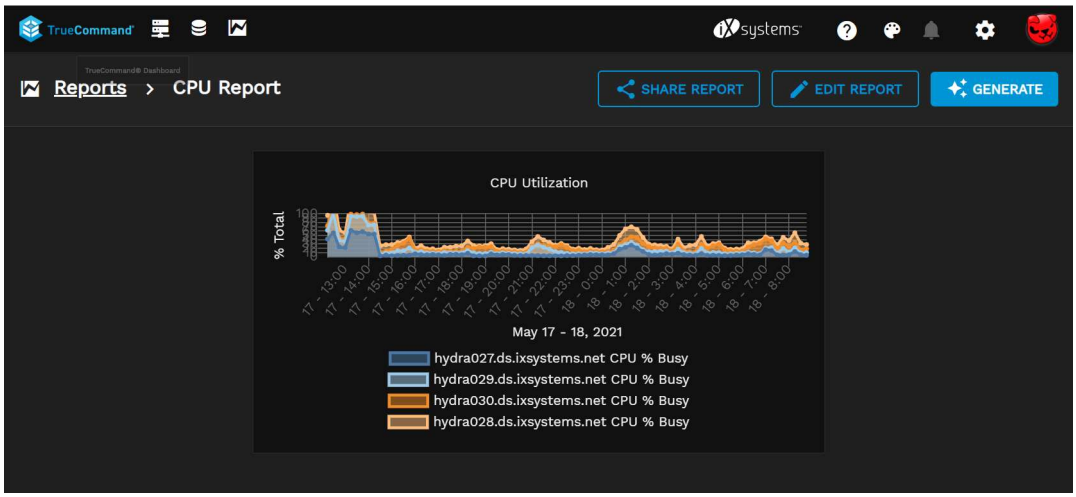
Once the date range is set, use the dropdown to select which systems you want included in the report.



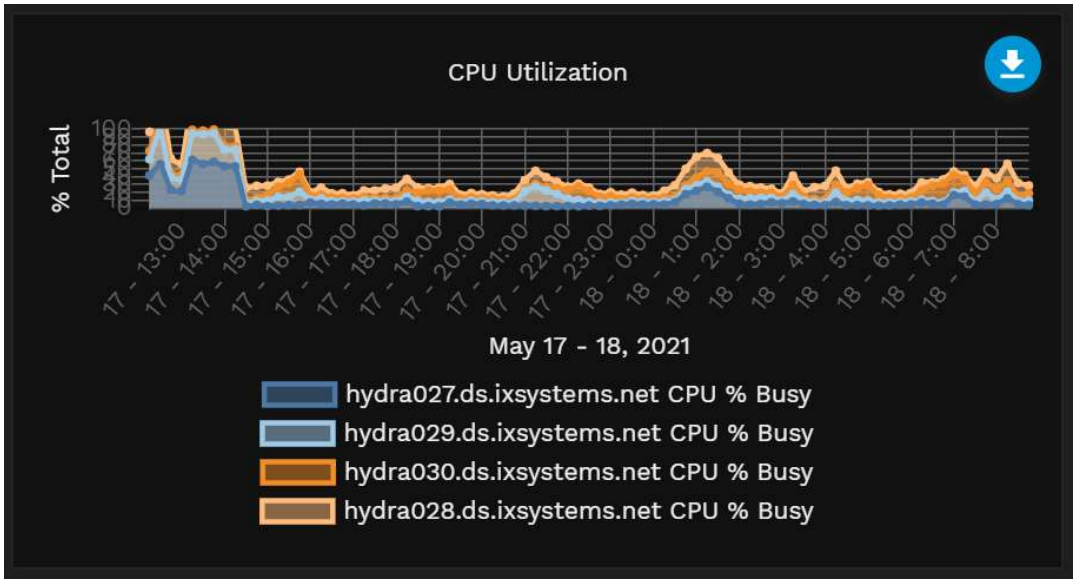
With the systems selected, click **Generate**



The report will be generated and the graph will appear.



To download the report metrics, hover your mouse over the report and click the blue down arrow that will appear. This downloads the data in JSON format.


CPU Utilization
% Total
100
17 - 13:00
17 - 14:00
17 - 15:00
17 - 16:00
17 - 17:00
17 - 18:00
17 - 19:00
17 - 20:00
17 - 21:00
17 - 22:00
17 - 23:00
18 - 0:00
18 - 1:00
18 - 2:00
18 - 3:00
18 - 4:00
18 - 5:00
18 - 6:00
18 - 7:00
18 - 8:00
May 17 - 18, 2021
hydra027.ds.ixsystems.net CPU % Busy
hydra029.ds.ixsystems.net CPU % Busy
hydra030.ds.ixsystems.net CPU % Busy
hydra028.ds.ixsystems.net CPU % Busy

7 - Alerts

TrueCommand allows for user notification based on custom defined alerts for connected TrueNAS systems. Method of alert notifications as well as theming of alerts in the TrueCommand interface can be user customized.

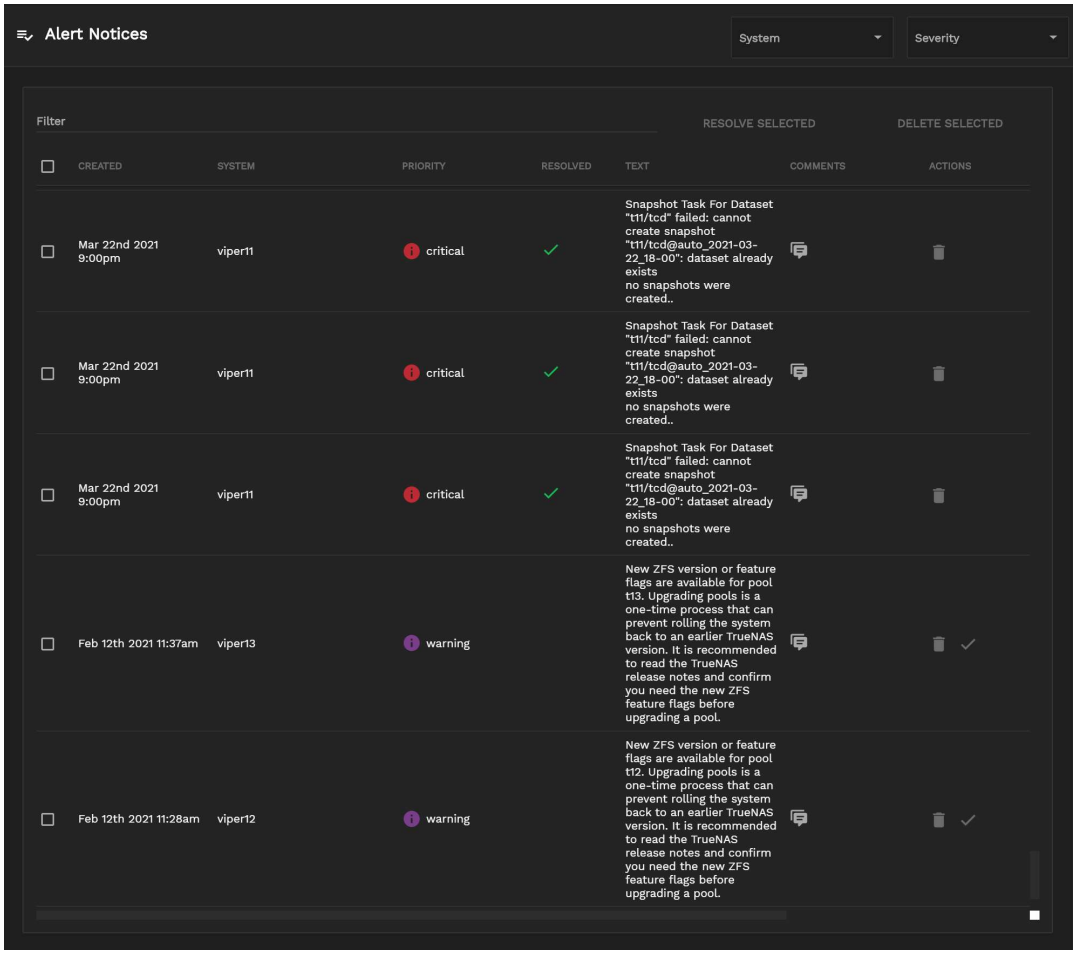
Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the **<** symbol to expand the menu to show the topics under this section.

7.1 - Alert Management

TrueCommand alerts provide visual warnings for monitored systems that require attention. Alerts are either generated by the monitored system or an alert rule created in TrueCommand.

Viewing All Alerts

To see all alerts that TrueCommand has discovered, open the **Configure** menu and click **All Alerts**. Administrator accounts can see all generated alerts. A non-administrator account can only view alerts according to their team and user account permissions.



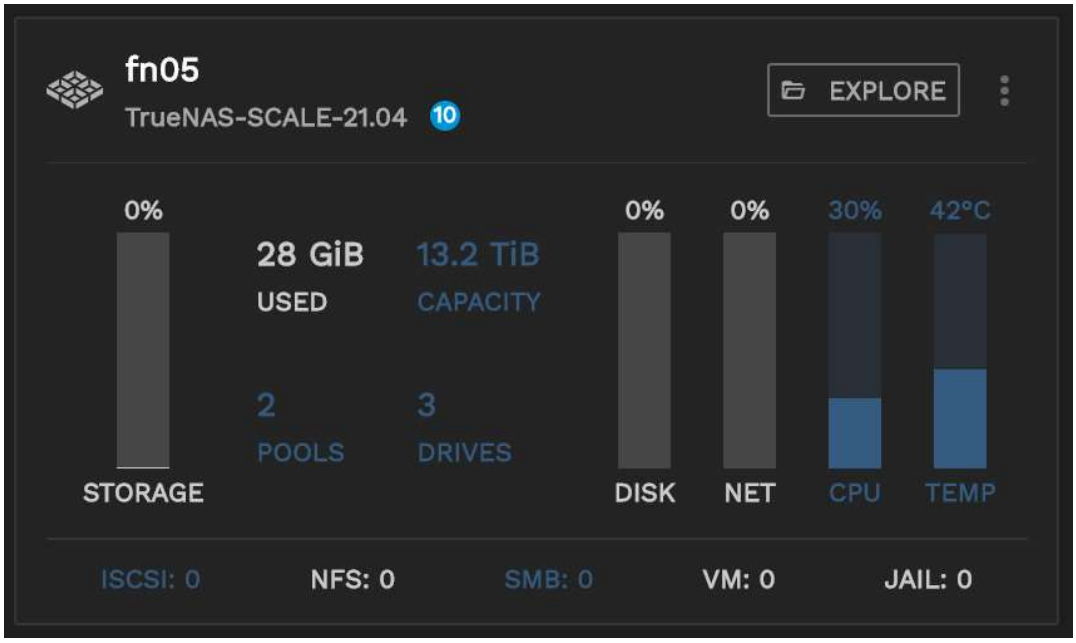
The **Active Alerts** tab shows all unresolved alerts. Alerts are moved to the **Resolved Alerts** tab by clicking *Resolve* Selected ✓.
To resolve multiple alerts, select each alert and click *Resolve* Selected ✓.

Click *View alert notice details (i)* to view any user comments about an alert.

Administrator accounts can delete an alert by clicking *Delete* Selected 🗑. Deleting an alert cannot be undone. To delete multiple alerts, select each alert and click *Delete* Selected 🗑.

Viewing Alerts by System

Alerts generated by a monitored system display in both the administrative **Systems** screen and the **Dashboard** as a number above the system icon. To view all alerts for a single system, go to the **Dashboard** and select a single system.

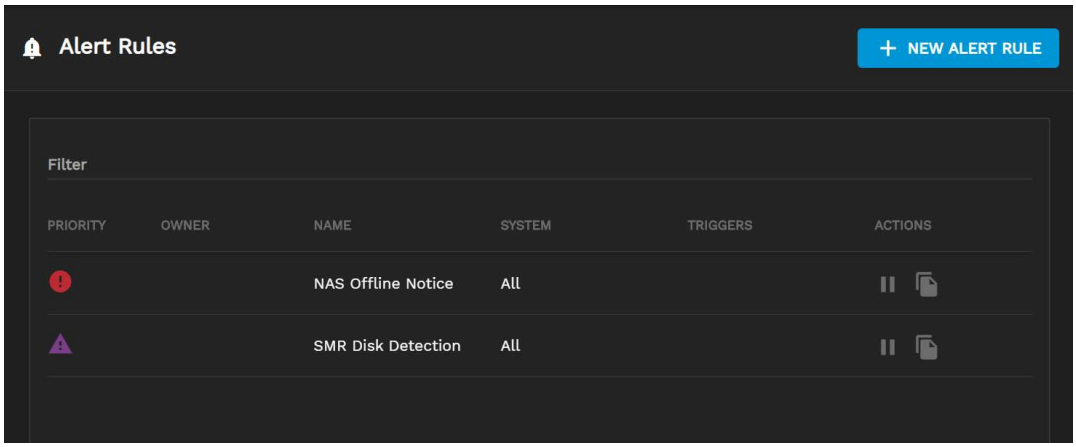


Each active and resolved alert for that system is visible in this tab. Clicking *View alert notice details (i)* shows details for that alert, including the option to leave comments about the alert.

Managing Alert Rules

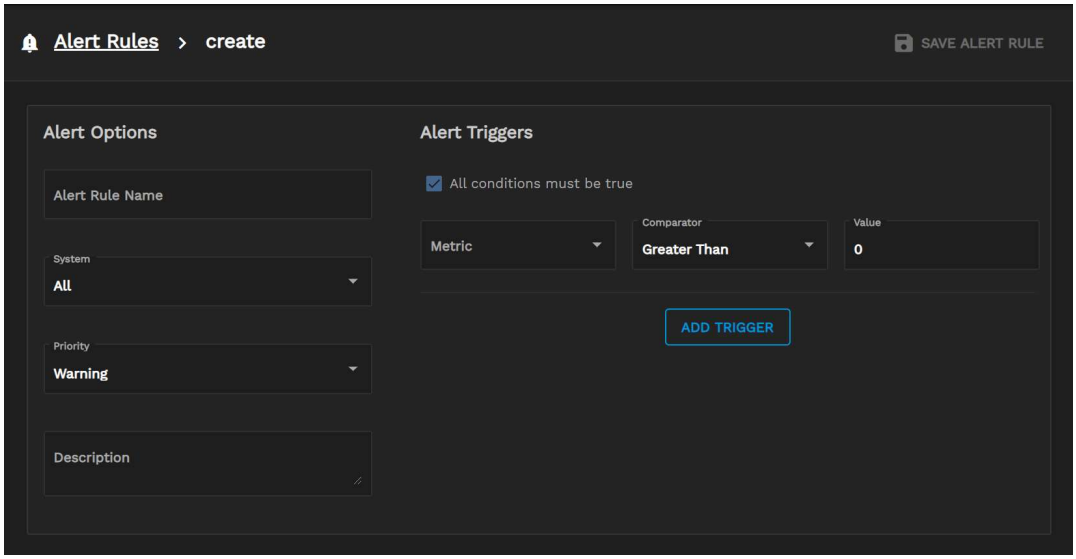
Alert rules generate alerts in TrueCommand. TrueCommand has several default rules built in. TrueCommand administrators and team members with the appropriate permissions can create new alert rules.

To view all TrueCommand alert rules, open the **Configure** menu and click **Alert Rules**.



Details about each TrueCommand alert rule are shown on this page, including which user account created the rule. Users can activate, suspend, edit, or delete alert rules using either an administrator account, or the account that created the rule.

Users can create new TrueCommand alert rules to monitor a wide variety of system information and generate a TrueCommand alert if specific conditions occur. To create a new alert rule, click + *NEW ALERT RULE* and follow the creation wizard:

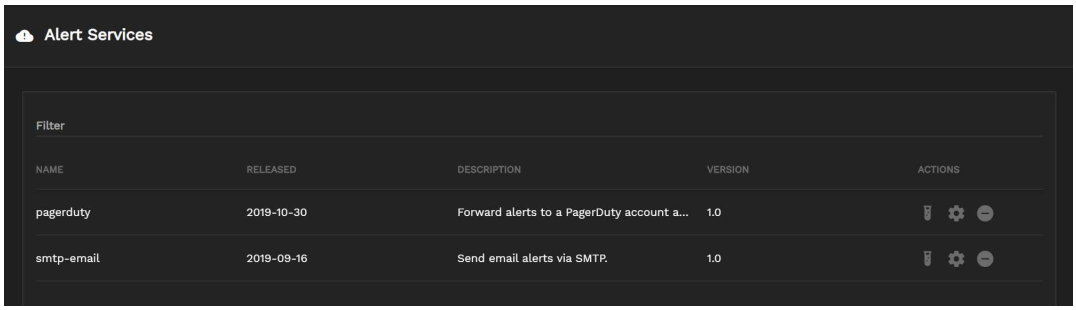


- Select a System: The rule will apply to these systems. Appropriate system permissions are required for non-administrative user accounts.
- Select a Data Source: Choose a data source for the rule. This is the type of information that can trigger an alert. For example, choosing *cpu_temp* means the alert rule monitors the temperature of the chosen system.
- Type and Threshold: Create the rule conditions:
  - Data type: This is the specific data TrueCommand will monitor. The options change depending on the **Data Source**.
  - Priority level: Choose *Information*, *Warning*, or *Critical*. This determines the category of alerts generated by this rule.
  - Comparison type: A conditional statement that applies to the **Data type** and the **Comparison value**.
  - Comparison value: Enter a value appropriate to the options scenario and options selected. This can act as a threshold or limitation on when an alert is generated by the rule.
- Finished: To create the new alert rule, click **CREATE ALERT**. To start over, click **RESET**.

Configuring Alert Services

> Configurable Alert Services are only available for local installations or containerized TrueCommand deployments. TrueCommand Cloud instances are preconfigured to use email alerts; PagerDuty is not an option.

TrueCommand uses different services to expand how alerts are communicated to individual users or administrators. Individual user accounts can use these services to manage how that account is notified of an alert. To configure an alert service plugin, open the **Configure** ⚙ menu and click **Alert Services**.



Each plugin has three options.

: Sent Test Alert

⚙ : Configure Plugin

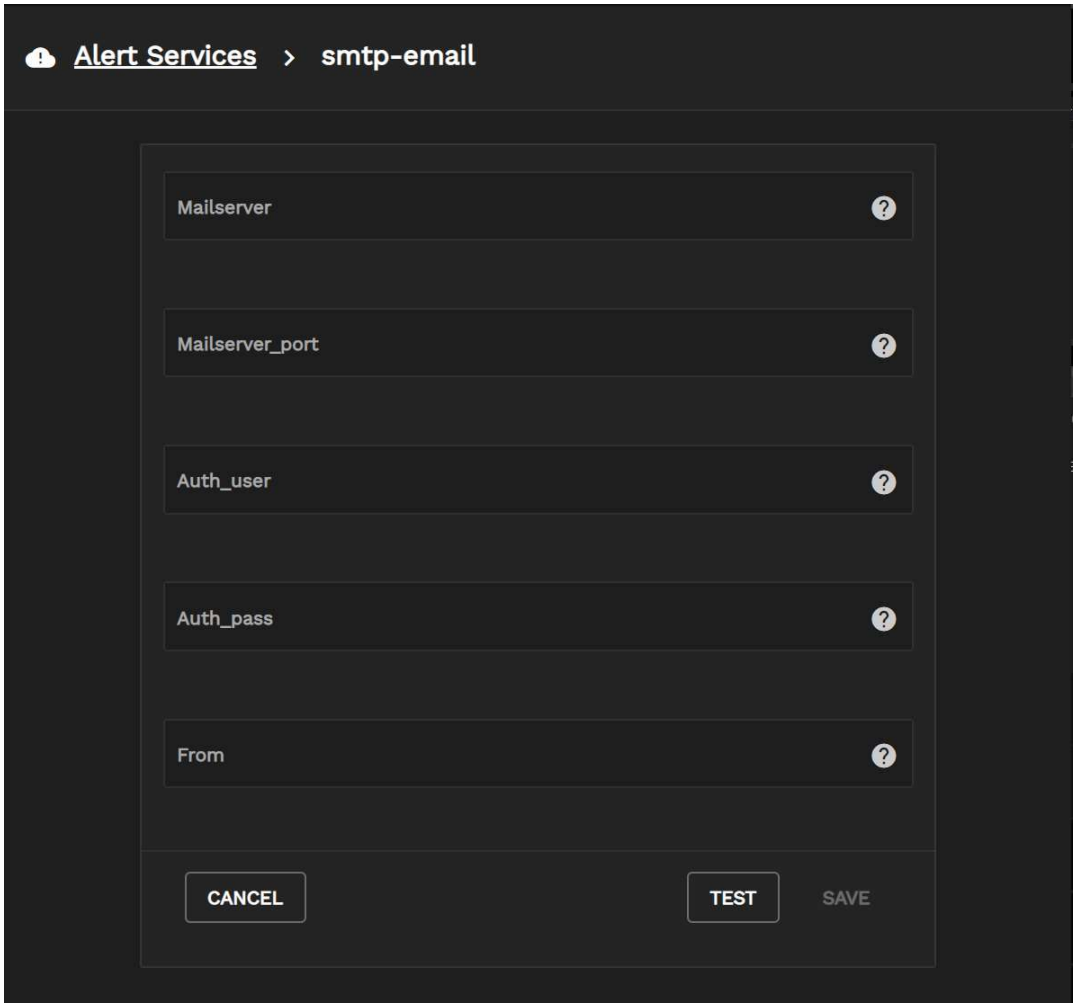
⊖ : Clear Plugin Configuration

Email

Before proceding, verify that the sending mailserver has TLS enabled.
TrueCommand cannot send emails through a mailserver without TLS.

> An email address must exist on the users profile page to recieve emails.

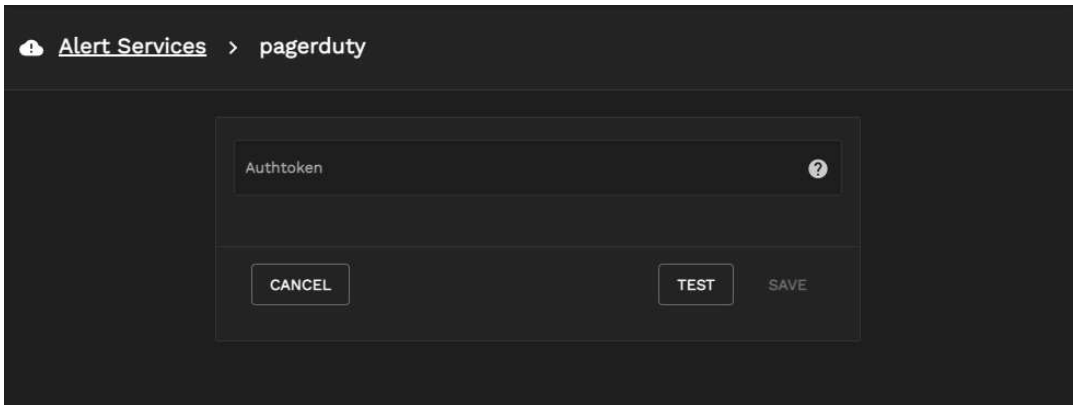
Enter the mailserver and port along with the user and password for the email account to be used. The *From* field allows you to customize the sender field of the email. For a *No-Auth* SMTP configuration, leave the password field blank.



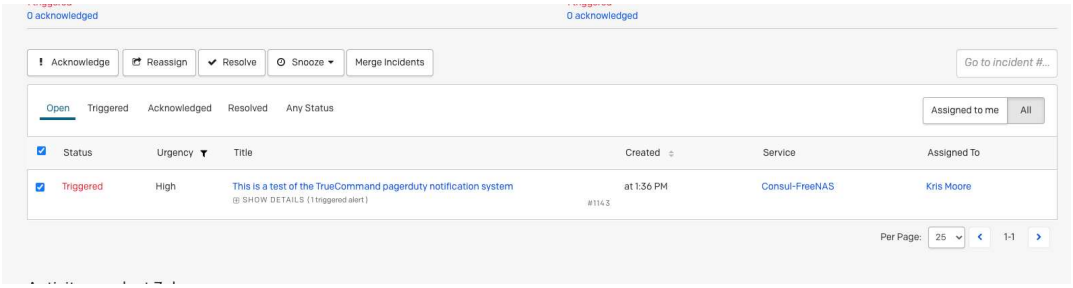
Click **Test** to verify that the configuarion is correct. If you did not receive a test alert email, check the values entered for accuracy.

PagerDuty

Open the **Configure Plugin** for PagerDuty. In the *Authtoken* section, enter your **Service Integration Key from PagerDuty**. If you have an active subscription with PagerDuty, this key should be available to you. Enter a *Title for incident reports* if desired. Click *TEST*.

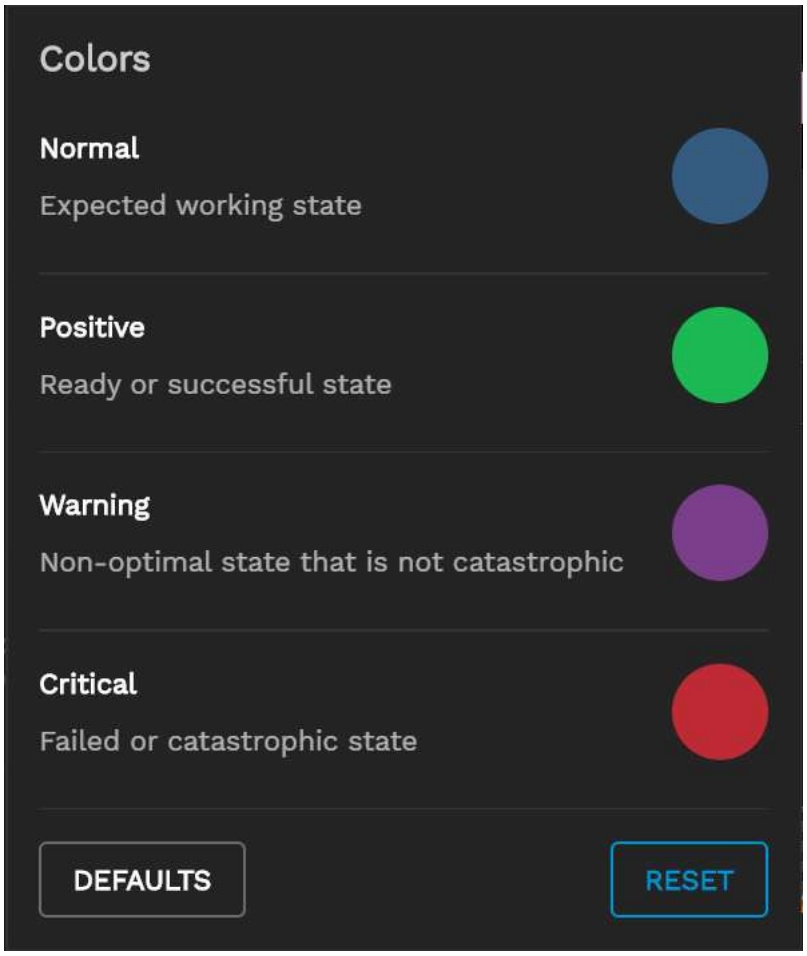


Login to your PagerDuty account and check for open incidents. There you should see the triggered test alert from TrueCommand. If you did not receive a test alert, check the **Service Integration Key from PagerDuty** for accuracy in the plugin configuration section of the alert service.

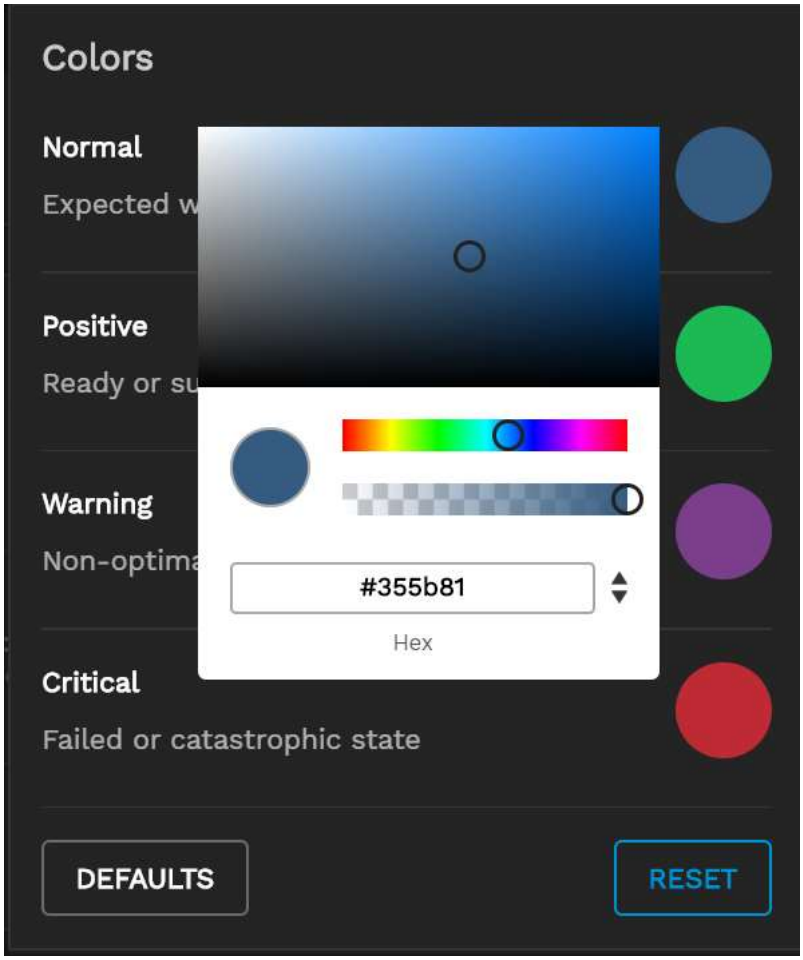

0 acknowledged
0 acknowledged
Acknowledge
Reassign
Resolve
Snooze
Merge Incidents
Go to incident #...
Open
Triggered
Acknowledged
Resolved
Any Status
Assigned to me
All
Status
Urgency
Title
Created
Service
Assigned To
Triggered
High
This is a test of the TrueCommand pagerduty notification system
SHOW DETAILS (1 triggered alert)
#1143
at 1:36 PM
Consul-FreeNAS
Kris Moore
Per Page:
25
1-1

7.2 - Colors

TrueCommand includes the ability to customize the alert colors to user preferences. The Theme pallet is located in the top banner on the right. To open the theme configuration menu, click the icon.



To change a color, click on the color to open a selection menu. Select the desired color or enter its HEX color value.



To remove changes and revert to the currently saved settings, click *Reset*. To reset all colors to the application defaults, click *Defaults*.

8 - Clustering

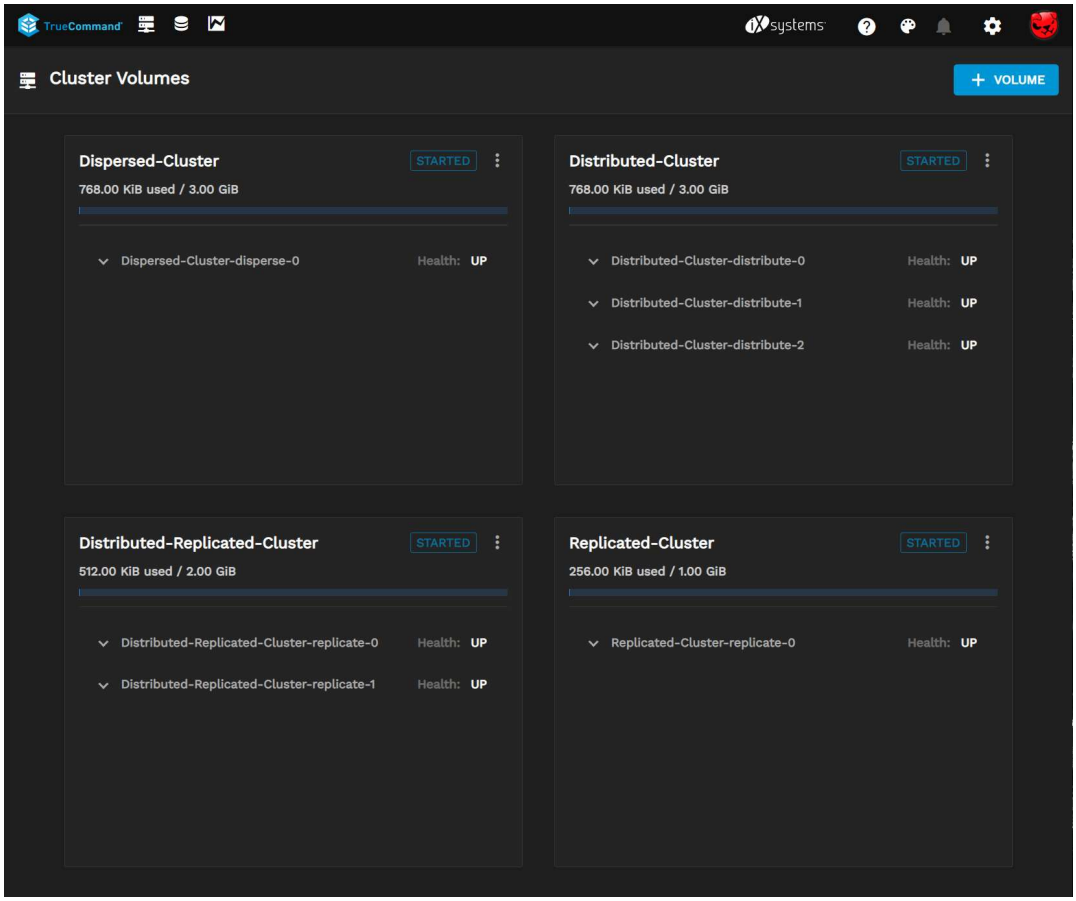
TrueCommand 2.0 in conjuction with TrueNAS SCALE has the ability to create clustered Volumes that span across multiple volumes.

There are five volume types:

- Replicated
- Distributed
- Dispersed
- Distributed Replicated
- Distributed Dispersed

> Cluster Volume management is a BETA feature in TrueCommand 2.0. Before attempting to use such features, please ensure that your data is backed up. Do not rely on this for critical data.

> Distributed Dispersed Volumes are not implemented at this time.



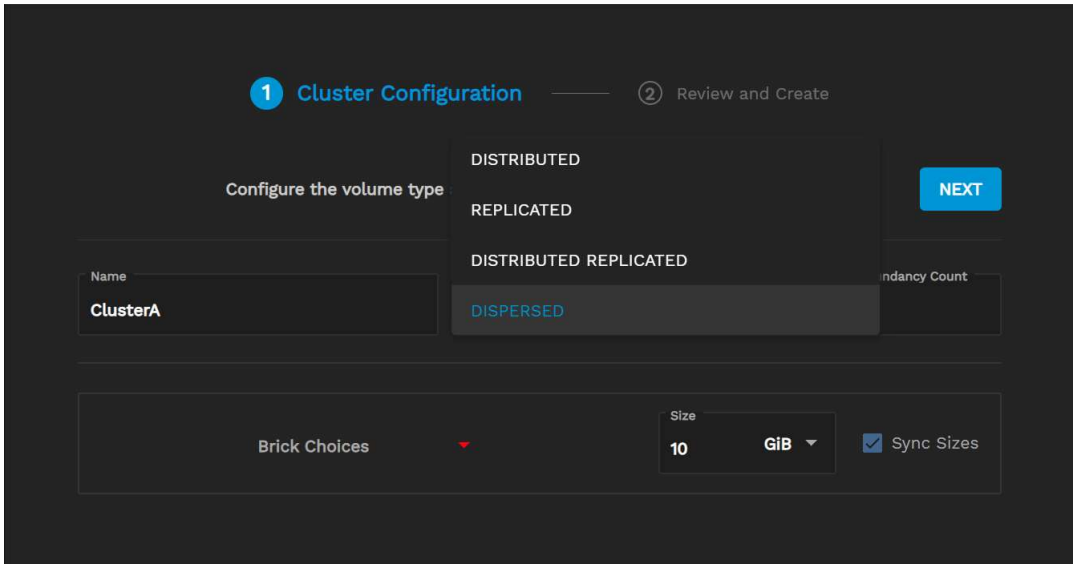
8.1 - Creating Clustered Volumes

Cluster Volume management is a BETA feature in TrueCommand 2.0. Before attempting to use such features, please ensure that your data is backed up. Do not rely on this for critical data.

Gluster requires TrueNAS systems to have a static IP. TrueNAS with DHCP enabled can not be part of a Cluster Volume.

To create a Cluster Volume, click the Cluster Volume button in the top left of the dashboard or the Cluster Volume button in the Settings Menu dropdown.

Once the Cluster Volumes page has loaded click **Create.** Name the Cluster, select the type in the *Volume Type* Drop down, and set the redundancy level.

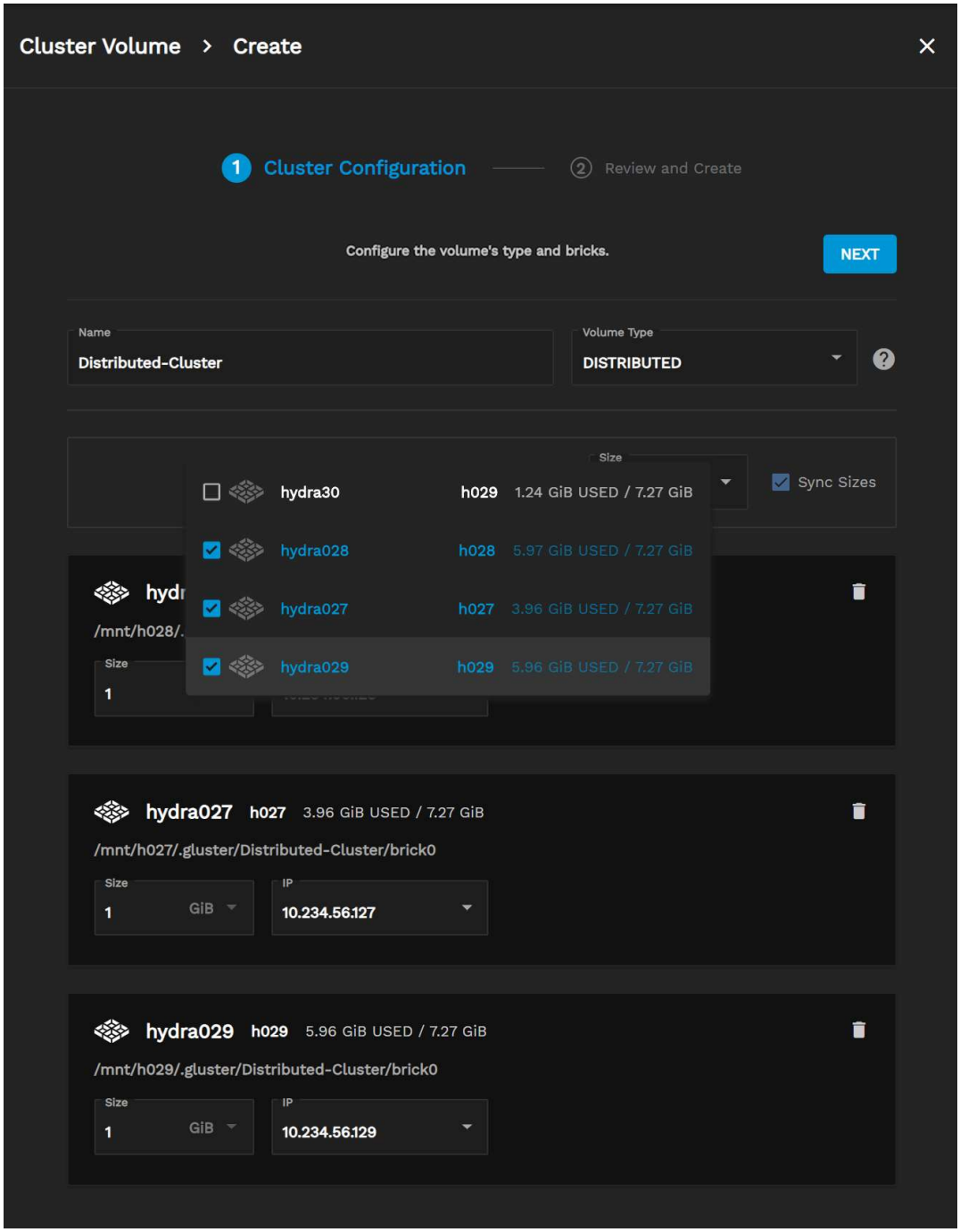


There are five types of Clustered Volumes.

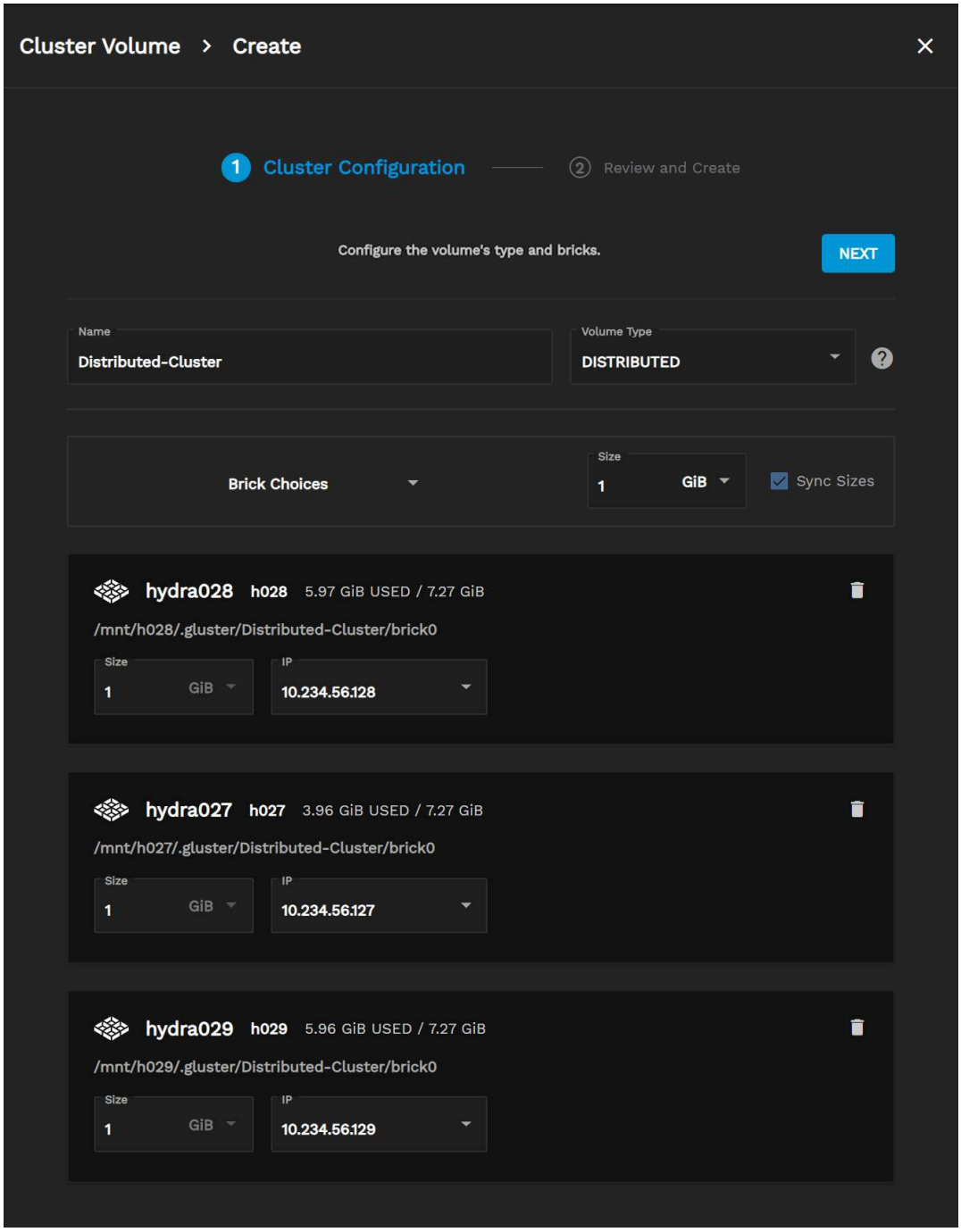
Distributed

In a Distributed Volume, files are distributed across the various bricks in the volume. File-A may be stored only in Brick-1 or Brick-2 but not on both. As a result, there is no data redundancy. The purpose for a Distributed Volume is to easily & cheaply scale the volume size. Warning: This means that a brick failure will lead to complete loss of data.

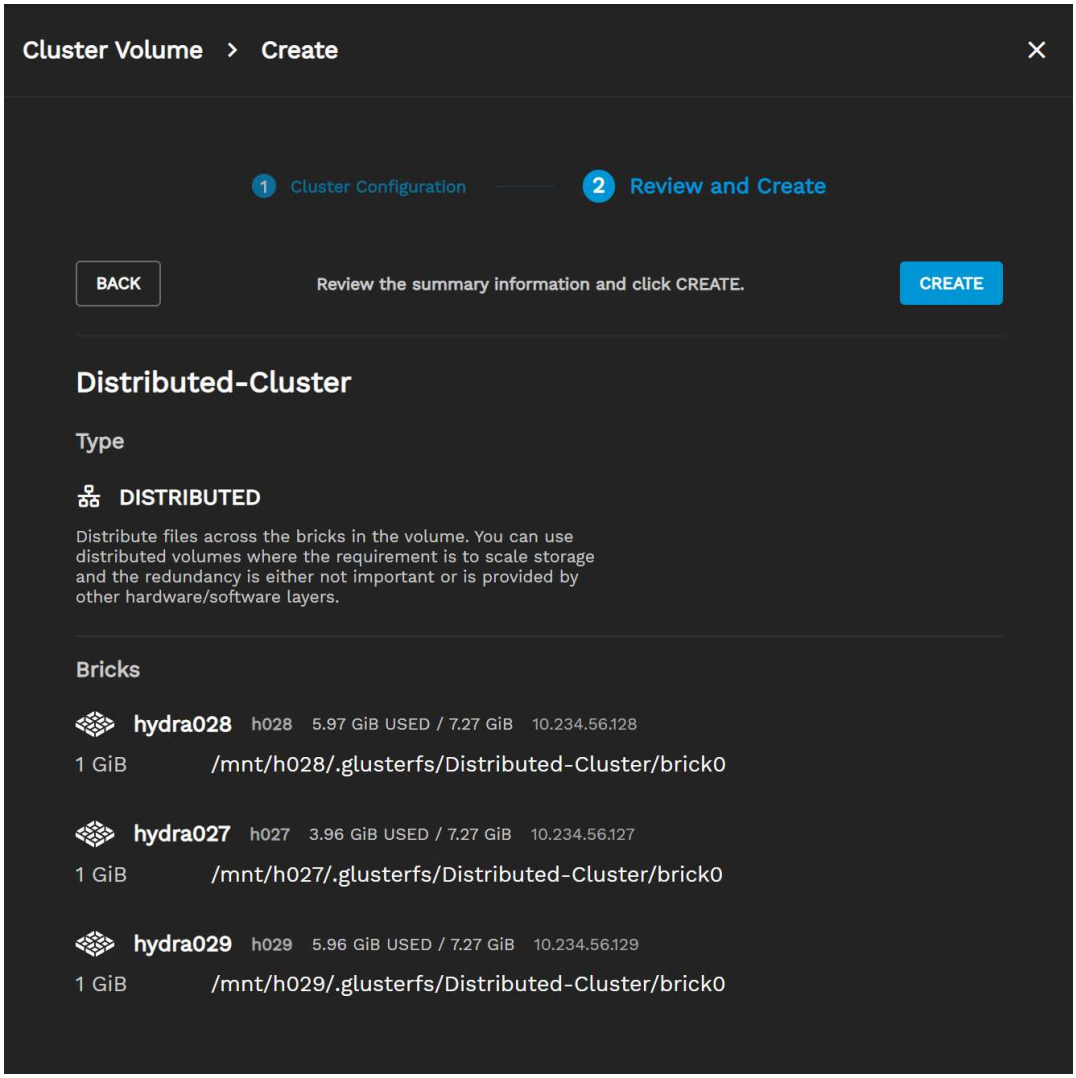
Click the *Brick Choices* drop down and check the locations to use for bricks.



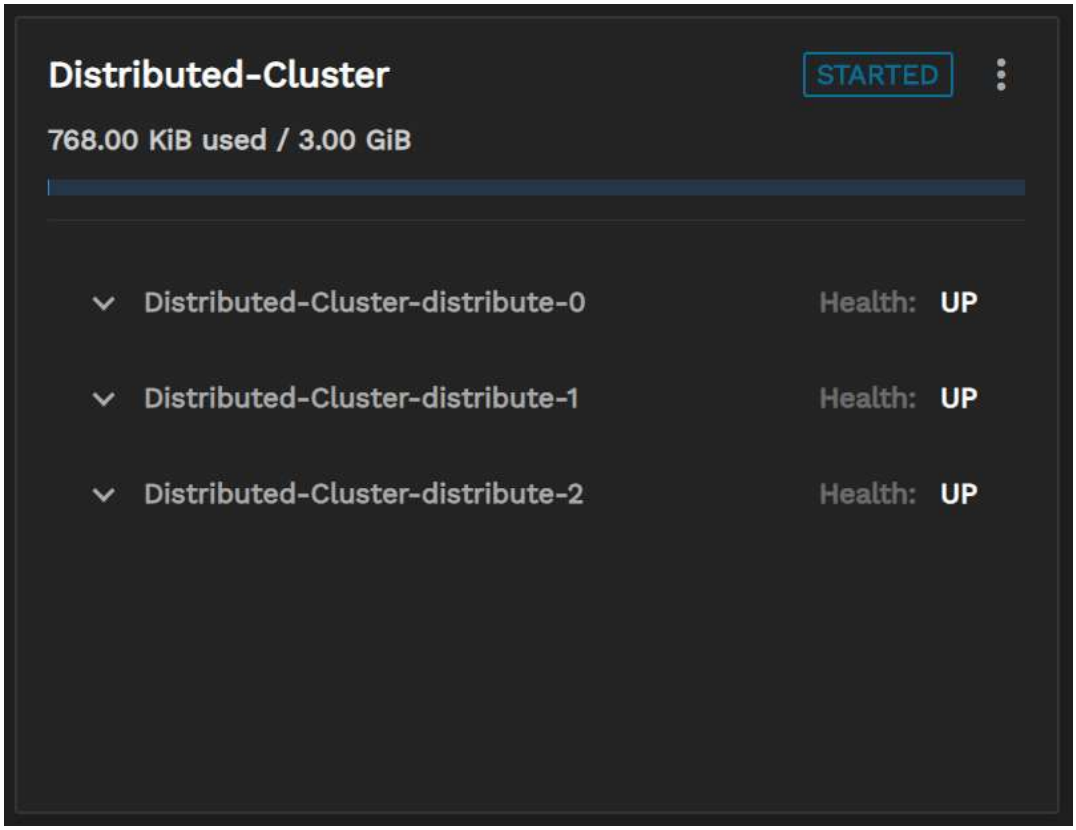
When finished click **Next.**



Review the configuration and click **Create** to create the Volume.



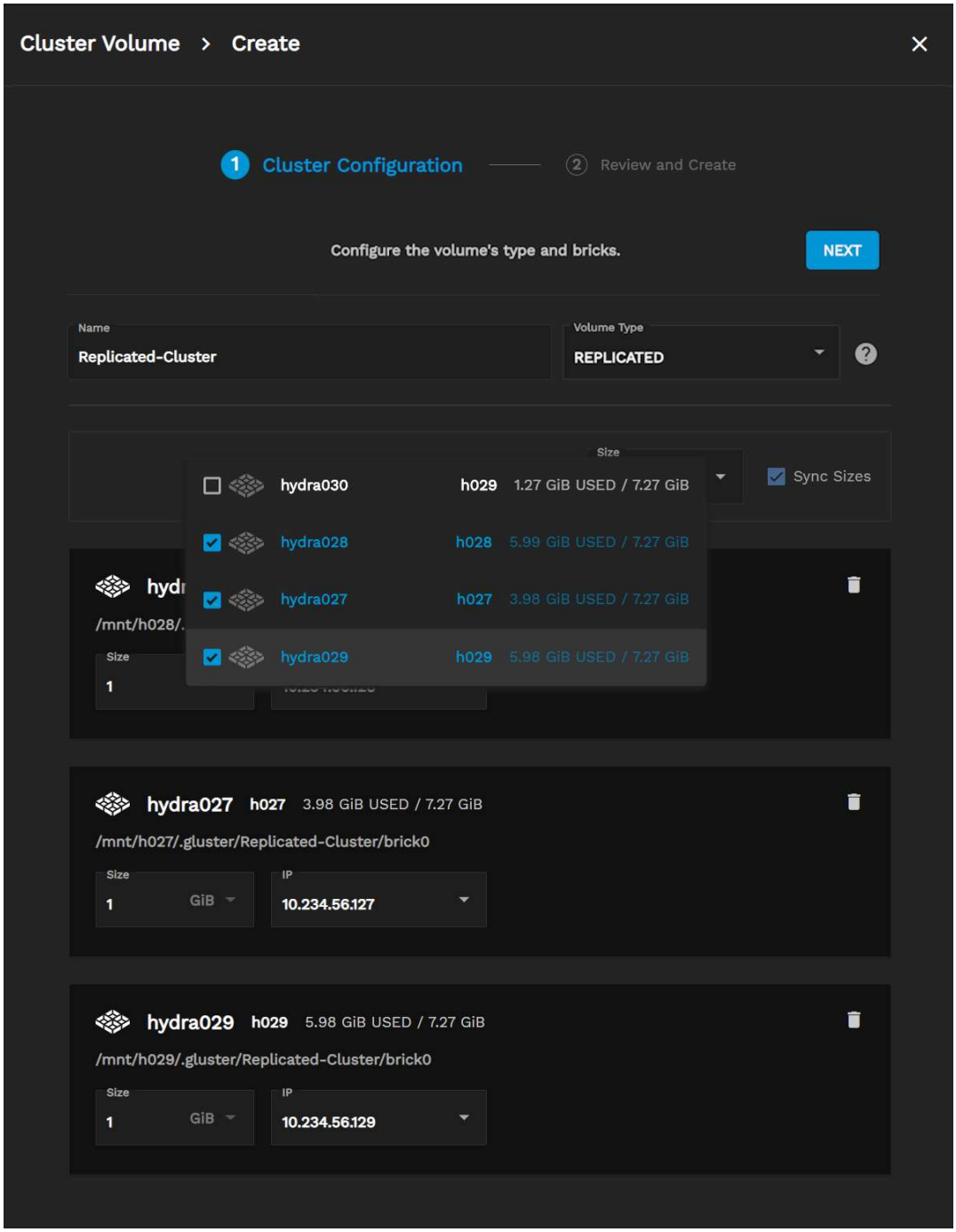
Once the volume is made, you can view its status.



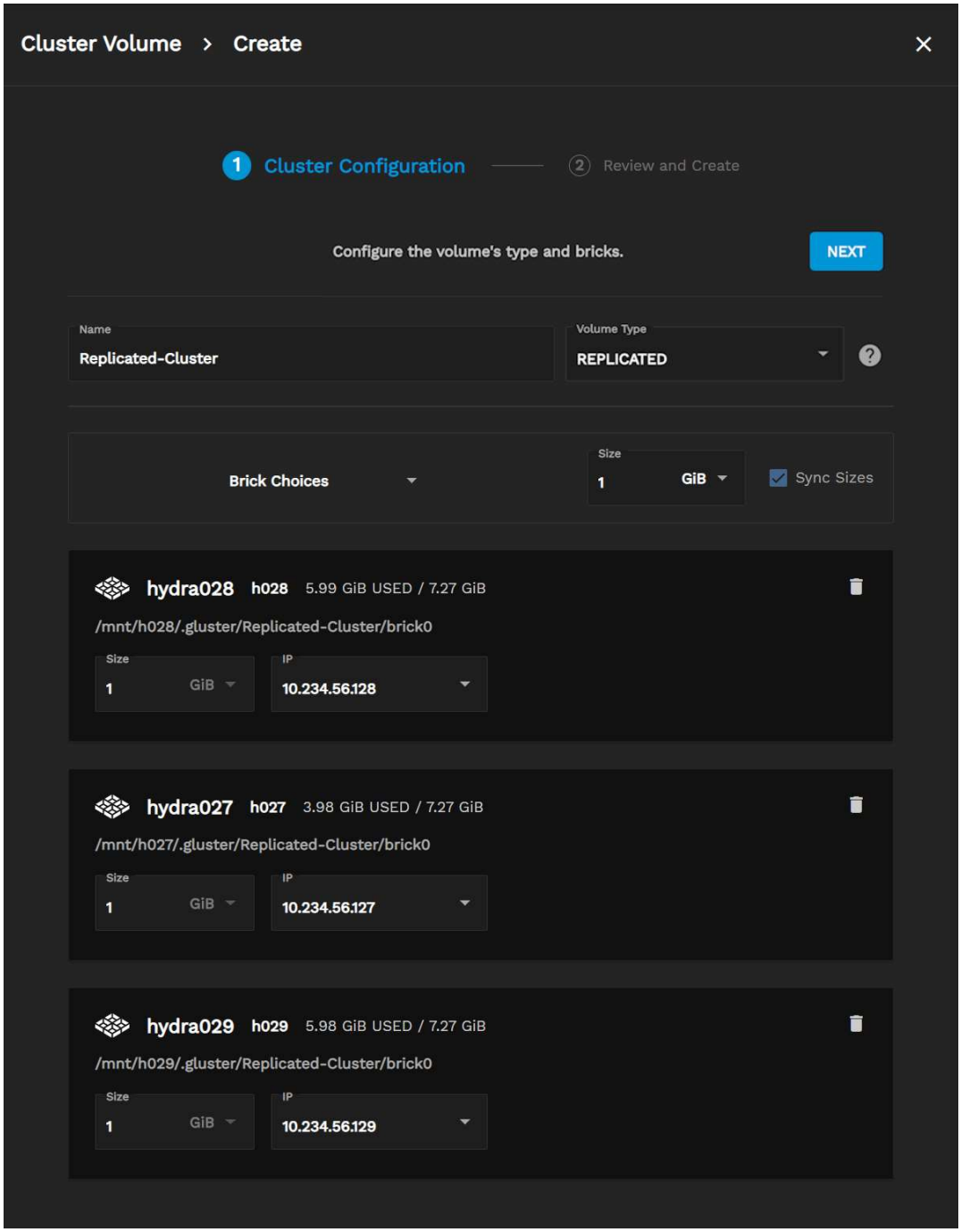
Replicated

In a Replicated Volume, the risk of data loss in a distributed volume is overcome. Exact copies of the all of the data are maintained on all bricks. The number of replicas in the volume is determined when creating the volume. At least three bricks are needed to create a volume. For further redundancy, add more bricks. A three brick volume will have 3 replicas, while a four brick volume will contain 4 replicas. A replicated volume will allow data to still be accessed even if a single brick fails. A Replicated volume is used for better reliability and data redundancy.

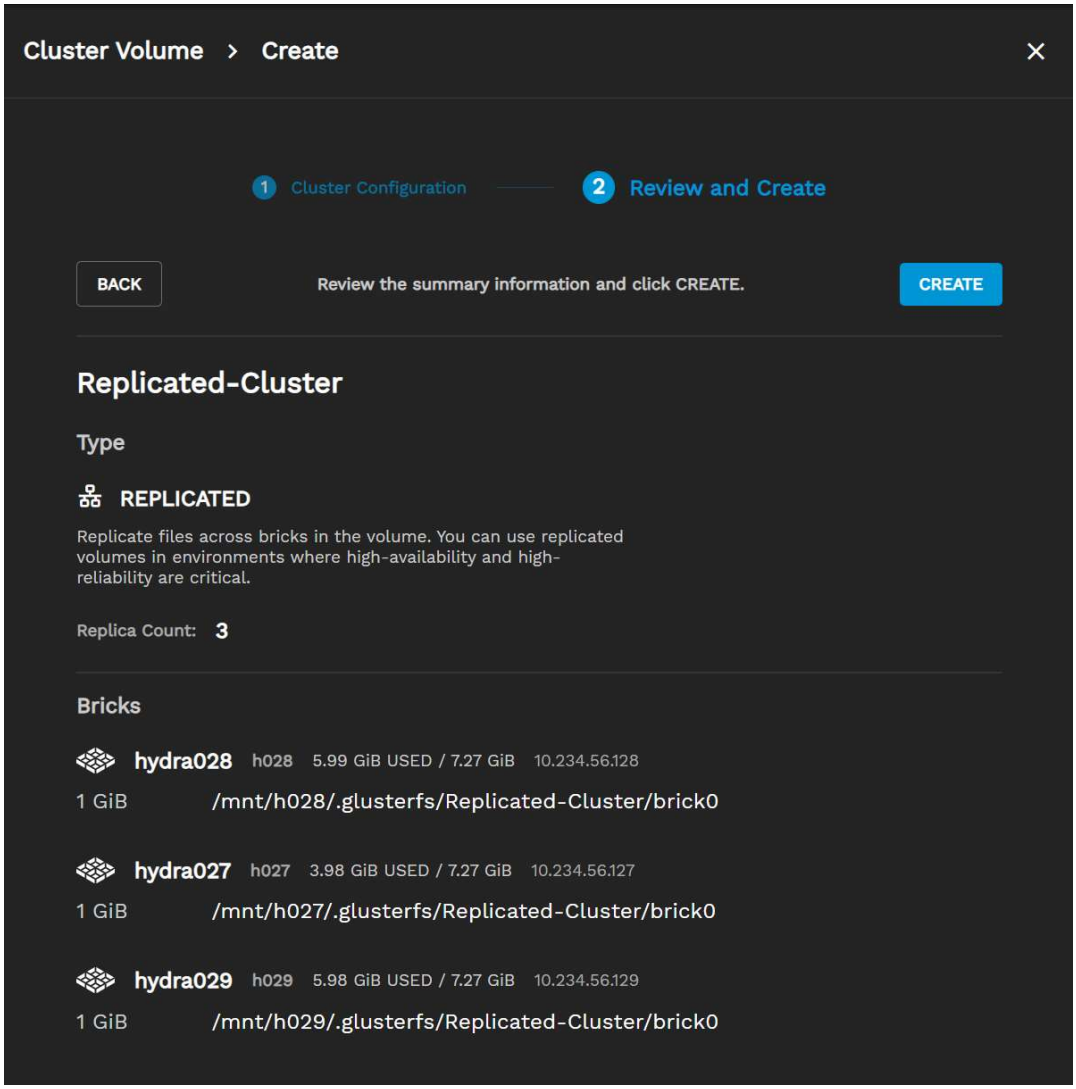
Click the *Brick Choices* drop down and check the locations to use for bricks.



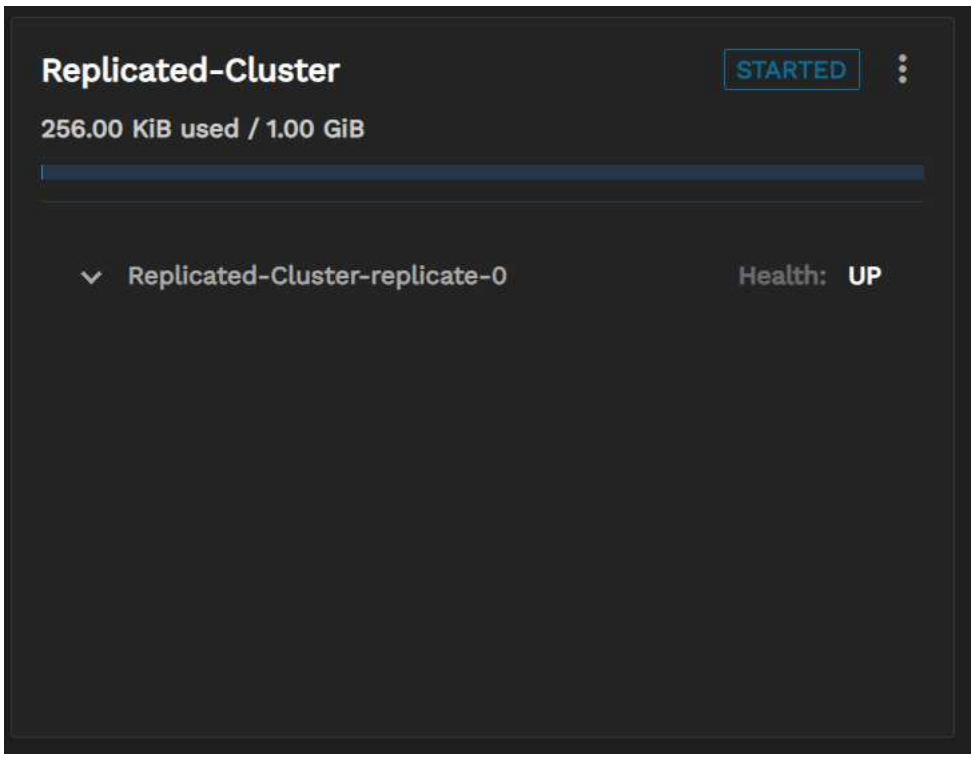
When finished click **Next.**



Review the configuration and click **Create** to create the Volume.



Once the volume is made, you can view its status.



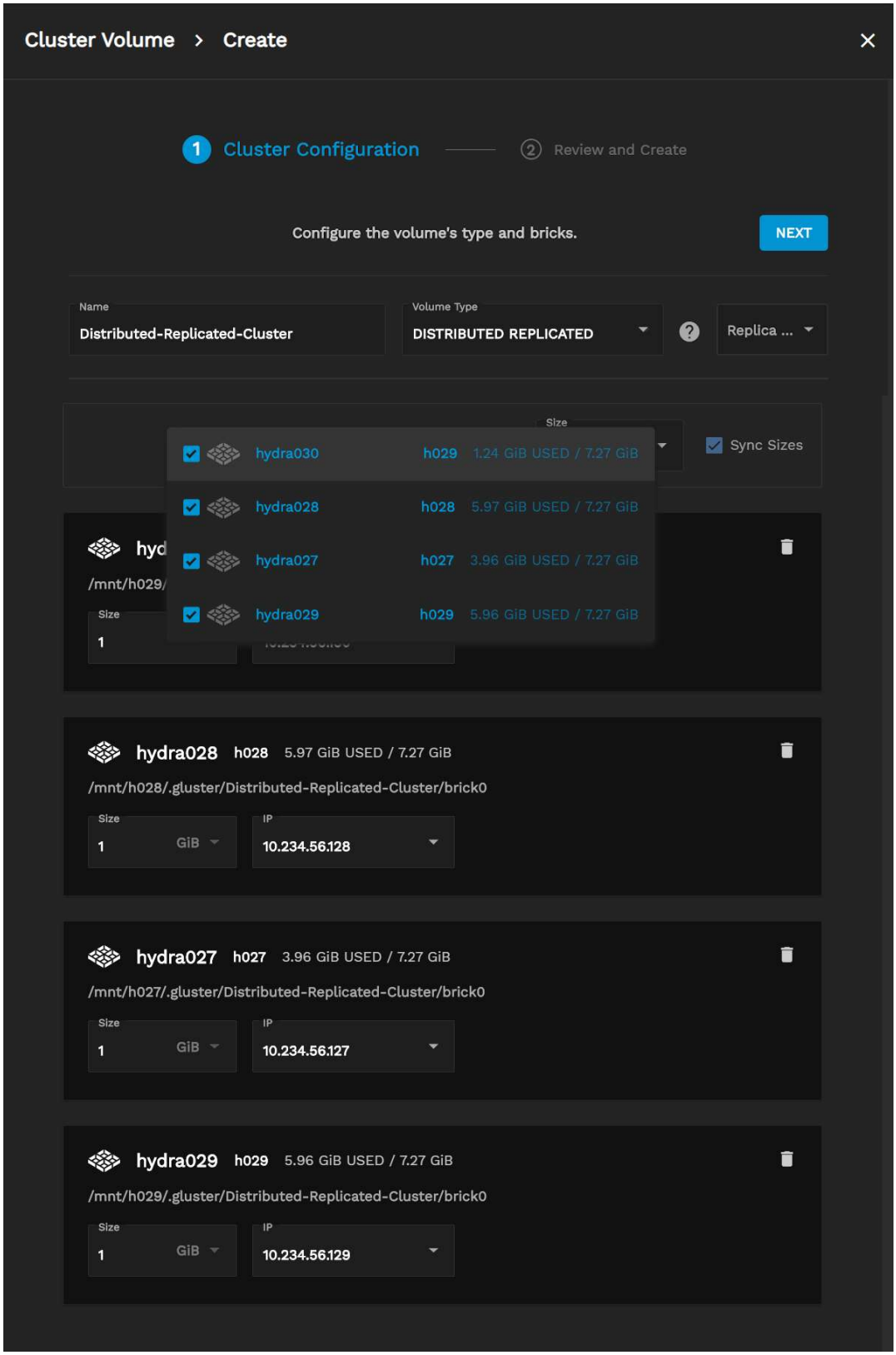
Distributed Replicated

In a Distributed Replicated Volume, data is distributed across replicated sets of bricks. The number of bricks must be a multiple of the replica count. The order in which bricks are specified is important because adjacent bricks become replicas of each other. This type of volume is best used when high availability of data due to redundancy and scaling storage is required. For example, an 8 brick volume with a replica count of two would result in the first two bricks become replicas of each other then the next two and so on. This volume would be referred to as 4x2. By contrast, in this 8 brick example, a replica count of 4 would result in four bricks become replica of each other and this volume would be referred to as 2x4 volume.

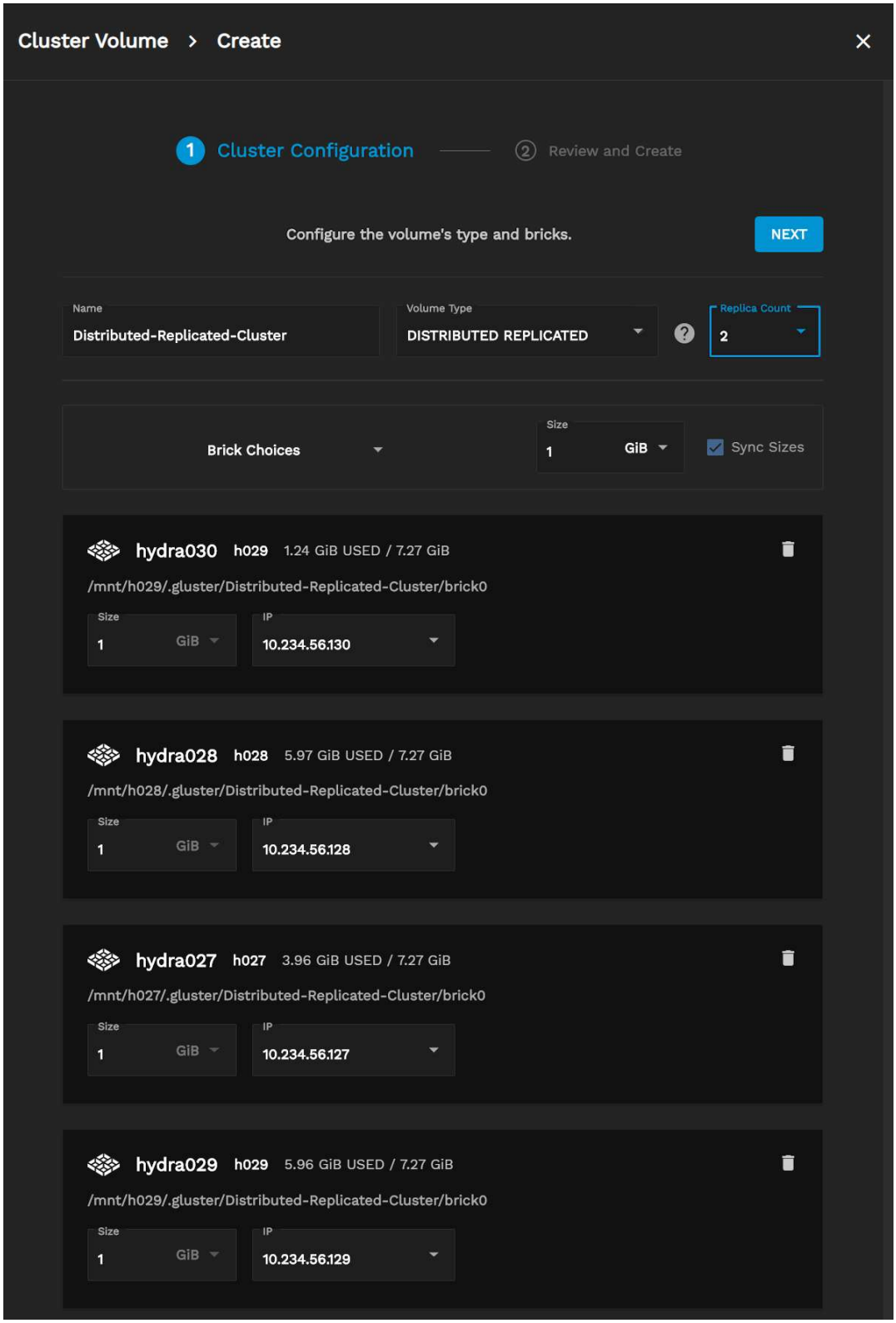
The **Replica value** value for a Distributed Replicated Volume must be a divisor of the total number of bricks selected. If 8 bricks are selected, the replica count can either be 2 or 4. A replica count of two will create a 4x2 volume where pairs of bricks replicate each other. A replica count of four will create a 2x4 volume where sets of 4 bricks replicate each other.

> Using a Replica count of that is not a divisor of the total number or bricks will results in a failed Volume Creation.

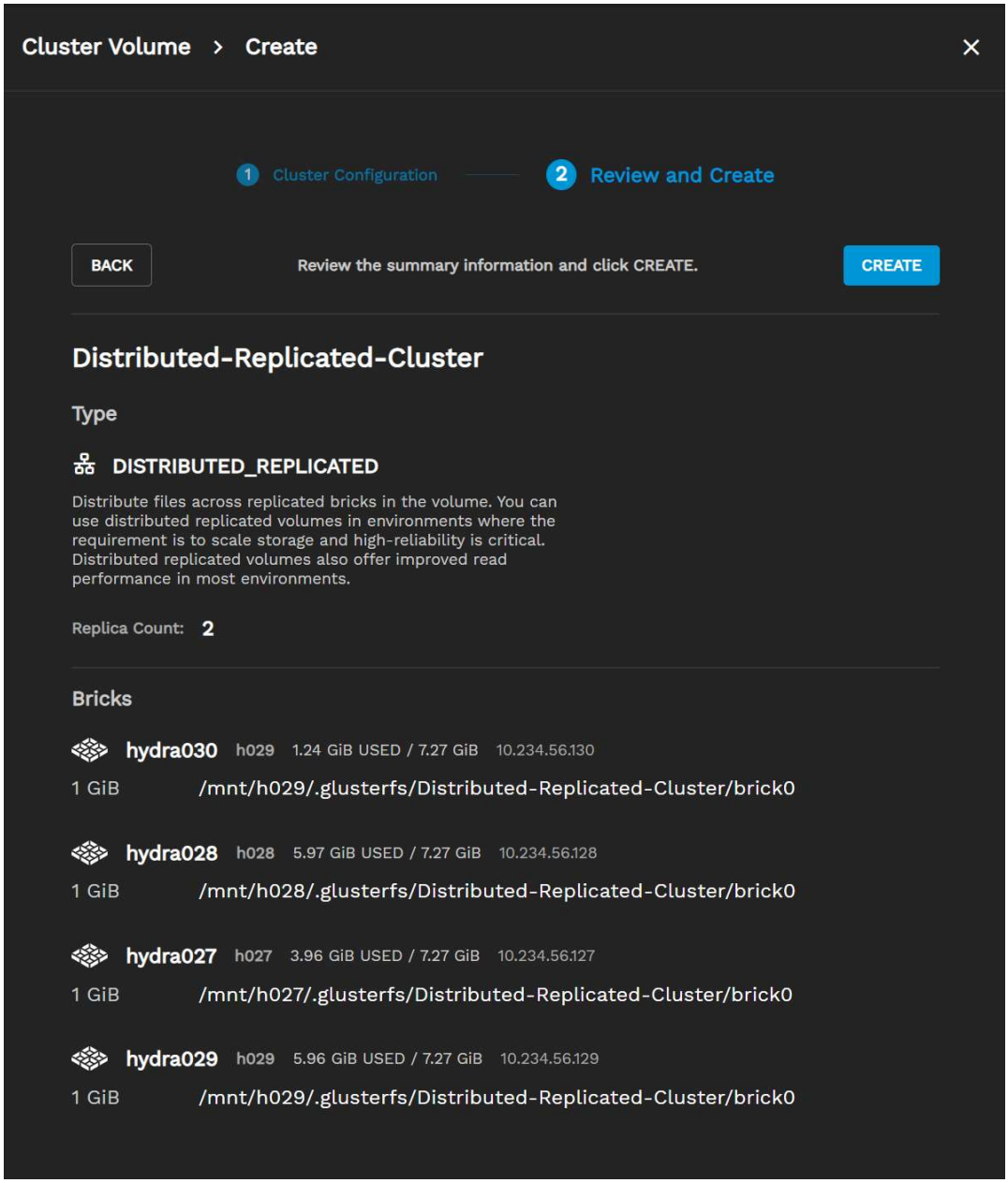
Click the *Brick Choices* drop down and check the locations to use for bricks.



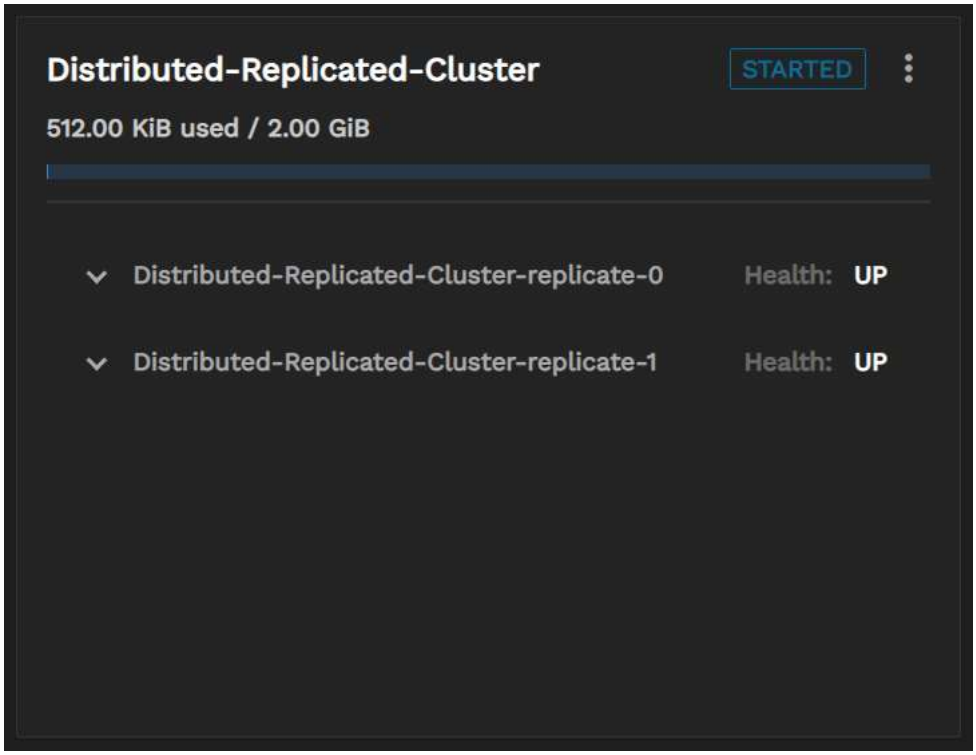
Select the *Replica Count* from the list. When finished click **Next.**



Review the configuration and click **Create** to create the Volume.



Once the volume is made, you can view its status.

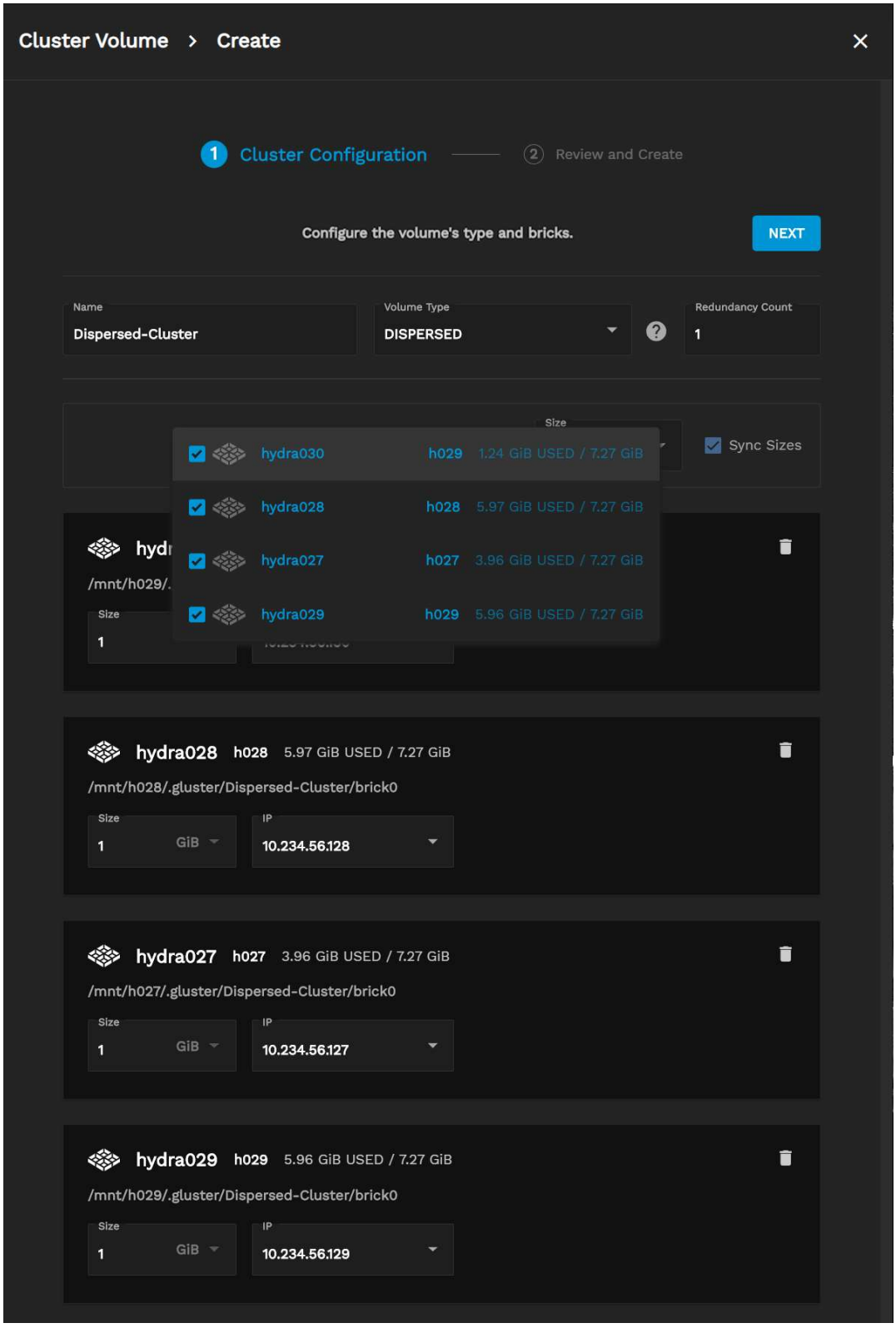


Dispersed

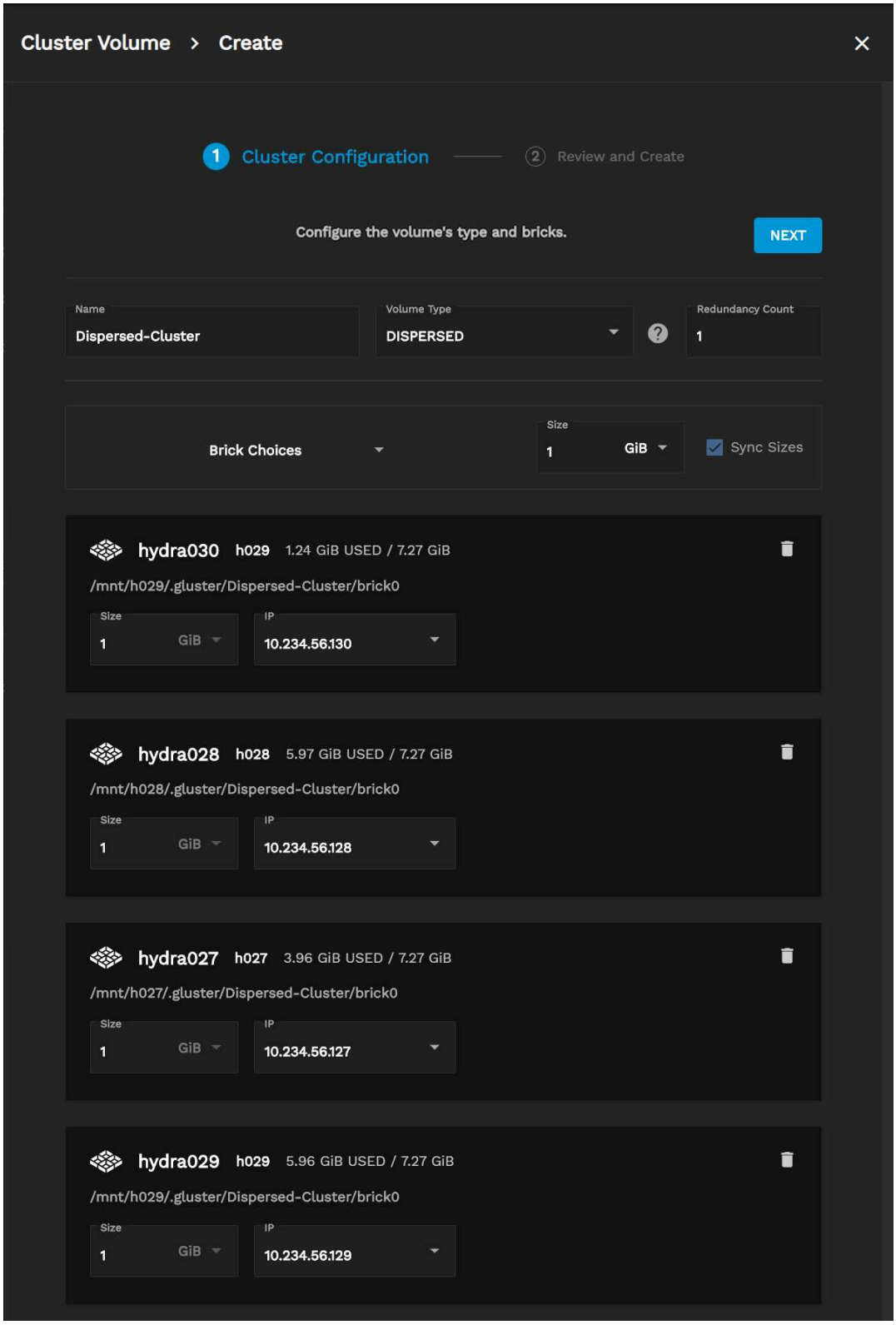
In a Dispersed Volume, the data is dispersed across the bricks and is based on on erasure codes. The data is stripped, with some redundancy added, across multiple bricks in the volume. Dispersed volumes allow a configurable level of reliability with minimal storage space waste. The number of redundant bricks in the volume is determined when creating the volume. The number of redundant bricks determines how many bricks can be lost without interrupting the operation of the volume.

The **Redundancy value** for a Dispersed Volume must be greater than 0 and less than n-1. The redundancy value can be considered to be the number of bricks you that can be lost before data loss occurs.

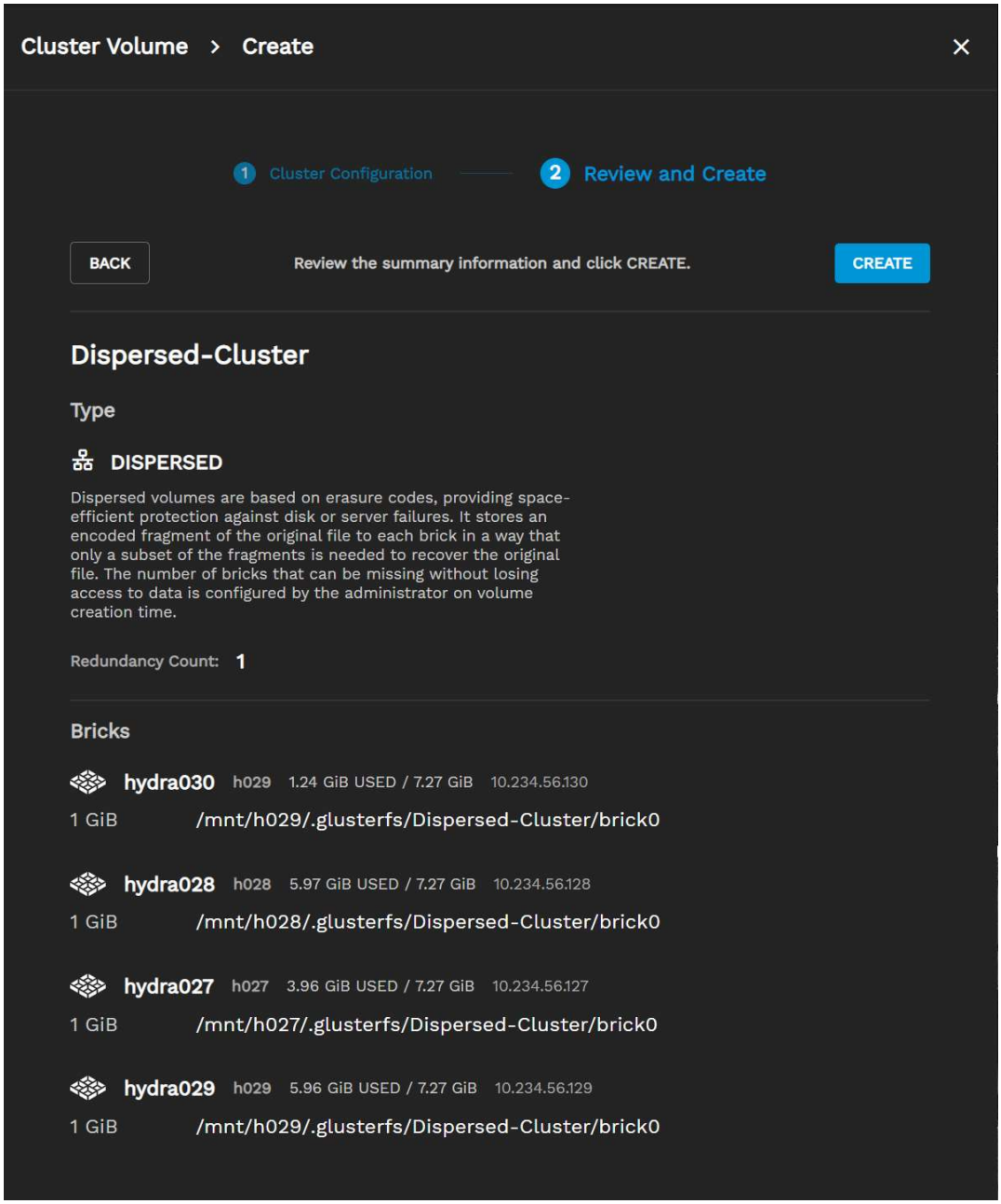
Click the *Brick Choices* drop down and check the locations to use for bricks.



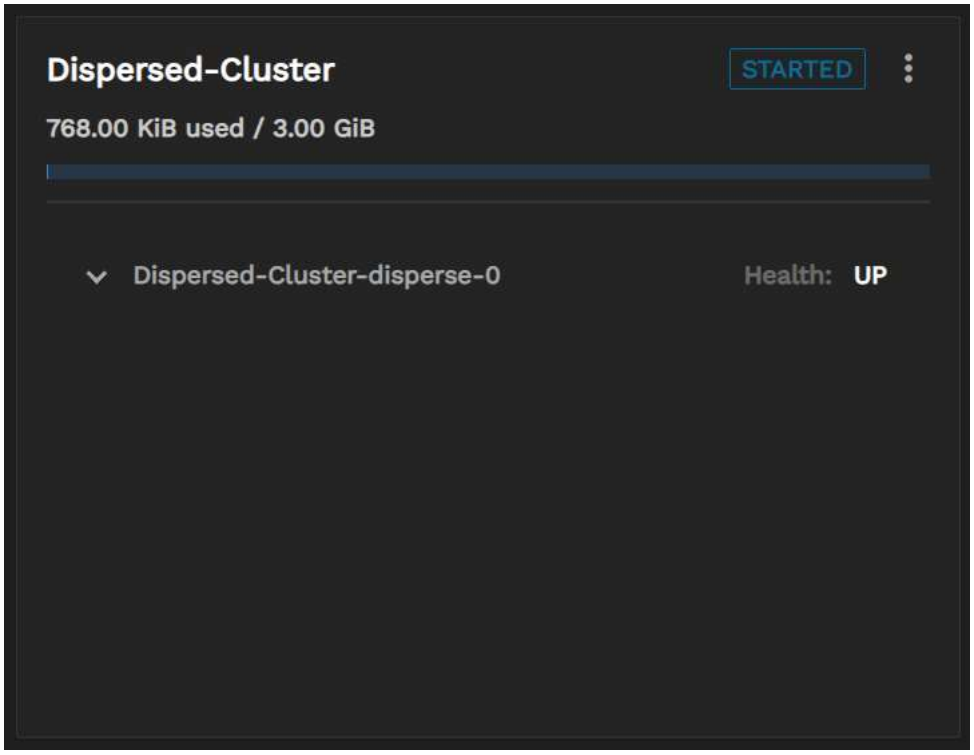
Select the *Redundancy value*. When finished click **Next.**



Review the configuration and click **Create** to create the Volume.



Once the volume is made, you can view its status.



Distributed Dispersed

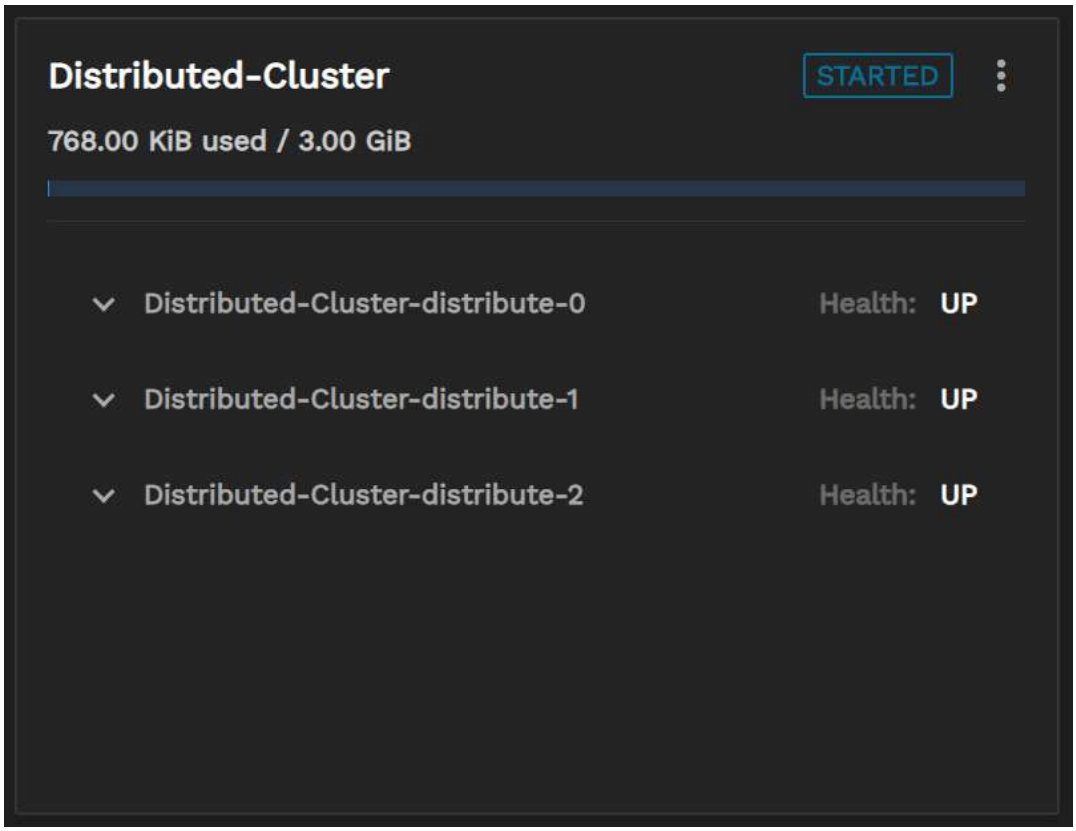
> Distributed Dispersed Volumes are not implemented at this time.

8.2 - Managing Clustered Storage

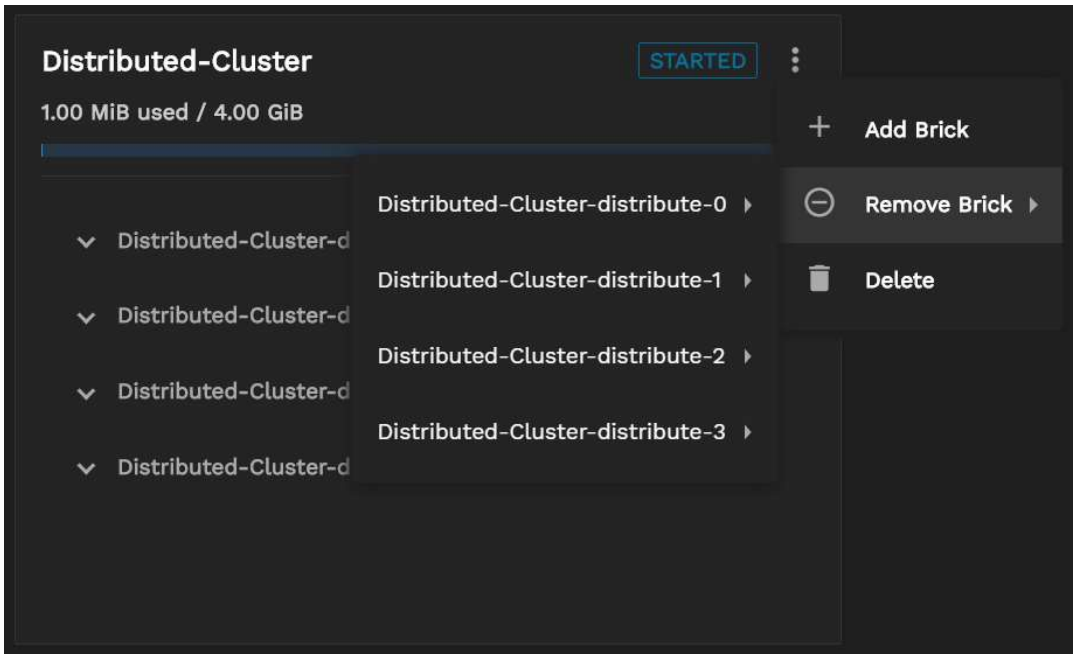
Clustered Volumes have differing management options based on cluster type.

> Removing and/or Replacing bricks from a clustered volume may lead to data corruption. Do not attempt to utilize this feature at the current time.

Distributed

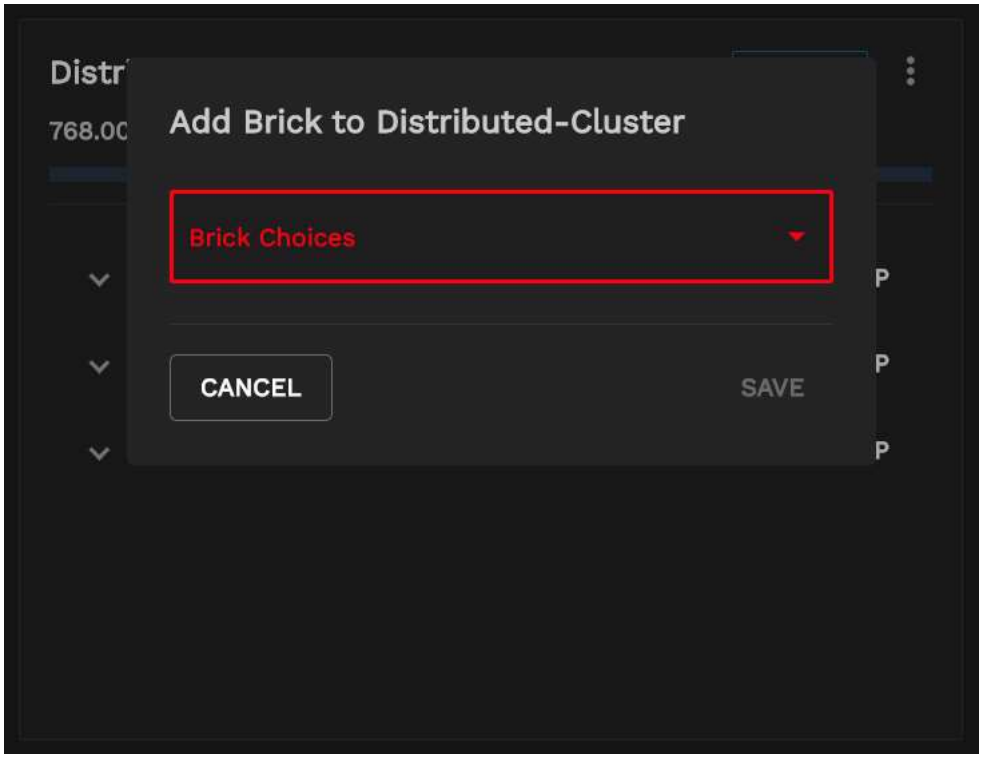


In a Distributed Volume the editing options are, adding a brick, replacing a brick, and to delete the cluster.

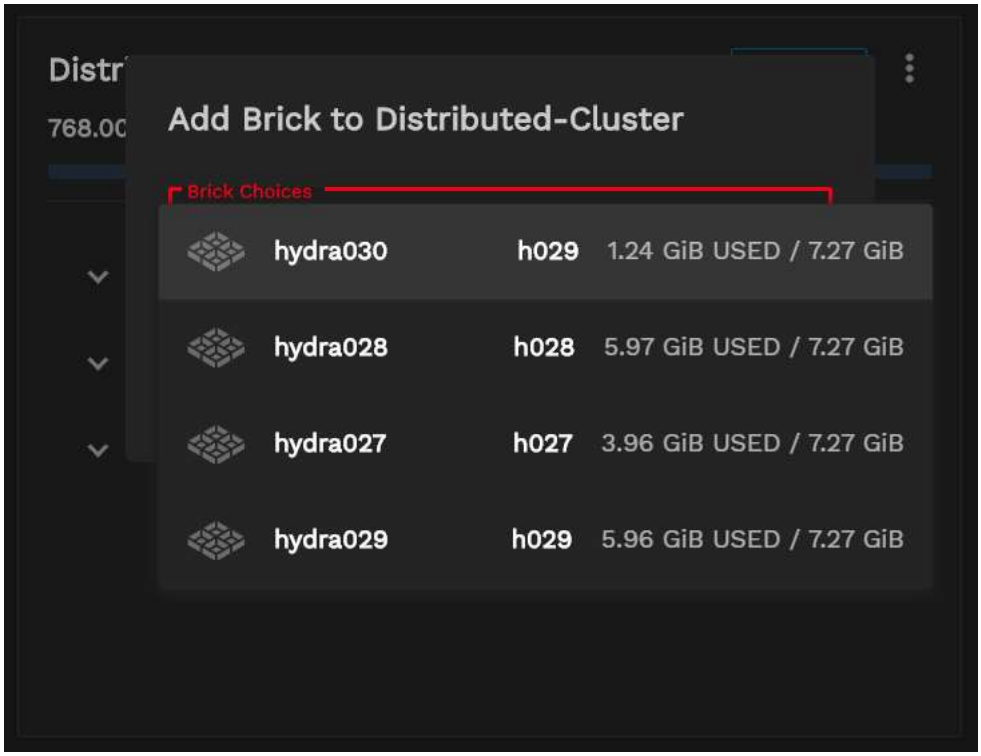


Add a brick to a Distributed Cluster

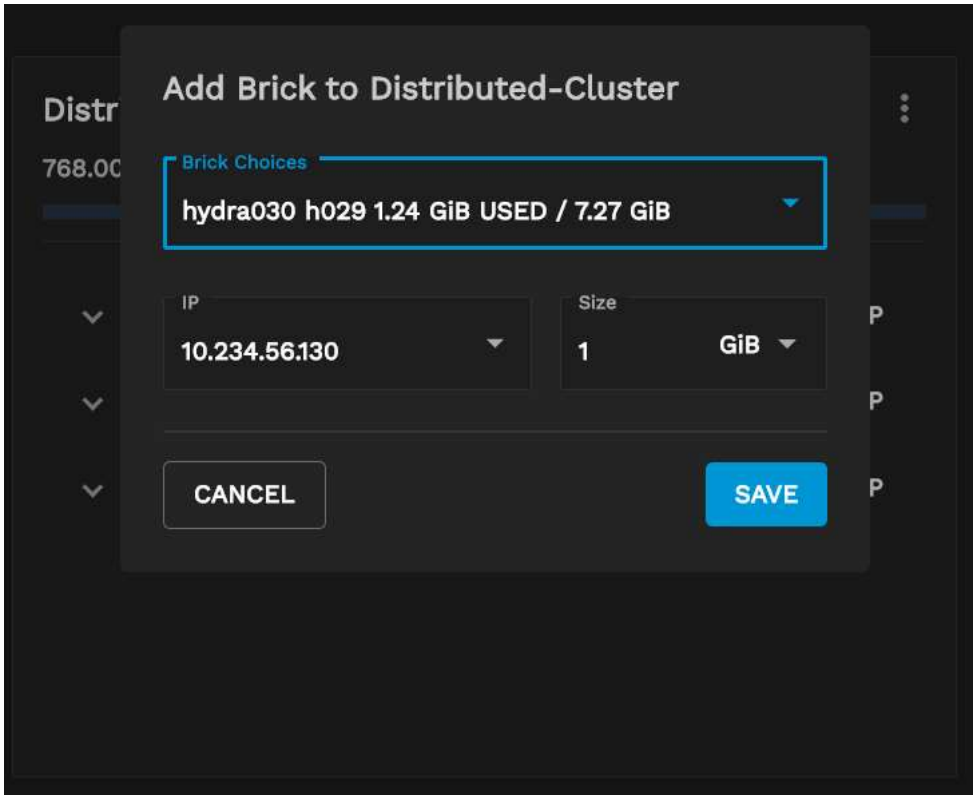
Click the three dots icon in the cluster overview card and select the **+ Add Brick** option to open the *Add Brick* menu.



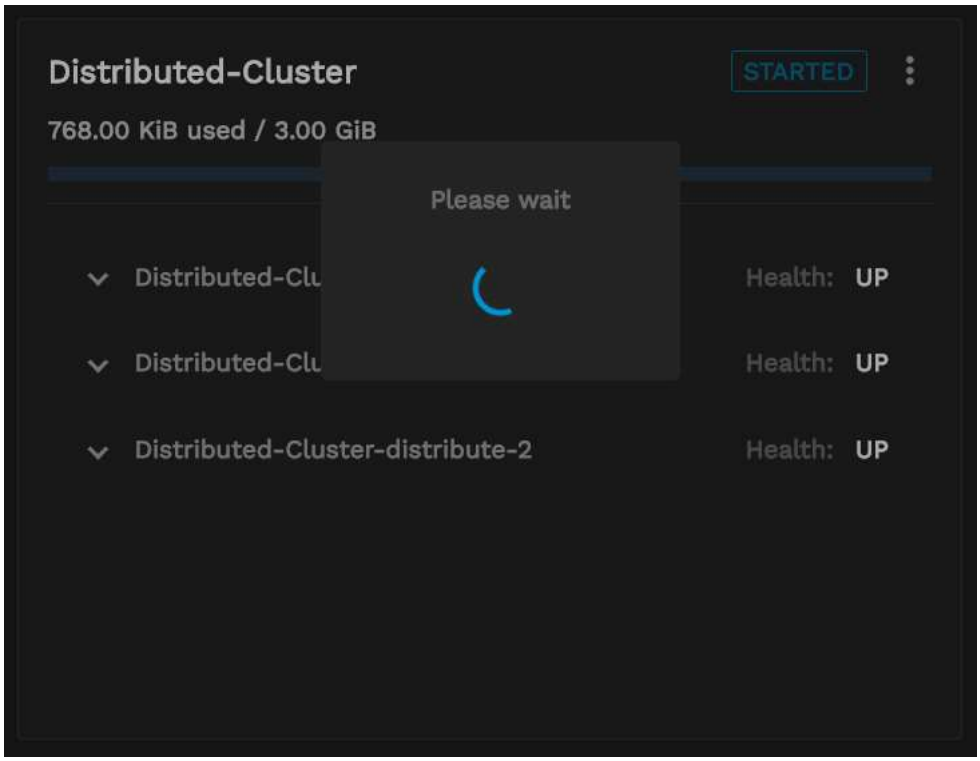
Click *Brick Choices* to display the list of systems available.



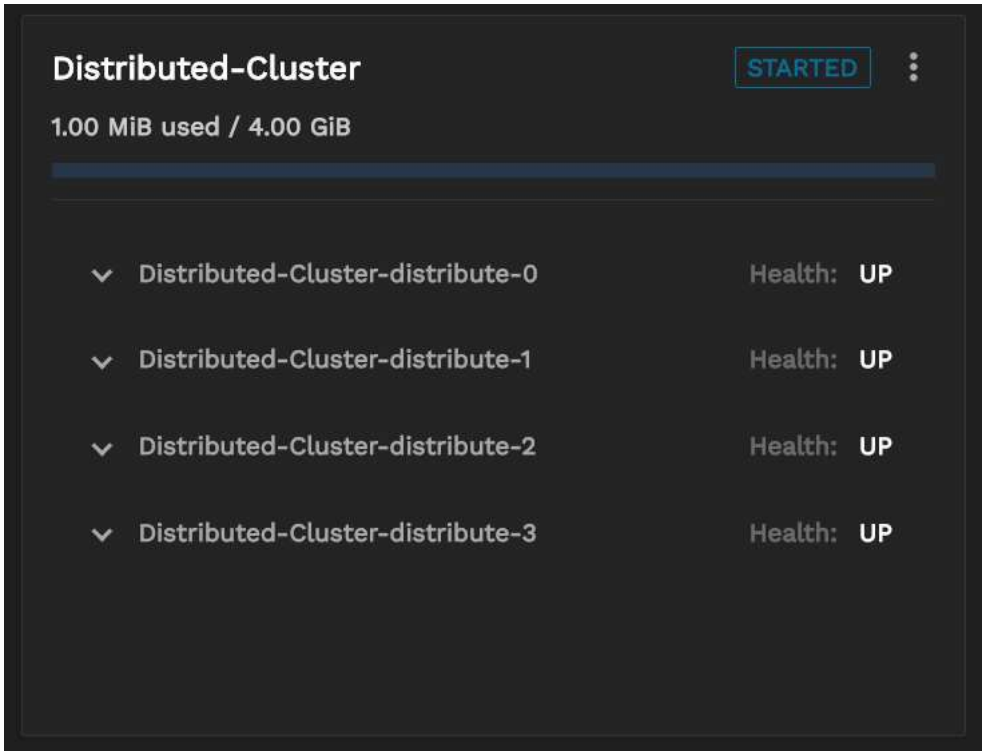
Selecting a system will display the options for the brick that will be created. It is strongly recommended that the size matches the existing bricks, but this can be changed if required.



When you are satisfied with the settings, click **SAVE** to add the brick. TrueCommmand and TrueNAS SCALE will now add the brick to the cluster.



When the new brick has been added, the cluster card will reflect the change.

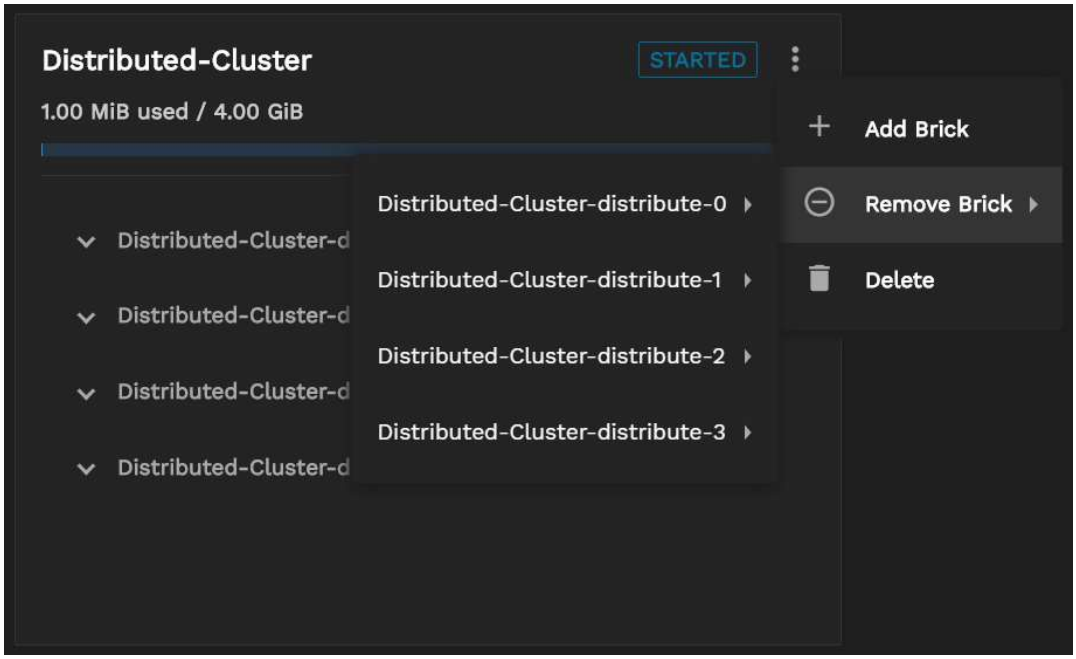


Removing a brick in a Distributed Cluster

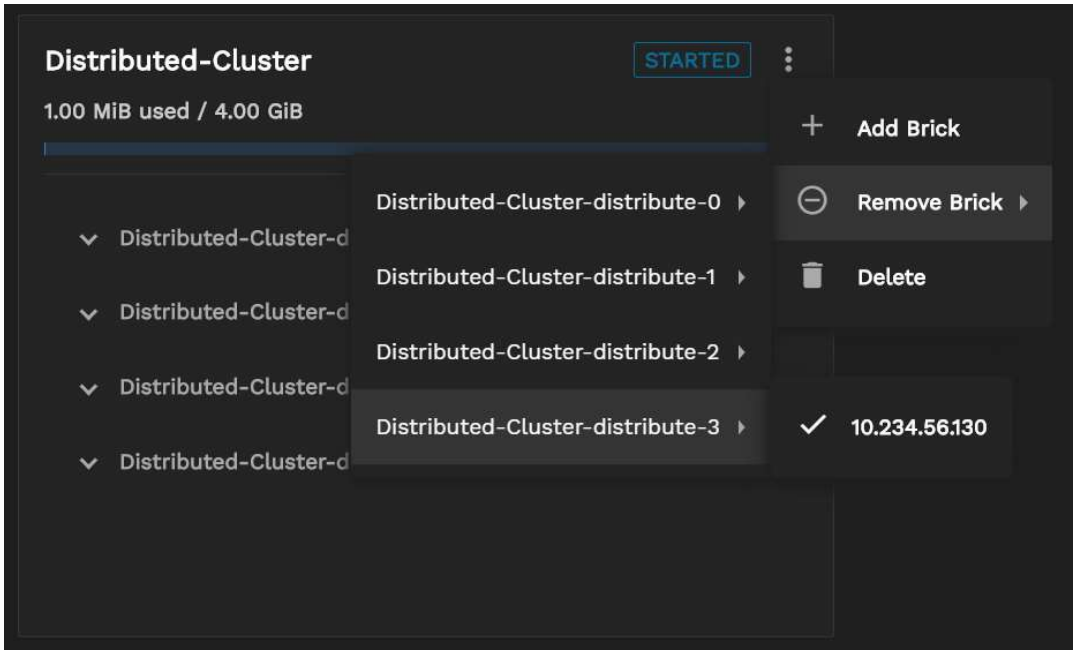
> This option is only avilable if a cluster has 4 or more bricks.

> This Feature is not fully implemented yet.

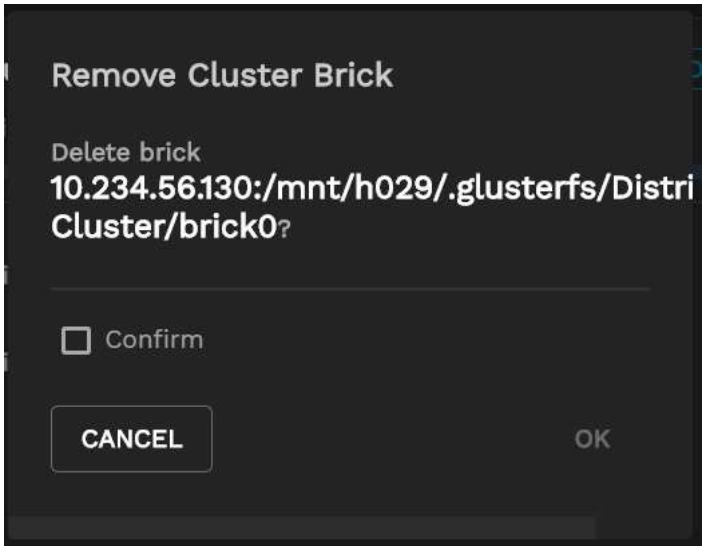
Click the three dots icon in the cluster overview card and hover the **Remove Brick** option for the list of bricks to appear.



Hover the mouse over the bricks listed to display their bricks. Click the **I**P to remove the brick.



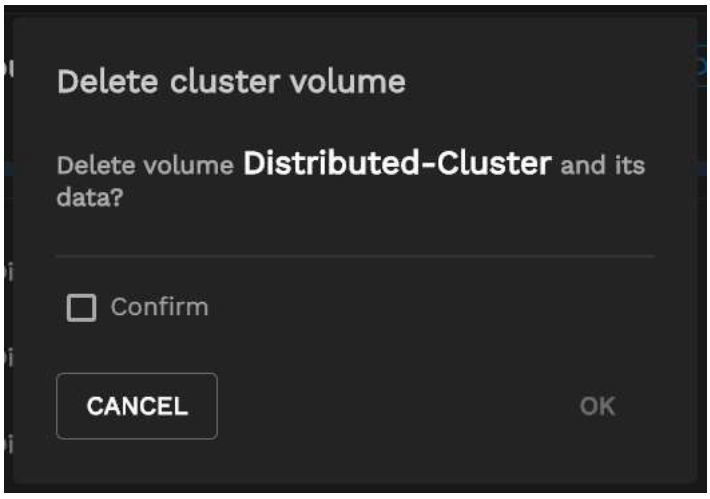
A confirmation box will appear and the deletion must be confirmed before proceeding.



After checking the confirm box, Click **OK** to remove the brick.

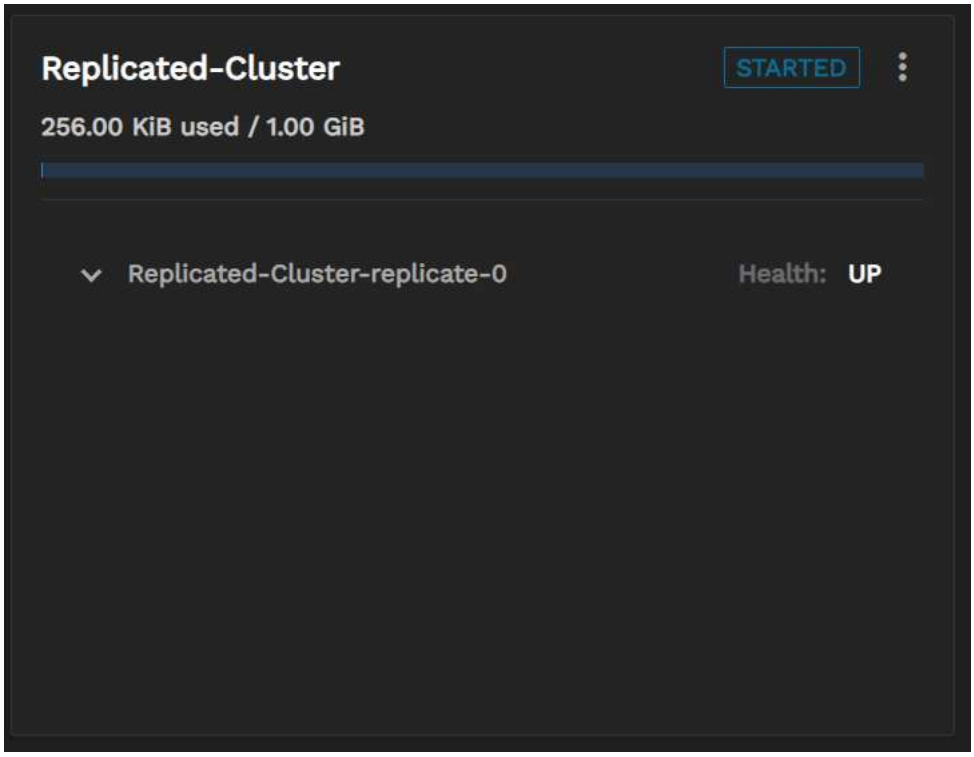
Deleting a Distributed Cluster

Click the three dots icon in the cluster overview card and select **Delete.** A confirmation box will appear and the deletion must be confirmed before proceeding.



After checking the confirm box, Click **OK** to delete the cluster.

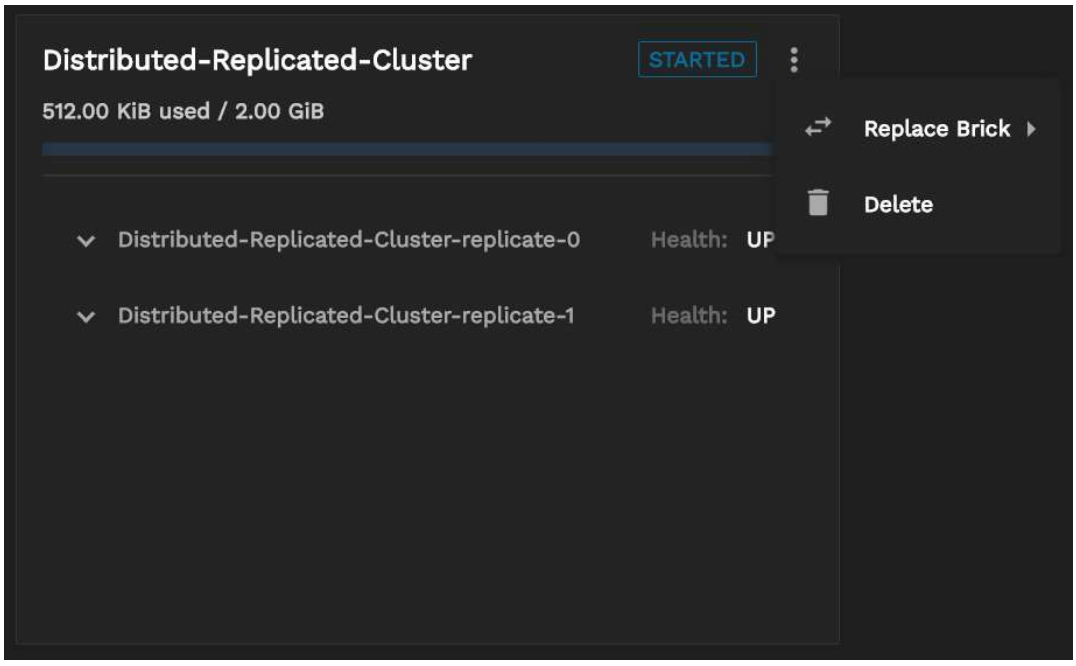
Replicated



In a Replicated Volume the editing options are replacing a brick and deleting the cluster.

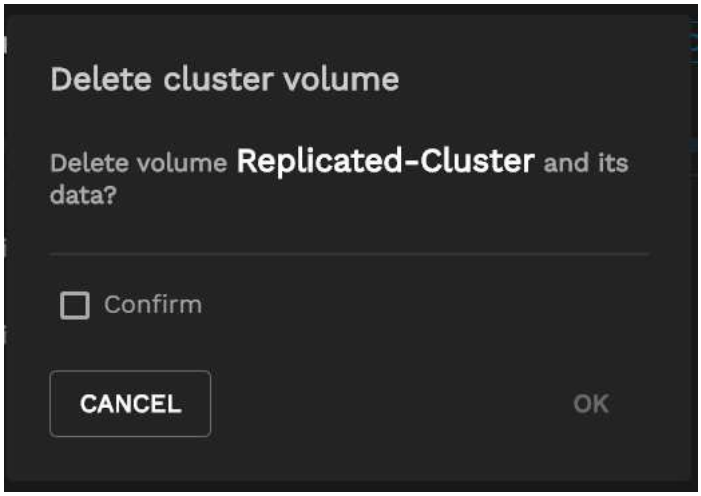
Replacing a Brick in a Replicated Cluster

> This Feature is not fully implemented yet.



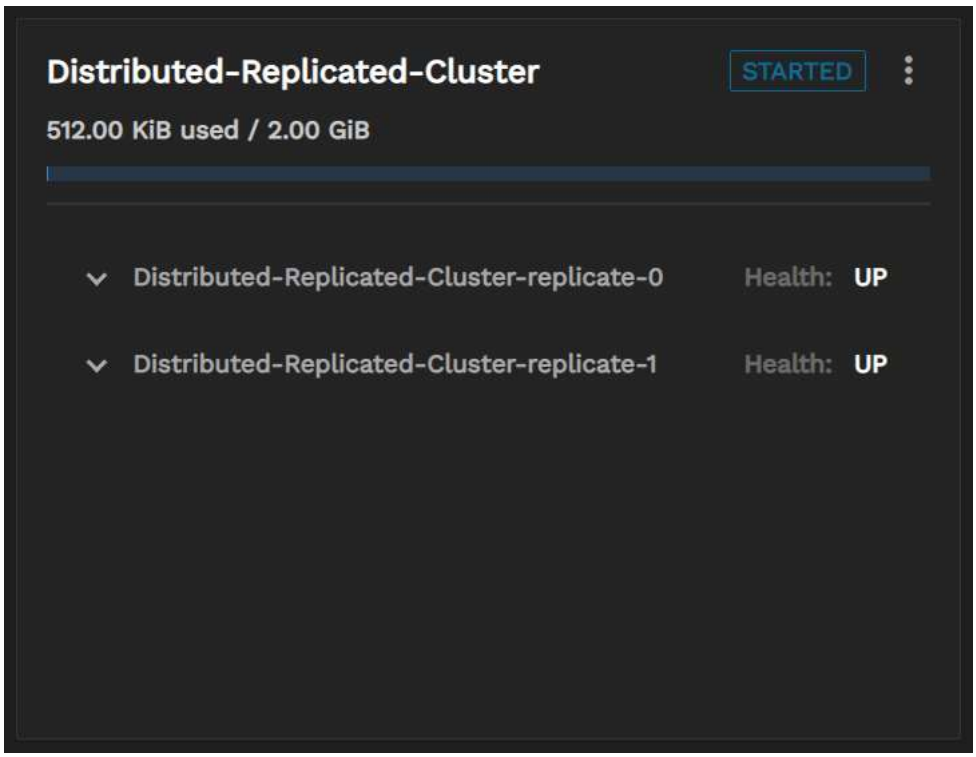
Deleting a Replicated Cluster

Click the three dots icon in the cluster overview card and select **Delete**. A confirmation box will appear and the deletion must be confirmed before proceeding.



After checking the confirm box, Click **OK** to delete the cluster.

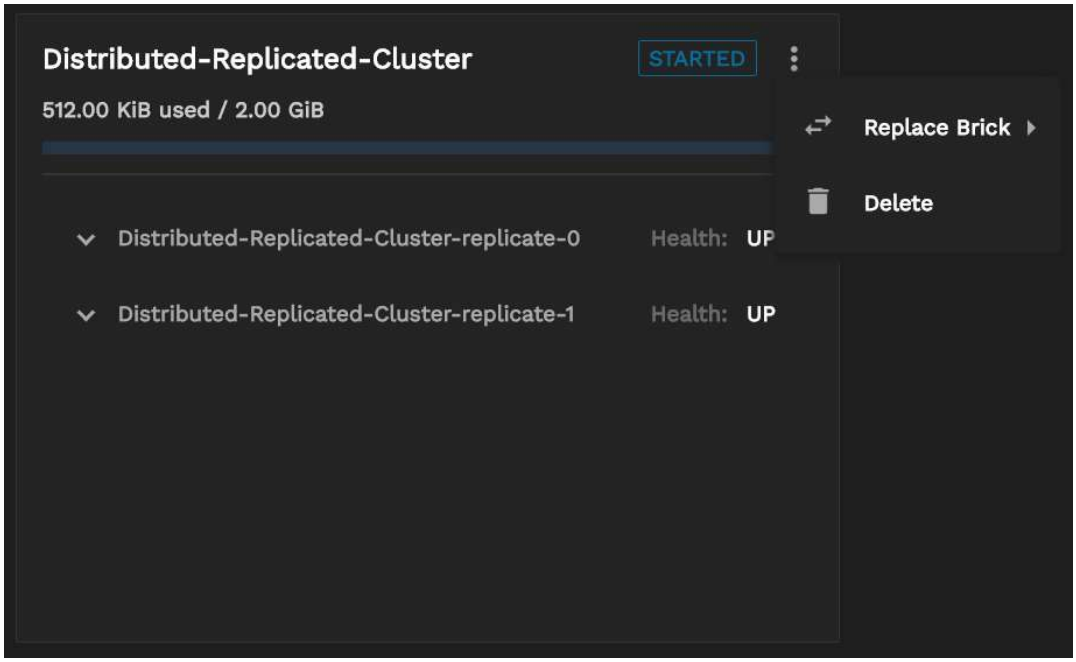
Distributed Replicated



In a Distributed Replicated the editing options are replacing a brick and deleting the cluster.

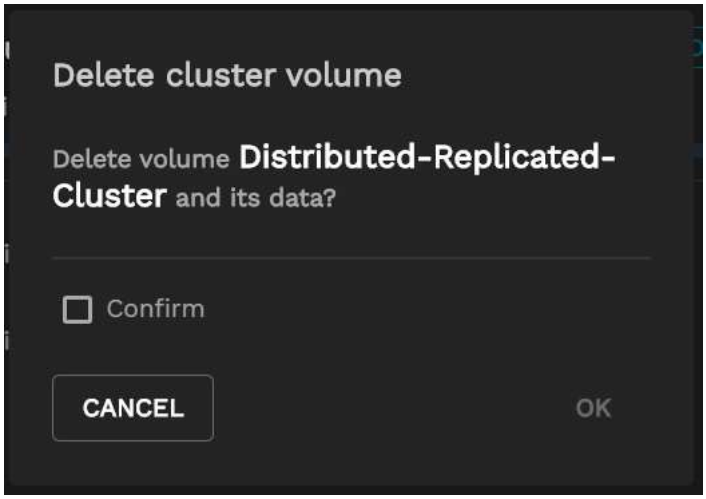
Replacing a Brick in a Distributed Replicated Cluster

> This Feature is not fully implemented yet.



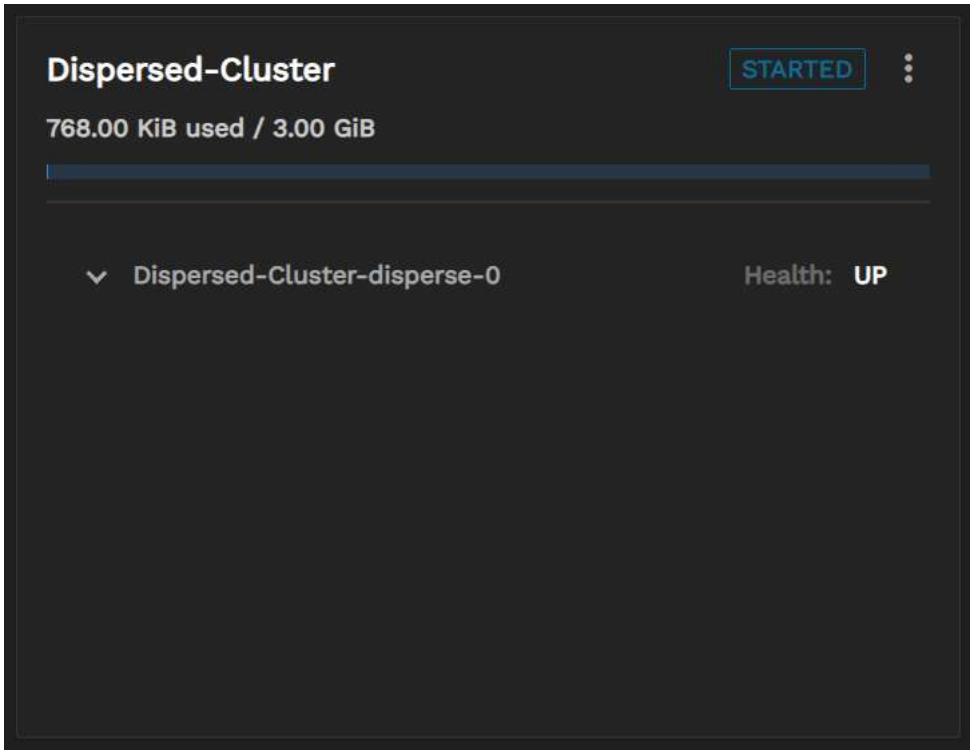
Deleting a Distributed Replicated Cluster

Click the three dots icon in the cluster overview card and select **Delete.** A confirmation box will appear and the deletion must be confirmed before proceeding.



After checking the confirm box, Click **OK** to delete the cluster.

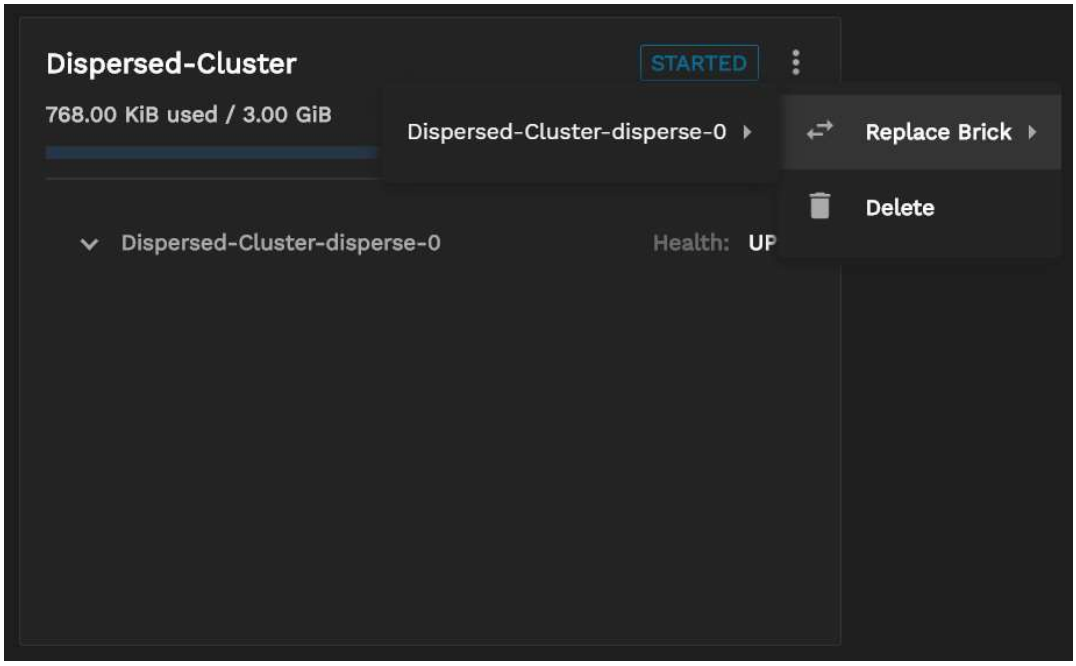
Dispersed



In a Dispersed Volume the editing options are replacing a brick and deleting the cluster.

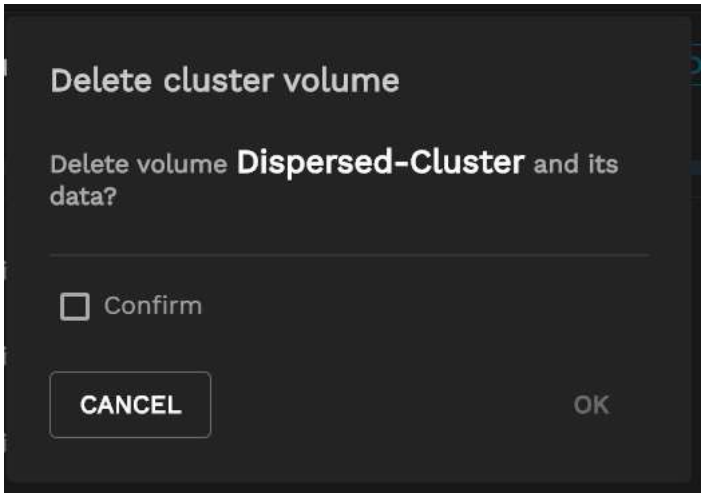
Replacing a Brick in a Dispersed Cluster

> This Feature is not fully implemented yet.



Deleting a Dispersed Cluster

Click the three dots icon in the cluster overview card and select **Delete**. A confirmation box will appear and the deletion must be confirmed before proceeding.



After checking the confirm box, Click **OK** to delete the cluster.

Distributed Dispersed

> Distributed Dispersed Volumes are not implemented at this time.

8.3 - Mounting Clustered Volumes

Manually Mounting Volumes

> Install the glusterfs client for your Linux distribution first, consult with your systems package documentation on specific steps to start that process.

To mount a volume, use the following command:

```
mount -t glusterfs HOSTNAME-OR-IPADDRESS:/VOLNAME MOUNTDIR
```

For example:

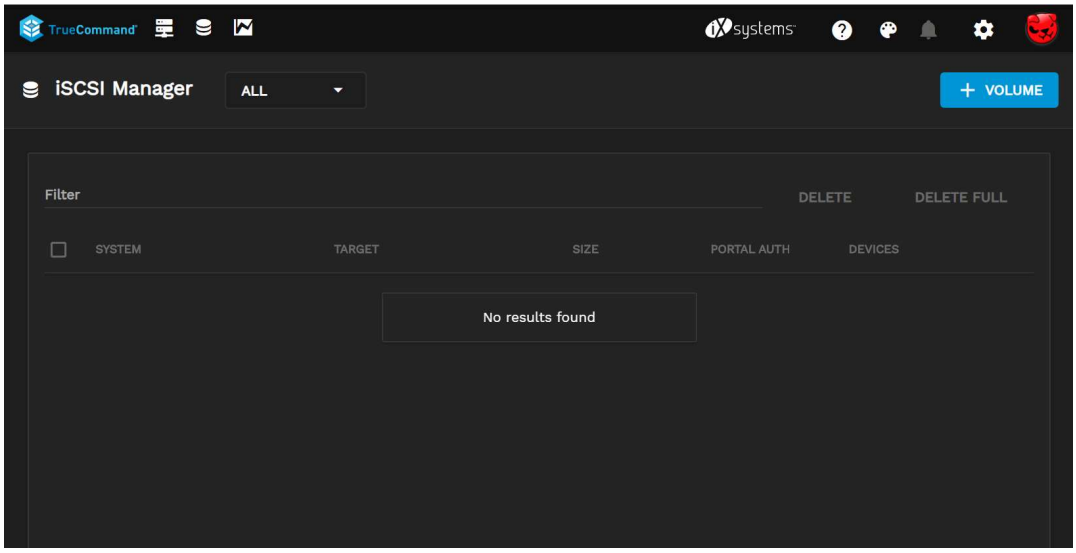
```
mount -t glusterfs server1:/test-volume /mnt/glusterfs
```

See http://gluster.org/ for additional references.

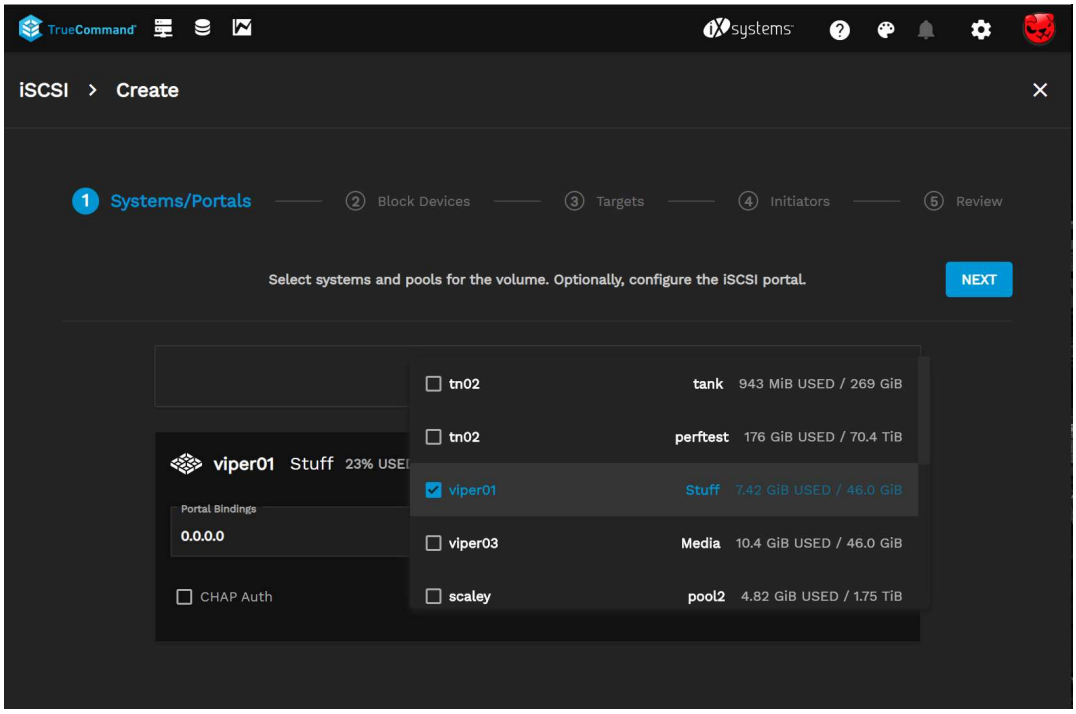
9 - iSCSI Volume Management

> iSCSI management is a brand new feature in TrueCommand 2.0. Always back up any data intended for storage or sharing!

Open the **iSCSI Manager** page by clicking the icon on the top bar.

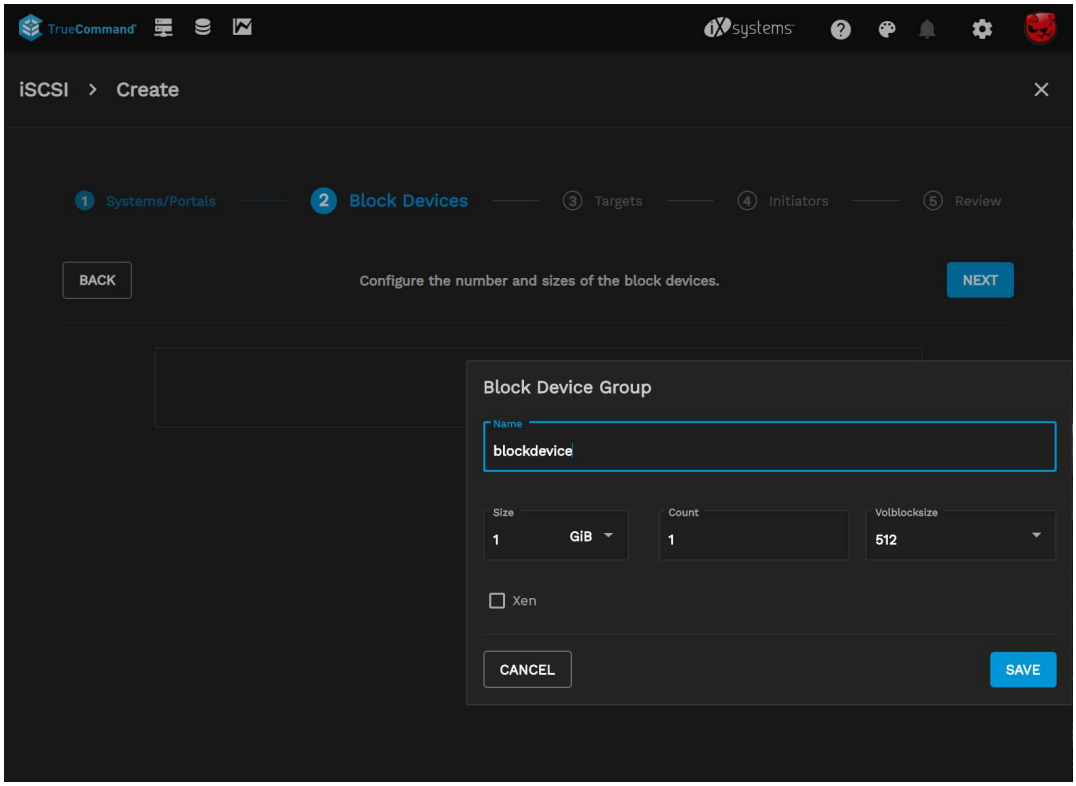


Start creating an iSCSI volume by clicking **+ Volume**. When the page opens, click **+ Add System Pool** and select a pool or multiple pools.



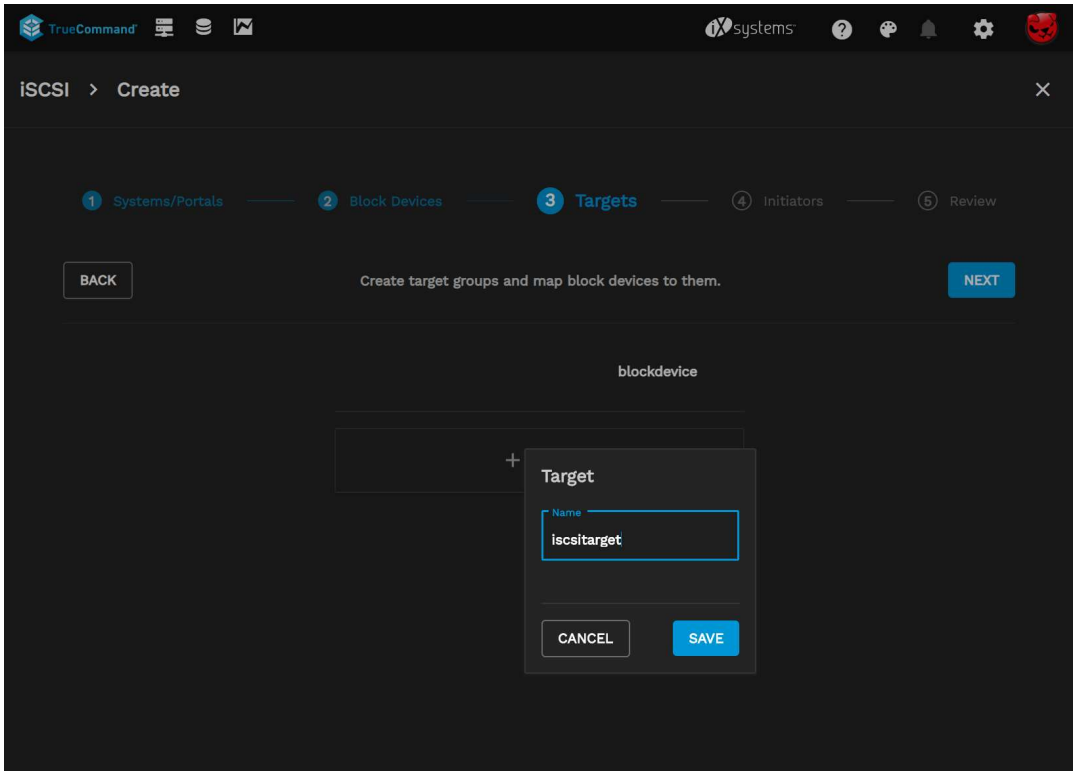
Click **Next**.

Click **+ Block Devices** to add Block devices. The *count* field creates a batch of iSCSI datastores with identical settings in the number specified.



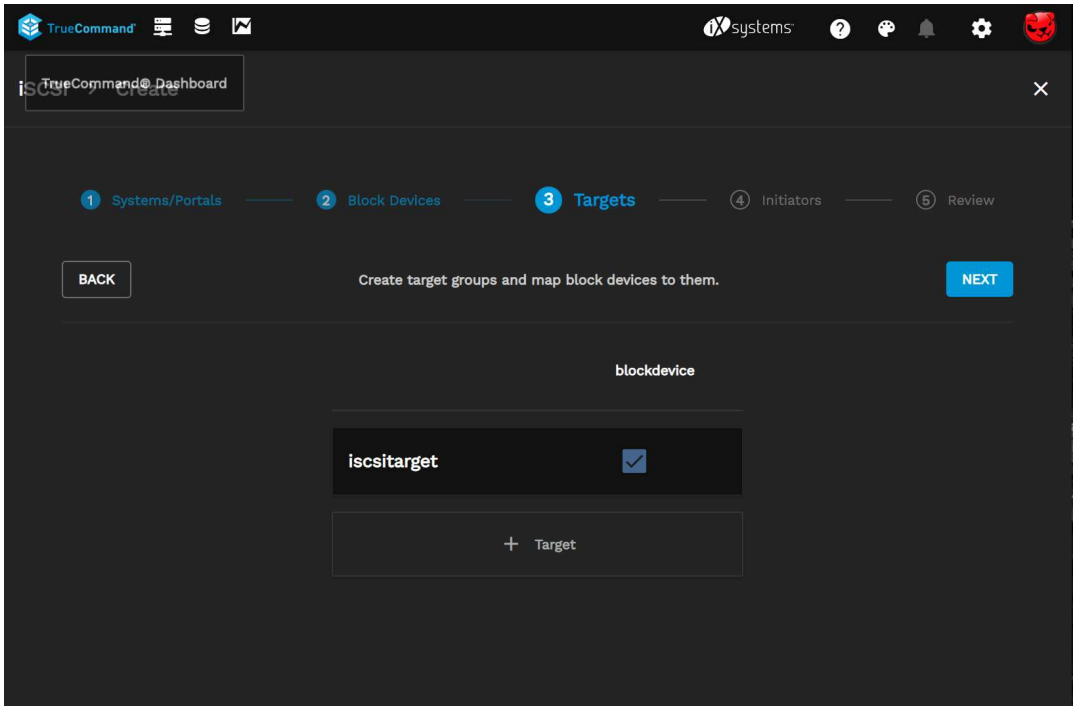
Click **SAVE** when finished and click **NEXT**.

Click **+ Target** and name the target.



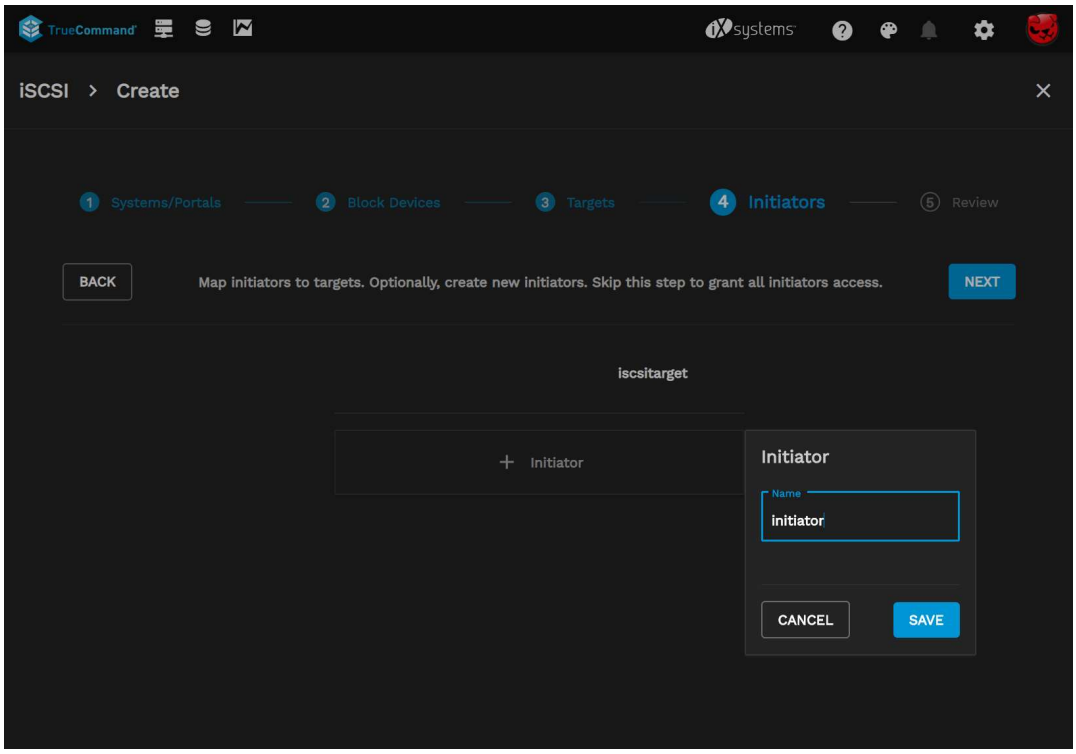
Click **SAVE** when finished and click **NEXT**.

Set the checkbox to assign the target to the block device.



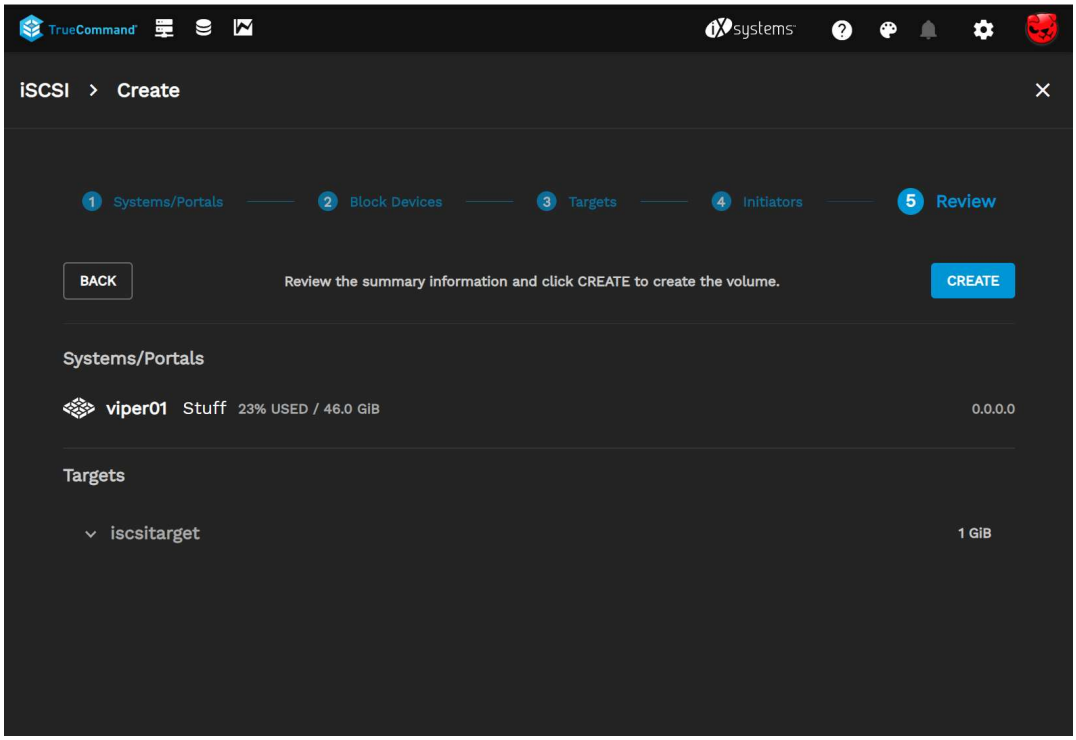
Click **NEXT**.

By default, all initiators are granted access to the target. To change this, click **+ Initiator**. Name the new initiator and set the checkbox to assign the initiator to the target.

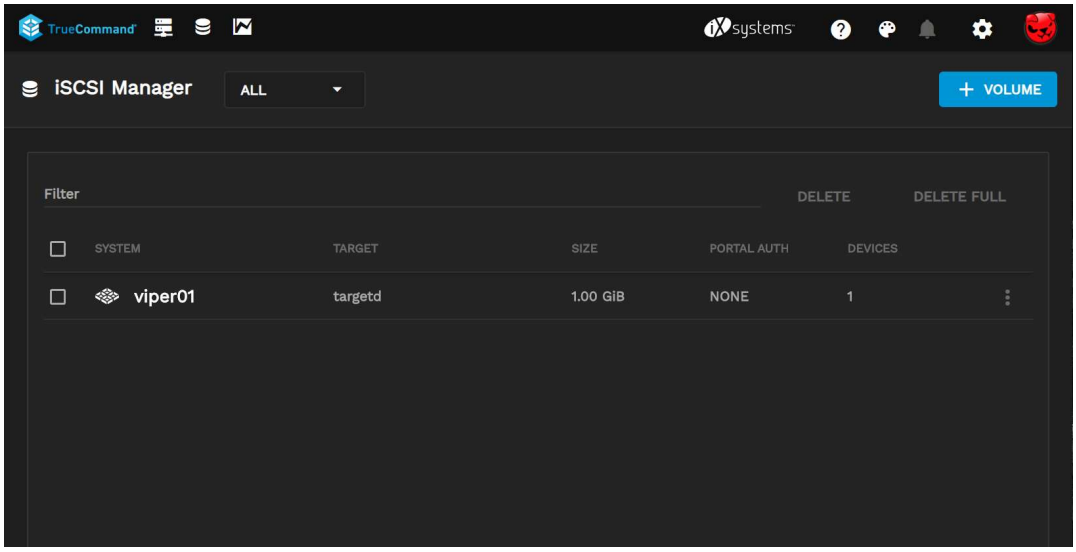


Click **NEXT**.

Review the configuration and click **Create**.



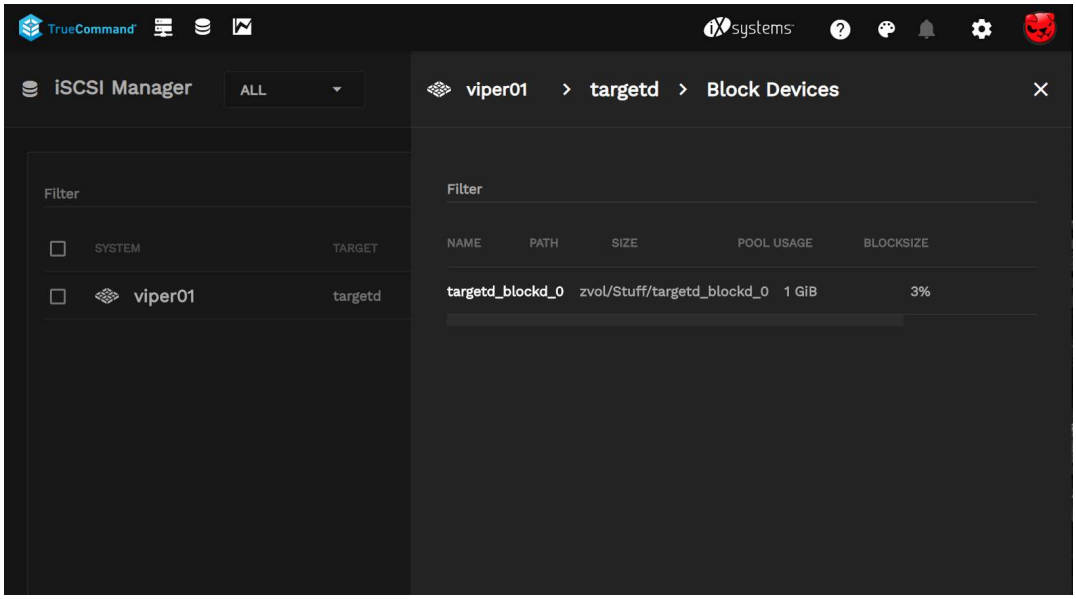
TrueCommand creates the iSCSI volume on the TrueNAS system and adds it to the iSCSI Manager.

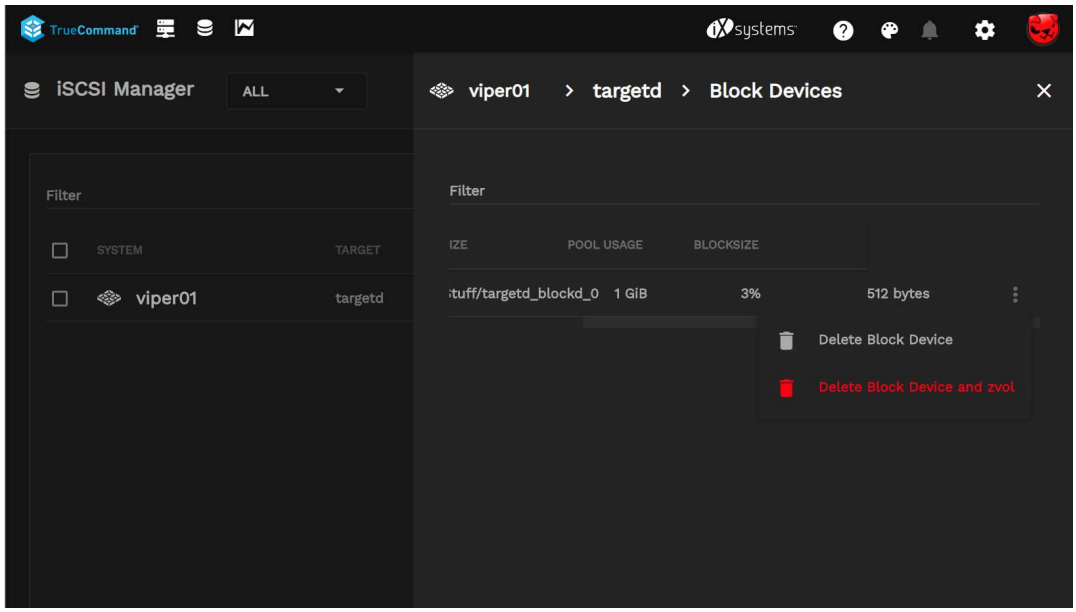


Using the TrueNAS web interface to update iSCSI settings takes approximately five minutes to resync with TrueCommand.

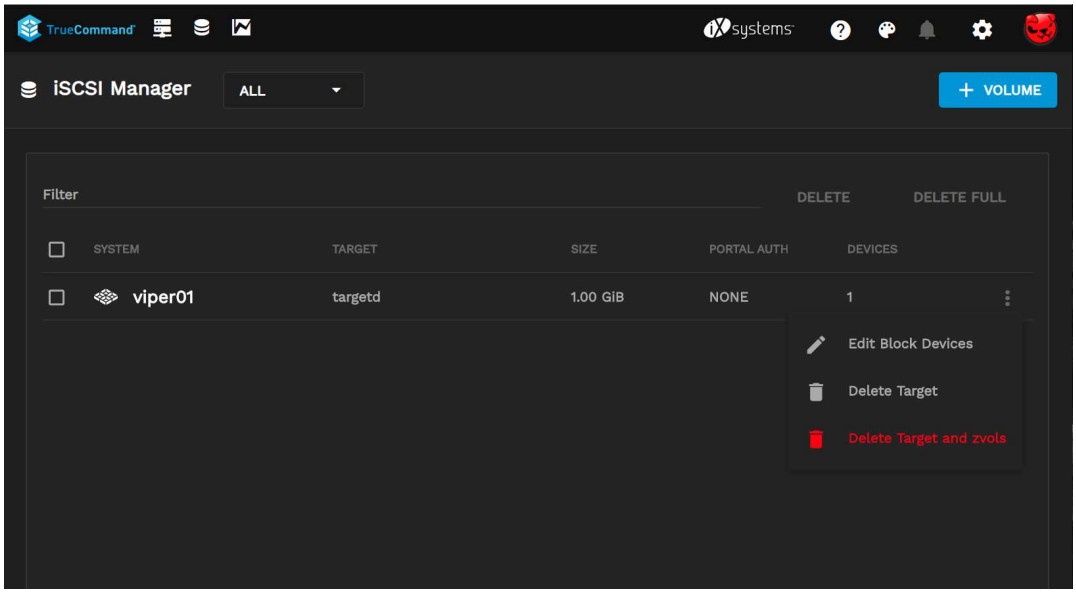
Deleting a Share

To delete a block device, open the options (three dots), select *Edit*, then click the three dots in the popout panel.





To delete the target click the three dots and select deleting target. To delete everything click the three dots and select deleting target + zvols is the “full” cleanup.



TrueCommand cannot delete Initiators and Init Groups because they can be tied to multiple targets. To remove these settings, delete them from each TrueNAS system.

10 - Recommendations

User-created recommendations are provided here, but be aware these are provided “as-is” and might not be officially supported by iXsystems, Inc.

Ready to get started? Choose a topic or article from the left-side Navigation pane. Click the **<** symbol to expand the menu to show the topics under this section.

10.1 - TrueCommand Cloud Security

The iX Portal

The iXsystems Account Services Portal is an easy to use site to manage TrueCommand Cloud Subscriptions and TrueNAS Mini Warranties.

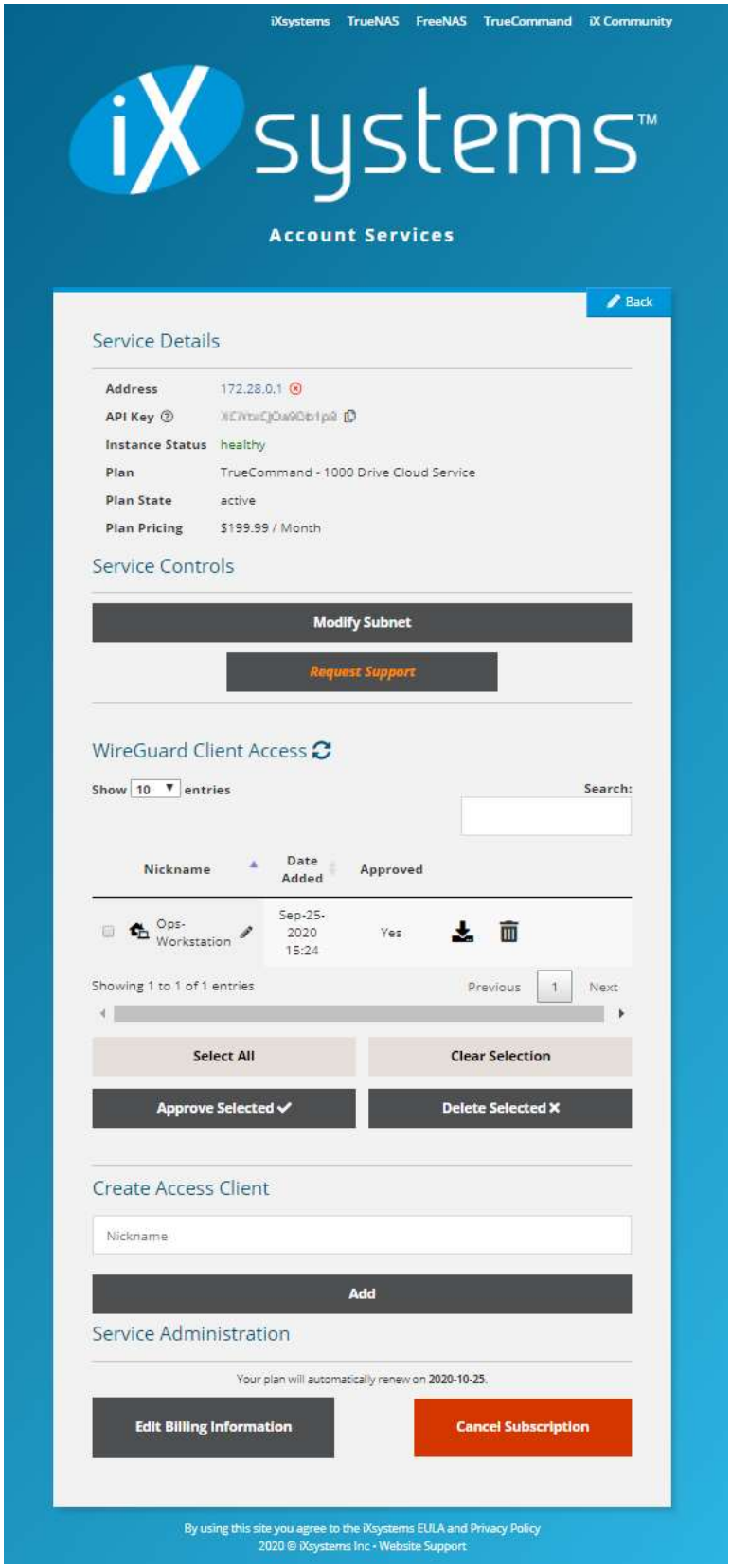
The iX Portal and TrueCommand Cloud use several security solutions to safeguard the application and connections.

- OAuth (Open Authorization) is an open standard for access rights and is a way for individuals on the Intenet to grant websites or applications access to their information on another website without divulging a password. Commonly, OAuth provides clients secure access to server resources on behalf of a resource owner. It is a process for site owners to authorize third-party access to their server without providing credentials.
- WireGuard is a open-source communication protocol that implements encrypted virtual private networks (VPNs). WireGaurd is designed to be easy to use, offer high speed performance, and have a low attack surface. WireGaurd is an alternative to IPsec and OpenVPN tunneling protocols.
- Two Factor Auth (2FA) is form of Multi-Factor Authentication method. 2FA is an extra layer of security to validate that an individual trying to gain access to an online account is actually who they say they are. A typical 2FA use case begins with a user entering their username and a password. Next, they are required to provide another piece of information. This second 'factor' could come from one of these categories: Something you know, Something you have, or Something you are. 2FA allows for one of those factors to be compromised and still prevent attackers from gaining access.

The iX Portal has the ability to use OAuth in place of a regular login and can utilize Two Factor Auth (2FA) if your OAuth provider provides that service.

The iX Portal also has email-based 2FA verification systems for sensitive operations to accounts.

TrueCommand Cloud services requires 2 forms of authentication. A user must have their username and password credentials to log in, but this depends on obtaining the Wireguard Configuration for their Client from the iX Portal. Administrators can create as many configurations as needed. Client configurations should never be used on more than one machine. TrueCommand Cloud logins can be across multiple systems, but each client system should use its own configuration. Client access can be revoked at any time from within the iX Portal.


iXsystems TrueNAS FreeNAS TrueCommand iX Community
iX systems™
Account Services
Back
Service Details
Address 172.28.0.1
API Key
Instance Status healthy
Plan TrueCommand - 1000 Drive Cloud Service
Plan State active
Plan Pricing $199.99 / Month
Service Controls
Modify Subnet
Request Support
WireGuard Client Access
Show 10 entries
Search:
Nickname
Date Added
Approved
Ops-Workstation
Sep-25-2020 15:24
Yes
Showing 1 to 1 of 1 entries
Previous 1 Next
Select All
Clear Selection
Approve Selected ✓
Delete Selected ✕
Create Access Client
Nickname
Add
Service Administration
Your plan will automatically renew on 2020-10-25.
Edit Billing Information
Cancel Subscription
By using this site you agree to the iXsystems EULA and Privacy Policy
2020 © iXsystems Inc • Website Support

11 - API Guide

TrueCommand API documentation is available from the web interface by opening the user menu and clicking **API**.

A static build of this version's API documentation is also provided here.

12 - Notices

12.1 - TrueCommand SaaS Agreement

Software as a Service Agreement

This Software as a Service Agreement (this **“Agreement”**) is a legally binding agreement between you (**“you”** or **“Customer”**) and iXsystems, Inc., a Delaware corporation (**“Provider”**). Provider and Customer may be referred to herein collectively as the **“Parties”** or individually as a **“Party.”** This Agreement governs your access to specific products, applications, tools, services and features that Provider makes available to you under an **“Order,”** as such term is hereafter defined.

WHEREAS, Provider provides access to the Services to its customers; and

WHEREAS, Customer desires to access the Services, and Provider desires to provide Customer access to the Services, subject to the terms and conditions of this Agreement.

WHEREAS, Customer’s right to access and use the Services, is expressly conditioned on your acceptance of this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. `<u>Definitions</u>.`

(a) **“Aggregated Statistics “** means data and information related to Customer’s use of the Services that is used by Provider in an aggregate and anonymized manner, including to compile statistical and performance information related to the provision and operation of the Services.

(b) **“Authorized User”** means Customer’s employees, consultants, contractors, clients, and agents (i) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement and (ii) for whom access to the Services has been purchased hereunder.

(c) **“Customer Data”** means, other than Aggregated Statistics, information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by or on behalf of Customer or an Authorized User through the Services.

(d) **“Documentation”** means Provider’s end user documentation relating to the Services available at www.truenas.com/docs/.

(e) “**Effective Date**” means the earliest of (i) the date you click **I** Agree; (ii) the date you access the Services; or (iii) the effective date set forth in the Order.

(f) “**Order**” means any order form or other ordering document, including any online subscription order specifying the level of the Services to be provided and the associated fees, and any addenda and supplements thereto. By entering into any Order, you agree to be bound by the terms of this Agreement.

(g) “**Provider IP**” means the Services, the Documentation, and any and all intellectual property provided to Customer or any Authorized User in connection with the foregoing. For the avoidance of doubt, Provider IP includes Aggregated Statistics and any information, data, or other content derived from Provider’s monitoring of Customer’s access to or use of the Services, but does not include Customer Data.

(h) “**Services**” means the products, applications, tools, services and features that Provider makes available to you as the software-as-a-service offering described in the Order.

(i) “**Third-Party Materials**” means materials and information, in any form or medium, including any open-source or other software, services (including, but not limited to, software as a service), documents, data, content, specifications, products, equipment, or components of or relating to the Services that are not proprietary to Provider.

2. Access and Use.

(a) Provision of Access. Subject to and conditioned on Customer’s payment of Fees and compliance with all other terms and conditions of this Agreement, Provider hereby grants Customer a non-exclusive, non-transferable (except in compliance with Section 12(g)) right to access and use the Services during the Term, solely for use by Authorized Users in accordance with the terms and conditions herein. Such use is limited to Customer’s legitimate business purposes. Provider shall provide to Customer the necessary passwords and network links or connections to allow Customer to access the Services.

(b) Documentation License. Subject to the terms and conditions contained in this Agreement, Provider hereby grants to Customer a non-exclusive, non-sublicensable, non-transferable (except in compliance with Section 12(g)) license to use the Documentation during the Term solely for Customer’s internal business purposes in connection with its use of the Services.

(c) Use Restrictions. Customer shall not use the Services for any purposes beyond the scope of the access granted in this Agreement. Customer shall not at any time, directly or indirectly, and shall not permit any Authorized Users to: (i) copy, modify, or create derivative works of the Services or Documentation, in whole or in part; (ii) rent, lease, lend, sell, license, assign, distribute, publish, transfer, or otherwise make available the Services or Documentation; (iii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Services, in whole or in part; (iv) remove any proprietary notices from the Services or Documentation; or (v) use the Services or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that

violates any applicable law.

(d) Reservation of Rights. Provider reserves all rights not expressly granted to Customer in this Agreement. Except for the limited rights and licenses expressly granted under this Agreement, nothing in this Agreement grants, by implication, waiver, estoppel, or otherwise, to Customer or any third party any intellectual property rights or other right, title, or interest in or to the Provider IP.

(e) Suspension. Notwithstanding anything to the contrary in this Agreement, Provider may temporarily suspend Customer's and any Authorized User's access to any portion or all of the Services if: (i) Provider reasonably determines that (A) there is a threat or attack on any of the Provider IP; (B) Customer's or any Authorized User's use of the Provider IP disrupts or poses a security risk to the Provider IP or to any other customer or vendor of Provider; (C) Customer, or any Authorized User, is using the Provider IP for fraudulent or illegal activities; (D) subject to applicable law, Customer has ceased to continue its business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding; or (E) Provider's provision of the Services to Customer or any Authorized User is prohibited by applicable law; (ii) any vendor of Provider has suspended or terminated Provider's access to or use of any third-party services or products required to enable Customer to access the Services; or (iii) in accordance with Section 5(a)(iii) (any such suspension described in subclause (i), (ii), or (iii), a "**Service Suspension**"). Provider shall use commercially reasonable efforts to provide written notice of any Service Suspension to Customer and to provide updates regarding resumption of access to the Services following any Service Suspension. Provider shall use commercially reasonable efforts to resume providing access to the Services as soon as reasonably possible after the event giving rise to the Service Suspension is cured. Provider will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Customer or any Authorized User may incur as a result of a Service Suspension.

(f) Aggregated Statistics. Notwithstanding anything to the contrary in this Agreement, Provider may collect and compile Aggregated Statistics. As between Provider and Customer, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are retained solely by Provider. Customer acknowledges that Provider may compile Aggregated Statistics based on Customer Data input into the Services. Customer agrees that Provider may (i) make Aggregated Statistics publicly available in compliance with applicable law, and (ii) use Aggregated Statistics to the extent and in the manner permitted under applicable law; provided that such Aggregated Statistics do not identify Customer or Customer's Confidential Information.

3. Customer Responsibilities.

(a) General. Customer is responsible and liable for all uses of the Services and Documentation resulting from access provided by Customer, directly or indirectly, whether such access or use is permitted by or in violation of this Agreement. Without limiting the generality of the foregoing, Customer is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Customer will be deemed a breach of this Agreement by Customer. Customer shall use reasonable efforts to make all Authorized Users aware of this Agreement's provisions as applicable to such Authorized User's use of the Services, and shall cause Authorized Users to comply with such provisions.

(b) Third-Party Materials. Provider may from time to time utilize Third-Party Materials in the provision of the Services. For purposes of this Agreement, such Third-Party Materials are subject to their own terms and conditions and the applicable flow-through provisions listed on www.ixsystems.com/support/, as amended. If Customer does not agree to abide by the applicable terms for any such Third-Party Materials, then Customer should not install or use the Services.

4. Service Levels and Support.

(a) Service Levels . Subject to the terms and conditions of this Agreement, Provider shall use commercially reasonable efforts to make the Services available in accordance with the service levels set out on the Order or as otherwise set forth in a separate Service Level Addendum.
(b) Support. The access rights granted hereunder entitle Customer to the support services described from time to time on Provider's website located at www.ixsystems.com/support/.

5. Fees and Payment.

(a) Fees. Customer shall pay Provider the fees ("**Fees**") as set forth in the Order, without offset or deduction. Customer shall make all payments hereunder in US dollars on or before the due date set forth on the Order. If Customer fails to make any payment when due, without limiting Provider's other rights and remedies, Provider may terminate this Agreement and Customer's and its Authorized Users' access to any portion or all of the Services, or suspend such access until such amounts are paid in full.

(b) Taxes. All Fees and other amounts payable by Customer under this Agreement are exclusive of taxes and similar assessments. Customer is responsible for all sales, use, and excise taxes, and any other similar taxes, duties, and charges of any kind imposed by any federal, state, or local governmental or regulatory authority on any amounts payable by Customer hereunder, other than any taxes imposed on Provider's income.

6. Confidential Information. From time to time during the Term, either Party may disclose or make available to the other Party information about its business affairs, products, confidential intellectual property, trade secrets, third-party confidential information, and other sensitive or proprietary information that is marked, designated, or otherwise identified as "confidential" (collectively, "**Confidential Information**"). Confidential Information does not include information that, at the time of disclosure is: (a) in the public domain; (b) known to the receiving Party at the time of disclosure; (c) rightfully obtained by the receiving Party on a non-confidential basis from a third party; or (d) independently developed by the receiving Party. The receiving Party shall not disclose the disclosing Party's Confidential Information to any person or entity, except to the receiving Party's employees who have a need to know the Confidential Information for the receiving Party to exercise its rights or perform its obligations hereunder. Notwithstanding the foregoing, each Party may disclose Confidential Information to the limited extent required (i) in order to comply with the order of a court or other governmental body, or as otherwise necessary to comply with applicable law, provided that the Party making the disclosure pursuant to the order shall first have given written notice to the other Party and made a reasonable effort to obtain a protective order; or (ii) to establish a Party's rights under this Agreement, including to make required court filings. On the expiration or termination of the Agreement, the receiving Party shall promptly return to the disclosing Party all copies, whether in written, electronic, or other form or media, of the disclosing Party's Confidential Information, or destroy all such copies and certify in writing to the disclosing Party that such Confidential Information has been destroyed. Each Party's obligations of non-disclosure with regard to Confidential Information are effective as of the Effective Date and will expire five years from the date first disclosed to the receiving Party; provided, however, with respect to any Confidential Information that constitutes a trade secret (as determined under

applicable law), such obligations of non-disclosure will survive the termination or expiration of this Agreement for as long as such Confidential Information remains subject to trade secret protection under applicable law.

7. Intellectual Property Ownership; Feedback.

(a) Provider IP. Customer acknowledges that, as between Customer and Provider, Provider owns all right, title, and interest, including all intellectual property rights, in and to the Provider IP and, with respect to Third-Party Materials, the applicable third-party providers own all right, title, and interest, including all intellectual property rights, in and to the Third-Party Materials.

(b) Customer Data. Provider acknowledges that, as between Provider and Customer, Customer owns all right, title, and interest, including all intellectual property rights, in and to the Customer Data. Customer hereby grants to Provider a non-exclusive, royalty-free, worldwide license to reproduce, distribute, and otherwise use and display the Customer Data and perform all acts with respect to the Customer Data as may be necessary for Provider to provide the Services to Customer, and a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to reproduce, distribute, modify, and otherwise use and display Customer Data incorporated within the Aggregated Statistics.

(c) Feedback. If Customer or any of its employees or contractors sends or transmits any communications or materials to Provider by mail, email, telephone, or otherwise, suggesting or recommending changes to the Provider IP, including without limitation, new features or functionality relating thereto, or any comments, questions, suggestions, or the like ("**Feedback**"), Provider is free to use such Feedback irrespective of any other obligation or limitation between the Parties governing such Feedback. Customer hereby assigns to Provider on Customer's behalf, and on behalf of its employees, contractors and/or agents, all right, title, and interest in, and Provider is free to use, without any attribution or compensation to any party, any ideas, know-how, concepts, techniques, or other intellectual property rights contained in the Feedback, for any purpose whatsoever, although Provider is not required to use any Feedback.

8. Warranty Disclaimer.

(a) THE PROVIDER IP IS PROVIDED "AS IS" AND PROVIDER HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. PROVIDER SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. PROVIDER MAKES NO WARRANTY OF ANY KIND THAT THE PROVIDER IP, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE.

9. Indemnification.

(a) Provider Indemnification.

(i) Provider shall indemnify, defend, and hold harmless Customer from and against any and all losses, damages, liabilities, costs (including reasonable attorneys' fees) ("**Losses**") incurred by Customer resulting from any third-party claim, suit, action, or proceeding ("**Third-Party Claim**") that the Services, or any use of the Services in accordance with this Agreement, infringes or misappropriates such third party's US patents, copyrights, or trade secrets, provided that Customer promptly notifies Provider in writing of the claim, cooperates with Provider, and allows Provider sole authority to control the defense and settlement of such claim.

(ii) If such a claim is made or appears possible, Customer agrees to permit Provider, at Provider's sole discretion, to (A) modify or replace the Services, or component or part thereof, to make it non-infringing, or (B) obtain the right for Customer to continue use. If Provider determines that neither alternative is reasonably available, Provider may terminate this Agreement, in its entirety or with respect to the affected component or part, effective immediately on written notice to Customer.

(iii) This Section 9(a) will not apply to the extent that the alleged infringement arises from: (A) use of the Services in combination with data, software, hardware, equipment, or technology not provided by Provider or authorized by Provider in writing; (B) modifications to the Services not made by Provider; (C) Customer Data ; or (D) Third-Party Materials.

(b) Customer Indemnification. Customer shall indemnify, hold harmless, and, at Provider's option, defend Provider from and against any Losses resulting from any Third-Party Claim that the Customer Data, or any use of the Customer Data in accordance with this Agreement, infringes or misappropriates such third party's intellectual property rights and any Third-Party Claims based on Customer's or any Authorized User's (i) negligence or willful misconduct; (ii) use of the Services in a manner not authorized by this Agreement; (iii) use of the Services in combination with data, software, hardware, equipment, or technology not provided by Provider or authorized by Provider in writing; or (iv) modifications to the Services not made by Provider, provided that Customer may not settle any Third-Party Claim against Provider unless Provider consents to such settlement, and further provided that Provider will have the right, at its option, to defend itself against any such Third-Party Claim or to participate in the defense thereof by counsel of its own choice.

(c) Sole Remedy. THIS SECTION 9 SETS FORTH CUSTOMER'S SOLE REMEDIES AND PROVIDER'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED CLAIMS THAT THE SERVICES INFRINGE, MISAPPROPRIATE, OR OTHERWISE VIOLATE ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY. IN NO EVENT WILL PROVIDER'S LIABILITY UNDER THIS SECTION 9 TWO TIMES THE TOTAL AMOUNTS PAID TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM OR ONE MILLION DOLLARS ($1,000,000), WHICHEVER IS LESS.

10. Limitations of Liability. IN NO EVENT WILL PROVIDER BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES; (b) INCREASED COSTS, DIMINUTION IN VALUE OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (c) LOSS OF GOODWILL OR REPUTATION; (d) USE, INABILITY TO USE, LOSS, INTERRUPTION, DELAY, OR RECOVERY OF ANY DATA, OR BREACH OF DATA OR SYSTEM SECURITY; OR (e) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER PROVIDER WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE. IN NO EVENT WILL

PROVIDER'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE EXCEED TWO TIMES THE TOTAL AMOUNTS PAID TO PROVIDER UNDER THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM OR ONE MILLION DOLLARS ($1,000,000), WHICHEVER IS LESS.

11. Term and Termination.

(a) Term. The term of this Agreement begins on the Effective Date and, unless terminated earlier pursuant to this Agreement's express provisions, will continue in effect until such date as provided on the Order (the "**Term**").

(b) Termination. In addition to any other express termination right set forth in this Agreement:

(i) Provider may terminate this Agreement, effective on written notice to Customer, if Customer: (A) fails to pay any amount when due under an Order; or (B) breaches any of its obligations under Section 2(c) or Section 6;

(ii) either Party may terminate this Agreement, effective on written notice to the other Party, if the other Party materially breaches this Agreement, and such breach: (A) is incapable of cure; or (B) being capable of cure, remains uncured 30 days after the non-breaching Party provides the breaching Party with written notice of such breach; or

(iii) either Party may terminate this Agreement, effective immediately upon written notice to the other Party, if the other Party: (A) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (B) files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law; (C) makes or seeks to make a general assignment for the benefit of its creditors; or (D) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

(c) Effect of Expiration or Termination. Upon expiration or earlier termination of this Agreement, Customer shall immediately discontinue use of the Provider IP and, without limiting Customer's obligations under Section 6, Customer shall delete, destroy, or return all copies of the Provider IP and certify in writing to the Provider that the Provider IP has been deleted or destroyed. Provider may delete or destroy all copies of Customer Data in its system or otherwise in its possession or control upon the expiration or termination of this Agreement. No expiration or termination will affect Customer's obligation to pay all Fees that may have become due before such expiration or termination or entitle Customer to any refund.

(d) Survival. This Section 11(d) and Section 1, 5, 6, 7, 8, 9, 10, and 12 survive any termination or expiration of this Agreement. No other provisions of this Agreement survive the expiration or earlier termination of this Agreement.

12. Miscellaneous.

(a) Entire Agreement. This Agreement, together with any other documents incorporated herein by reference and all related addenda and exhibits, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, and representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related addenda and exhibits, and any other documents incorporated herein by reference, the following order of precedence governs: (i) first, the Order; (ii) second, this Agreement; (iii) third, any other documents incorporated herein by reference.

(b) Notices. All notices, requests, consents, claims, demands, waivers, and other communications hereunder (each, a "**Notice**") must be in writing and addressed to the Parties at the addresses set forth on the Order (or to such other address that may be designated by the Party giving Notice from time to time in accordance with this Section). All Notices must be delivered by personal delivery, nationally recognized overnight courier (with all fees pre-paid), facsimile or email (with confirmation of transmission), or certified or registered mail (in each case, return receipt requested, postage pre-paid). Except as otherwise provided in this Agreement, a Notice is effective only: (i) upon receipt by the receiving Party; and (ii) if the Party giving the Notice has complied with the requirements of this Section.

(c) Force Majeure. In no event shall either Party be liable to the other Party, or be deemed to have breached this Agreement, for any failure or delay in performing its obligations under this Agreement (except for any obligations to make payments), if and to the extent such failure or delay is caused by any circumstances beyond such Party's reasonable control, including but not limited to acts of God, flood, fire, earthquake, explosion, war, terrorism, invasion, riot or other civil unrest, strikes, labor stoppages or slowdowns or other industrial disturbances, or passage of law or any action taken by a governmental or public authority, including imposing an embargo.

(d) Amendment and Modification; Waiver. No amendment to or modification of this Agreement is effective unless it is in writing and signed by an authorized representative of each Party. No waiver by any Party of any of the provisions hereof will be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, (i) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof, and (ii) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

(e) Severability. If any provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties shall negotiate in good faith to modify this Agreement so as to effect their original intent as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

(f) Governing Law; Submission to Jurisdiction. This Agreement is governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of the State of California. Any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of California in each case located in San Jose, California, and each Party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action, or proceeding.

(g) Assignment. Customer may not assign any of its rights or delegate any of its obligations hereunder, in each case whether voluntarily, involuntarily, by operation of law or otherwise, without the prior written consent of Provider, which consent shall not be unreasonably withheld, conditioned, or delayed. Any purported assignment or delegation in violation of this Section will be null and void. No assignment or delegation will relieve the assigning or delegating Party of any of its obligations hereunder. This Agreement is binding upon and inures to the benefit of the Parties and their respective permitted successors and assigns.

(h) Export Regulation. Customer shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), that prohibit or restrict the export or re-export of the Services or any Customer Data outside the US.

(i) US Government Rights. Each of the Documentation and the software components that constitute the Services is a “commercial item” as that term is defined at 48 C.F.R. § 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. § 12.212. Accordingly, if Customer is an agency of the US Government or any contractor therefor, Customer only receives those rights with respect to the Services and Documentation as are granted to all other end users, in accordance with (a) 48 C.F.R. § 227.7201 through 48 C.F.R. § 227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. § 12.212, with respect to all other US Government users and their contractors.

(j) Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 6 or, in the case of Customer, Section 2(c), would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

(k) Acceptance. You accept this Agreement, by: (i) checking the box indicating acceptance or (ii) signing an Order that references and incorporates this Agreement. If the individual accepting this Agreement is accepting on behalf of a company or other legal entity, such individual represents that they have the authority to bind such entity and its affiliates to these terms and conditions, in which case the term “Customer” shall refer to such entity and its affiliates. If the individual accepting this Agreement does not have such authority, or does not agree with the terms and conditions of this Agreement, such individual must not accept this agreement or use the Services.

SERVICE LEVEL ADDENDUM

Capitalized terms used but not defined in this Service Level Addendum (“SLA”) shall have the meaning given to those terms in the Software as a Service Agreement by and between iXsystems, Inc. and _____.

The parties intend to review this on either party's reasonable request. Any revisions to the service levels must be authorized by both parties.

1. Defined Terms. For purposes of this SLA, the following terms shall have the following meanings:

"**Key Performance Indicator (KPI)**" means a Service Level measurement that is not subject to Service Credits, but that is important to Customer's business. Upon reasonable notice, Customer may request that a KPI be converted to a Service Level, in which case the parties will negotiate in good faith a Service Credit applicable to such measurement. The parties will amend this SLA to reflect any such change.

"**Service Credit**" means a percentage of Service Fees to be credited to Customer if Provider fails to meet a Service Level, as set forth in this SLA.

"**Service Level**" means a performance standard that Provider is required to meet in providing the Services, as set forth in this SLA.

2. Service Scope. This SLA covers the following Services:

3. [LIST OF INCLUDED SERVICES]

This SLA does not cover the following:

[LIST OF EXCLUDED SERVICES]

3. Customer Obligations. The Customer's responsibilities and obligations in support of this SLA include the following:

(a) Providing information, and authorizations, as required by the Provider for performing the Services.

(b) Adhering to policies and processes established by the Provider for reporting service failures and incidents and prioritizing service requests.

(c) Making a representative available (i) for regular meetings to review the SLA and (ii) to consult with the Provider for resolving service-related incidents or requests.

(d) Paying fees and costs as required by the Agreement.

4. Provider Obligations. The Provider's responsibilities and obligations in support of this SLA include:

(a) Meeting applicable incident response times.

(b) Adhering to the Customer's policies and practices as applicable to the performance of the Services.

(c) Making a representative available (i) for regular meetings to review the SLA and (ii) to resolve service-related incidents or requests.

5. Assumptions. Provider's performance of the Services under this SLA is subject to the following assumptions, constraint, and dependencies:

(a) Information provided by Customer to Provider as required for the Services will be accurate and timely.

(b) Provider's procedures and delivery of Services may be affected by changes in relevant Customer internal policies or in applicable laws or regulations.

6. Service Levels and Service Credits.

(a) The following table sets forth the Services measured under this SLA, the applicable Service Levels, and the Service Credits to which Customer will be entitled if Provider fails to meet the Service Levels during any monthly measurement period. The total amount of Service Credits shall not exceed 100% of Provider's fees in any monthly measurement period.

Service	Measurement	Service Level	Service Credit
[SERVICE A]	[CALCULATION]	[NUMBER][%/[UNIT]]	[NUMBER]%
[SERVICE B]	[CALCULATION]	[NUMBER][%/[UNIT]]	[NUMBER]%

(c) The Service Credits set forth in this SLA shall be considered liquidated damages or Customer's sole and exclusive remedy for Provider's failure to meet Service Levels. Customer shall not be entitled to any other rights or remedies set forth in the Agreement.

7. Other Terms and Conditions.

(a) Single Point of Contact. Provider and Customer shall each appoint a person (a "Single Point of Contact") who shall be available to receive communications and coordinate responses to questions or failures with respect to the Service Levels. Notwithstanding the foregoing sentence, in the event of any emergency relating to any Service, a party shall attempt to contact the appointed Single Point of Contact of the other party, but may also directly contact any person most able to resolve the emergency quickly. The initial Single Points of Contact for each party shall be:

For Provider: [NAME AND TITLE]

For Customer: [NAME AND TITLE]

Either party may change its Single Point of contact upon notice to the other party.

12.2 - TrueCommand Terms of Service

iXsystems Software End User License Agreement

Important - Please Read This EULA Carefully

PLEASE CAREFULLY READ THIS END USER LICENSE AGREEMENT (EULA) BEFORE CLICKING THE AGREE BUTTON. THIS AGREEMENT SERVES AS A LEGALLY BINDING DOCUMENT BETWEEN YOU AND IXSYSTEMS, INC. BY CLICKING THE AGREE BUTTON, DOWNLOADING, INSTALLING, OR OTHERWISE USING IXSYSTEMS SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS IN THIS AGREEMENT, DO NOT USE OR INSTALL IXSYSTEMS SOFTWARE.

This agreement is provided in accordance with the Commercial Arbitration Rules of the American Arbitration Association (the “AAA Rules”) under confidential binding arbitration held in Santa Clara County, California. To the fullest extent permitted by applicable law, no arbitration under this EULA will be joined to an arbitration involving any other party subject to this EULA, whether through class arbitration proceedings or otherwise. Any litigation relating to this EULA shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California. All matters arising out of or relating to this agreement shall be governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule.

1.0 Definitions

1.1 “Company”, **“iXsystems”** and **“iX”** means iXsystems, Inc., on behalf of themselves, subsidiaries, and affiliates under common control.

1.2 “iXsystems Software” means the iXsystems software.

1.3 “Device” means digital computer equipment and peripheral equipment.

1.4 “Product” means, individually and collectively, iXsystems Software.

1.5 “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements, each of which has its own copyright and its own applicable license terms.

1.6 “Licensee”, **“You”** and **“Your”** refers to the person, organization, or entity that has agreed to be bound by this EULA including any employees, affiliates, and third party contractors that provide services to You.

1.7 “Agreement” refers to this document, the iXsystems End User License Agreement.

2.0 License

Subject to the terms set forth in this Agreement, iXsystems grants You a non-exclusive, non-transferable, revocable, limited license without the option to sublicense, to use iXsystems Software on Your Device(s) in accordance with Your authorized purchase and use of a Product(s) or iXsystems Software for Your internal business purposes. This use includes but is not limited to using or viewing the instructions, specifications, and documentation provided with the Product.

3.0 License Restrictions

The Product, is protected by copyright laws and international treaties, as well as other intellectual property laws, statutes, and treaties. The Product is licensed, not sold to You the end user. You do not acquire any ownership interest in the Product or any other rights to such Product, other than to use such Product in accordance with the license granted under this Agreement, subject to all terms, conditions, and restrictions. iXsystems reserves and shall retain its entire right, title, and interest in and to the Product, and all intellectual property rights arising out of or relating to the Product, subject to the license expressly granted to You in this Agreement.

The Product may contain iXsystems’ trademarks, trade secrets, and proprietary collateral. iXsystems strictly prohibits the acts of decompiling, reverse engineering, or disassembly of the Product. You agree to use commercially reasonable efforts to safeguard the Product and iXsystems’ intellectual property, trade secrets, or other proprietary information You may have access to, from infringement, misappropriation, theft, misuse, or unauthorized access. You will promptly notify iXsystems if You become aware of any infringement of the Product and cooperate with iXsystems in any legal action taken by iXsystems to enforce its intellectual property rights. By accepting this Agreement, You agree You will not disclose, copy, transfer, or publish benchmark results relating to the Product without the express written consent of iXsystems. You agree not to use, or permit others to use, the Product beyond the scope of the license granted under Section 2, unless otherwise permitted by iXsystems, or in violation of any law, regulation or rule, and you will not modify, adapt, or otherwise create derivative works or improvements of the Product. You are responsible and liable for all uses of the Product through access thereto provided by You, directly or indirectly.

4.0 General

4.1 Entire Agreement - This Agreement, together with any associated purchase order, service level agreement, and all other documents and policies referenced herein, constitutes the entire agreement between You and iXsystems for use of the iXsystems Software and all other prior negotiations, representations, agreements, and understandings are superseded hereby. No agreements altering or supplementing the terms hereof may be made except by means of a written document signed by Your duly authorized representatives and those of iXsystems.

4.2 Waiver and Modification - No failure of either party to exercise or enforce any of its rights under this EULA will act as a waiver of those rights. This EULA may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

4.3 Severability - If any provision of this EULA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this EULA will not be affected.

4.4 United States Government End Users - For any Product licensed directly or indirectly on behalf of a unit or agency of the United States Government, this paragraph applies. Company's proprietary software embodied in the Product: (a) was developed at private expense and is in all respects Company's proprietary information; (b) was not developed with government funds; (c) is Company's trade secret for all purposes of the Freedom of Information Act; (d) is a commercial item and thus, pursuant to Section 12.212 of the Federal Acquisition Regulations (FAR) and DFAR Supplement Section 227.7202, Government's use, duplication or disclosure of such software is subject to the restrictions set forth by the Company and Licensee shall receive only those rights with respect to the Product as are granted to all other end users.

4.5 Foreign Corrupt Practices Act - You will comply with the requirements of the United States Foreign Corrupt Practices Act (the "FCPA") and will refrain from making, directly or indirectly, any payments to third parties which constitute a breach of the FCPA. You will notify Company immediately upon Your becoming aware that such a payment has been made. You will indemnify and hold harmless Company from any breach of this provision.

4.6. Title - iXsystems retains all rights, titles, and interest in iXsystems Software and in and all related copyrights, trade secrets, patents, trademarks, and any other intellectual and industrial property and proprietary rights, including registrations, applications, registration keys, renewals, and extensions of such rights.

4.7 Contact Information - If You have any questions about this Agreement, or if You want to contact iXsystems for any reason, please email legal@ixsystems.com.

4.8 Maintenance and Support - You may be entitled to support services from iXsystems after purchasing iXsystems Software, Products, or a support contract. iXsystems will provide these support services based on the length of time of the purchased support contract. This maintenance and support is only valid for the length of time that You have purchased with the Product. iXsystems may from time to time and at their sole discretion vary the terms and conditions of the maintenance and support agreement based on different business environmental and personnel factors. For more information on our Maintenance and Support contract, refer to ixsystems.com/iXsystems_SLA.

4.9 Force Majeure - iXsystems will not be deemed to be in default of any of the provisions of this Agreement or be liable for any delay or failure in performance due to Force Majeure, which shall include without limitation acts of God, earthquake, weather conditions, labor disputes, changes in law, regulation or government policy, riots, war, fire, epidemics, acts or omissions of vendors or suppliers, equipment failures, transportation difficulties, malicious or criminal acts of third parties, or other occurrences which are beyond iXsystems' reasonable control.

4.10 Termination - iXsystems may terminate or suspend Your license to use the Product or Software and cease any and all support, services, or maintenance under this Agreement without prior notice, or liability, and for any reason whatsoever, including, without limitation, if any of the terms and conditions of this Agreement are breached. Upon termination, rights to use the Product and Software will immediately cease. Other provisions of this Agreement will survive termination including, without limitation, ownership provisions, warranty disclaimers, indemnity, and limitations of liability.

4.11 Open Source Software Components - iXsystems uses Open Source Software components in the development of the Software and Product. Open Source Software components that are used in the Product are composed of separate components each having their own trademarks, copyrights, and license conditions.

4.12 Assignment - Licensee shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without iXsystems' prior written consent. No delegation or other transfer will relieve Licensee of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section is void. iXsystems may freely assign or otherwise transfer all or any of its rights, or delegate or otherwise transfer all or any of its obligations or performance, under this Agreement without Licensee's consent. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

5.0 Export Control Regulations

The Product or Software may be subject to US export control laws, including the US Export Administration Act and its associated regulations. You shall not, directly or indirectly, export, re-export, or release the Product to, or make the Product accessible from, any jurisdiction or country to which export, re-export, or release is prohibited by law, rule, or regulation. You shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the Product available outside the US.

6.0 Data Collection and Privacy

iXsystems Software may collect information relating to Your use of the Product, including information that has been provided directly or indirectly through automated means. Usage of iXsystems Software, geolocation information, user login credentials, and device and operating system identification are allowed according to iXsystems' privacy policy. By accepting this Agreement and continuing to use the Product, you agree that iXsystems may use any information provided through direct or indirect means in accordance with our privacy policy and as permitted by applicable law, for purposes relating to management, compliance, marketing, support, security, update delivery, and product improvement.

7.0 Limitation of Liability and Disclaimer of Warranty

THE PRODUCT IS PROVIDED "AS IS" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IXSYSTEMS, ON ITS OWN BEHALF AND ON BEHALF OF ITS AFFILIATES AND ITS AND THEIR RESPECTIVE LICENSORS AND SERVICE PROVIDERS, EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE PRODUCT, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND WARRANTIES THAT MAY ARISE OUT OF COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, OR TRADE PRACTICE. WITHOUT LIMITATION TO THE FOREGOING, IXSYSTEMS PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE PRODUCT WILL MEET THE LICENSEE'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE, OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS, OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE, OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW: (A) IN NO EVENT WILL IXSYSTEMS OR ITS AFFILIATES, OR ANY OF ITS OR THEIR RESPECTIVE LICENSORS OR SERVICE PROVIDERS, BE LIABLE TO LICENSEE, LICENSEE'S AFFILIATES, OR ANY THIRD PARTY FOR ANY USE, INTERRUPTION, DELAY, OR INABILITY TO USE THE PRODUCT; LOST REVENUES OR PROFITS; DELAYS, INTERRUPTION, OR LOSS OF SERVICES, BUSINESS, OR GOODWILL; LOSS OR CORRUPTION OF DATA; LOSS RESULTING FROM SYSTEM OR SYSTEM SERVICE FAILURE, MALFUNCTION, OR SHUTDOWN; FAILURE TO ACCURATELY TRANSFER, READ, OR TRANSMIT INFORMATION; FAILURE TO UPDATE OR PROVIDE CORRECT INFORMATION; SYSTEM INCOMPATIBILITY OR PROVISION OF INCORRECT COMPATIBILITY INFORMATION; OR BREACHES IN SYSTEM SECURITY; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES, WHETHER ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT IXSYSTEMS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; (B) IN NO EVENT WILL IXSYSTEMS' AND ITS AFFILIATES', INCLUDING ANY OF ITS OR THEIR RESPECTIVE LICENSORS' AND SERVICE PROVIDERS', COLLECTIVE AGGREGATE LIABILITY UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ITS SUBJECT MATTER, UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, EXCEED THE TOTAL AMOUNT PAID TO IXSYSTEMS PURSUANT TO THIS AGREEMENT FOR THE PRODUCT THAT IS THE SUBJECT OF THE CLAIM; (C) THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF THE LICENSEE'S REMEDIES UNDER THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE.

You hereby acknowledge that you have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein by accepting this agreement or continuing to use this product.

12.3 - End of Life Notices

12.3.1 - TrueCommand 1.1

September 29, 2020

TrueCommand 1.1 has reached its End of Life and is no longer receiving security updates. The TrueCommand 1.3.2 release announcement can be found at https://www.ixsystems.com/blog/truecommand-1-3-2/.

Please schedule a time to upgrade to the latest version of TrueCommand. If assistance is required, please contact the iXsystems Support Team.

Contact Method	Contact Options
Web	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone	Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time: US-only toll-free: 1-855-473-7449 option 2 Local and international: 1-408-943-4100 option 2
Telephone	After Hours (24x7 Gold Level Support only): US-only toll-free: 1-855-499-5131 International: 1-408-878-3140 (international calling rates will apply)

12.3.2 - TrueCommand 1.0

September 29, 2020

TrueCommand 1.0 has reached its End of Life and is no longer receiving security updates. The TrueCommand 1.3.2 release announcement can be found at https://www.ixsystems.com/blog/truecommand-1-3-2/.

Please schedule a time to upgrade to the latest version of TrueCommand. If assistance is required, please contact the iXsystems Support Team.

Contact Method	Contact Options
Web	https://support.ixsystems.com
Email	support@ixsystems.com
Telephone	Monday - Friday, 6:00AM to 6:00PM Pacific Standard Time: US-only toll-free: 1-855-473-7449 option 2 Local and international: 1-408-943-4100 option 2
Telephone	After Hours (24x7 Gold Level Support only): US-only toll-free: 1-855-499-5131 International: 1-408-878-3140 (international calling rates will apply)