



TeamDrive Host Server Installation and Configuration

Release 3.0.013.6

Lenz Grimmer, Barry Leslie, Paul McCullagh, Eckhard Pruehs

December 09, 2014

1	Copyright Notice	1
2	Trademark Notice	3
3	Introduction	5
3.1	Hardware Requirements	5
3.2	Operating System Requirements	5
3.3	Required Skills	6
3.4	Storage Requirements	6
3.5	Network Requirements	6
4	Introduction to the TeamDrive Hosting Service	9
4.1	TeamDrive Hosting Service Overview	9
4.2	TeamDrive Hosting Basics	12
4.3	Directory Structure of Hosted Data	12
4.4	Spaces, Owners, and Depots	13
4.5	Background Tasks Performed by <code>td-hostserver</code>	13
5	Operating System Configuration	15
5.1	Installing a base operating system	15
5.2	Enable Time Synchronization with NTP	15
5.3	Disable SELinux	15
5.4	Firewall configuration	15
6	Installing the Host Server Components	17
6.1	Enable the TeamDrive Host Server <code>yum</code> Repository	17
6.2	Download and Install the TeamDrive Host Server Package	17
7	Apache <code>http</code> Server Installation and Configuration	19
7.1	Update <code>httpd.conf</code>	19
7.2	Disable Unneeded Apache Modules	19
7.3	Configure <code>mod_ssl</code>	20
8	MySQL Installation and Configuration	21
8.1	Installing MySQL Server	21
8.2	Creating TeamDrive MySQL User and Databases	23
9	Initial Host Server Configuration	25
9.1	Mount the Space Storage Volume	25
9.2	Starting the Host Server Instance	25
9.3	Registering and Activating the Host Server	26
9.4	Setup and Administration	29
9.5	Host Servers (Hosts)	29
9.6	Volumes	31
9.7	Associating the Host Server with a Provider	32
9.8	Testing Client Access	32

10 Post-Installation Tasks	33
10.1 Starting the Apache http Server at Boot Time	33
10.2 Starting TeamDrive Service at Boot Time	33
10.3 Installing SSL certificates	33
10.4 Next steps	33
11 Troubleshooting	35
11.1 List of relevant configuration files	35
11.2 List of relevant log files	35
11.3 Common errors	36
12 Appendix	39
12.1 Abbreviations	39
13 Release Notes - Version 3.0.013	41
14 Release Notes - Version 3.0.011 and older	45
15 Document History	47

COPYRIGHT NOTICE

Copyright © 2014, TeamDrive Systems GmbH. All rights reserved.

TeamDrive Systems GmbH

<https://www.teamdrive.com>

Max-Brauer-Allee 50

22765 Hamburg, Germany

Email: info@teamdrive.com

TRADEMARK NOTICE

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Apache HTTP Server, Apache, and the Apache feather logo are trademarks of The Apache Software Foundation.

MySQL is a registered trademark of Oracle and/or its affiliates.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices.

VMware is a trademark or registered trademark of VMware, Inc. in the United States and/or other jurisdictions.

“Amazon Web Services”, “Amazon S3” are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries.

“Red Hat Linux” and “CentOS” are trademarks of Red Hat, Inc. in the U.S. and other countries.

All other names and trademarks used herein are the property of their respective owners.

INTRODUCTION

The TeamDrive Host Server provides the scalable storage component required for TeamDrive Clients to store their Space data.

This manual will guide you through the installation of your own local hosting service for TeamDrive. This document is intended for administrators who need to install and configure a TeamDrive Hosting Service.

Warning: The TeamDrive Host Server installation requires a running TeamDrive Registration Server instance. If you are setting up both components on your own premises, please start with setting up the Registration Server as outlined in the TeamDrive Registration Server installation guides. If you are using a Registration Server instance hosted by some other service provider, make sure you can access it and you have performed an initial setup/configuration already.

3.1 Hardware Requirements

To operate a TeamDrive Hosting Service you need a **64-bit** system with a minimum of 2 processors (or 1 processor with dual-core or quad-core), a minimum of 2 GB RAM and a redundant storage system (e.g. RAID-5) that is sufficiently large and scalable if required.

The exact sizing depends heavily on the anticipated number of concurrent client connections, the bandwidth required and the amount of space data to be stored. Please contact us via sales@teamdrive.net for assistance.

We recommend a quad-core processor with 8 GB RAM.

3.2 Operating System Requirements

We recommend using a recent 64-bit version of **Red Hat Enterprise Linux 6** (RHEL 6) or a derivative distribution like **CentOS 6**, **Oracle Linux 6** or **Scientific Linux 6** as the operating system platform.

This document is written with this OS environment in mind — the names of packages, configuration files and path names might be different on other Linux distributions. If you have any questions about using other Linux distributions, please contact sales@teamdrive.net.

You will need at least Apache http Server version 2.2.9 (version 2.4 is currently not supported) which should be configured using the “prefork” MPM (<http://httpd.apache.org/docs/2.2/mod/prefork.html>). The prefork option is more scalable under load than the worker option and is usually the default configuration on Linux distributions.

The TeamDrive Host Server processes need to open a large number of file descriptors. Make sure that the values in `ulimit` are set sufficiently high, e.g. by setting “nofile — max number of open files” in file `/etc/security/limits.conf`.

In addition, the TeamDrive Hosting Service requires the Yvva Runtime Environment version 1.0.0 or later, and a MySQL Database Server version 5.1 or later (MySQL 5.5 or 5.6 are recommended for performance reasons).

3.3 Required Skills

When installing the TeamDrive Hosting Service, we assume that you have basic knowledge of:

- VMware: importing and deploying virtual machines, configuring virtual networking and storage (when using a pre-installed Virtual Appliance)
- **Linux system administration:**
 - Adding/configuring software packages
 - Editing configurations files
 - Starting/stopping services
 - Creating user accounts
 - Assigning file ownerships and privileges
 - Creating and mounting file systems
 - Setting up environment variables
- Apache web server: installation and configuration, adding and enabling modules, modifying configuration files
- MySQL Database: installation and configuration, administration/maintenance, using the MySQL command line client, basic SQL
- Basic knowledge of application server technology

3.4 Storage Requirements

Storage Volumes are used to store the TeamDrive Clients' Space data, so they can grow quite significantly in size. We strongly suggest to place them on a dedicated file system/storage volume or an NFS mount that supports proper file locking (e.g. NFSv4).

When using a block device like a local/virtual hard disk or an iSCSI target, we suggest using ext3, ext4 or XFS on top of a logical volume (LVM) as the file system for this storage area. Using LVM provides some additional flexibility for increasing the storage capacity of a single volume dynamically.

It should be ensured that the Space storage volumes that are mounted on the servers are equipped with sufficient security measures against failure and data loss. Strategies could include mirrored drives or some form of RAID at the minimum; even better is a SAN system with upstream NAS heads. Alternatively, block-by-block replication (as provided by many enterprise storage systems) can be implemented.

3.5 Network Requirements

The bandwidth of the Host Server's network interface plays a vital role in defining the overall performance and responsiveness of the TeamDrive Service. Clients need to be able to quickly upload new Space data, so it is available for download for all other Clients invited to that Space. Usually, the amount of outgoing traffic (delivering Space data to clients) exceeds the inbound traffic.

The system must have IP connectivity, using a fixed IP address and a resolvable fully qualified domain name. This host name becomes part of the URLs used by the TeamDrive clients to access the TeamDrive Spaces and can not be changed once the service is in operation. The Host Server itself needs to be able to properly resolve host names, too.

If the Host Server is located behind a firewall, please ensure that it is reachable via HTTP (TCP port 80) and HTTPS (TCP port 443) by the TeamDrive Clients.

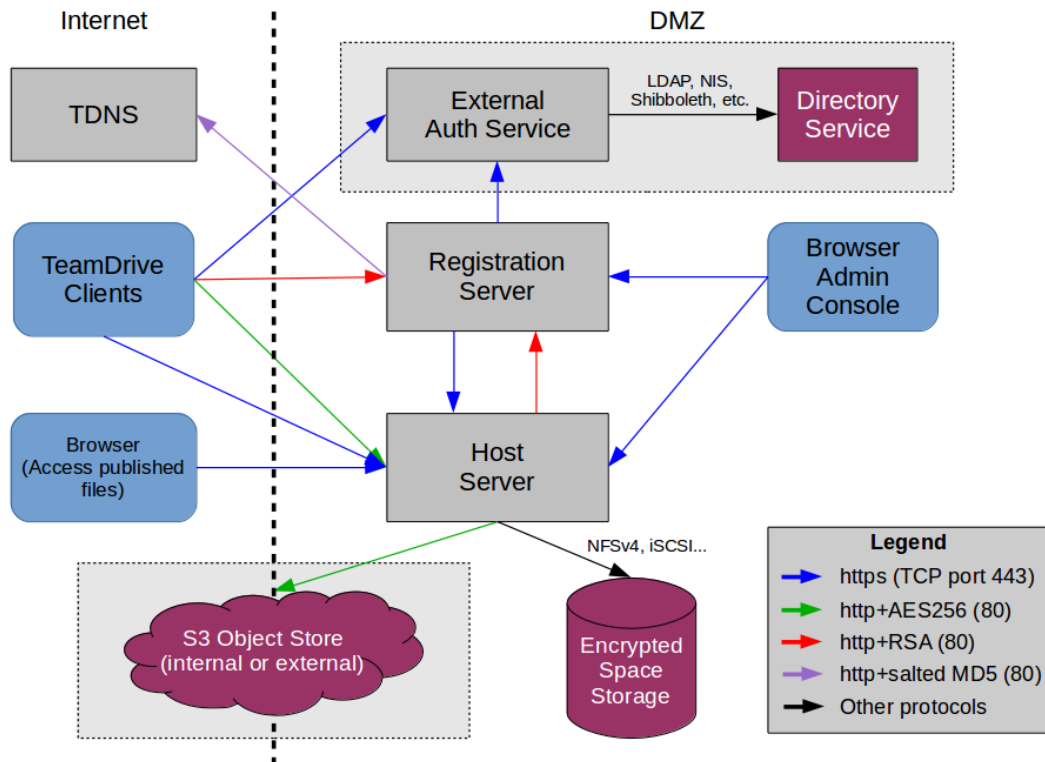


Figure 3.1: TeamDrive Hosting Service Networking Overview

For the initial registration and the exchange of cryptographic keys, the Host Server must be able to establish HTTP connections (TCP port 80) to the Registration Server. After the registration and activation, no further connections from the Host Server to the Registration Server will be established.

To perform API calls (e.g. to create new Space Depots or to query for existing Spaces for a particular user), the TeamDrive Registration Server must be able to establish outgoing HTTP/HTTPS connections to the TeamDrive Hosting Service.

INTRODUCTION TO THE TEAMDRIVE HOSTING SERVICE

4.1 TeamDrive Hosting Service Overview

The TeamDrive Hosting Service consists of a number of components which are illustrated below:

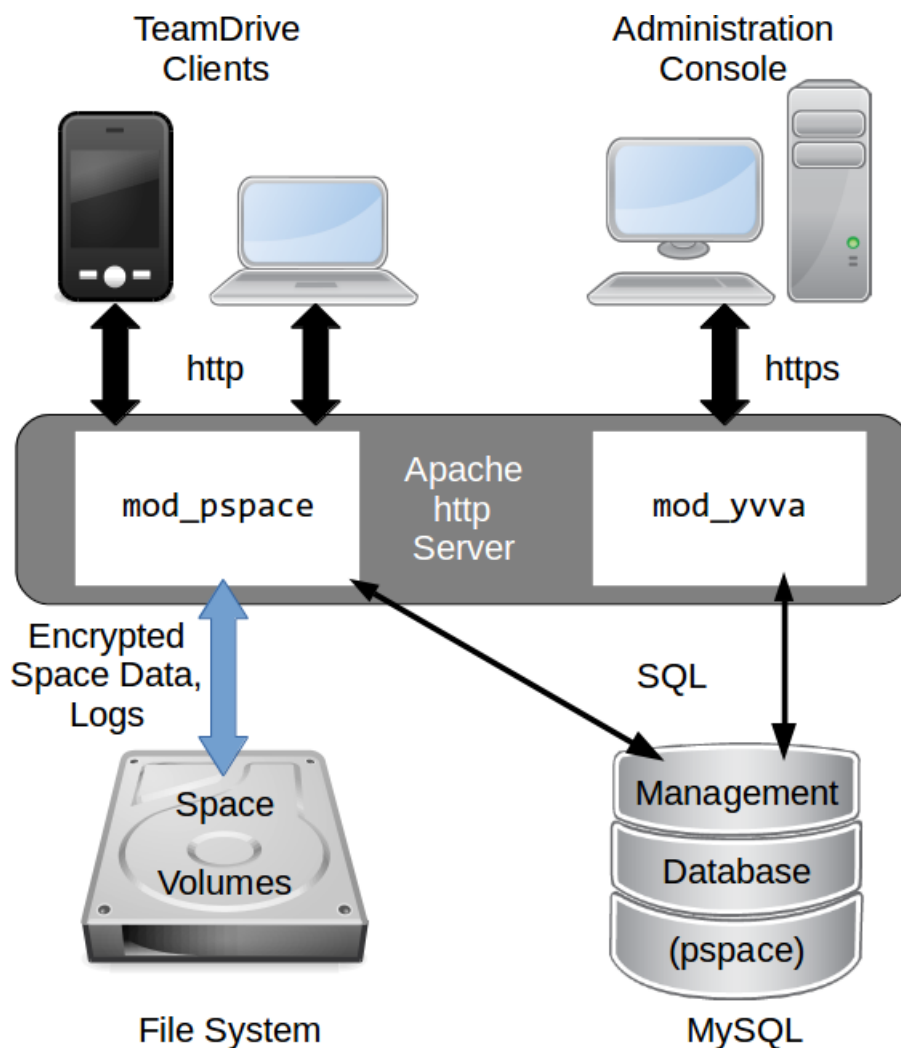


Figure 4.1: TeamDrive Hosting Service Overview

The TeamDrive Apache module `mod_pspace` handles the communication and exchange of data with the TeamDrive Clients. In the default configuration, Space data is stored on a regular file system or an NFSv4 share.

The TeamDrive Hosting Service Administration Console and TeamDrive Hosting Service API is served by the Yvva Apache module `mod_yvva`.

The list of Spaces, access data, usage statistics and other administrative information is stored in the Management MySQL Database called `pspace`.

Additionally, an Amazon S3-compatible object store can be used as second tier storage. This significantly reduces the load on the first tier storage with regards to disk space utilization and I/O. In this case, only data “in flight” like the files being uploaded by the TeamDrive Clients and the Space log files are stored temporarily on the first tier storage until the upload completed. Only the so-called `last.log` files reside permanently on the first tier storage in this configuration.

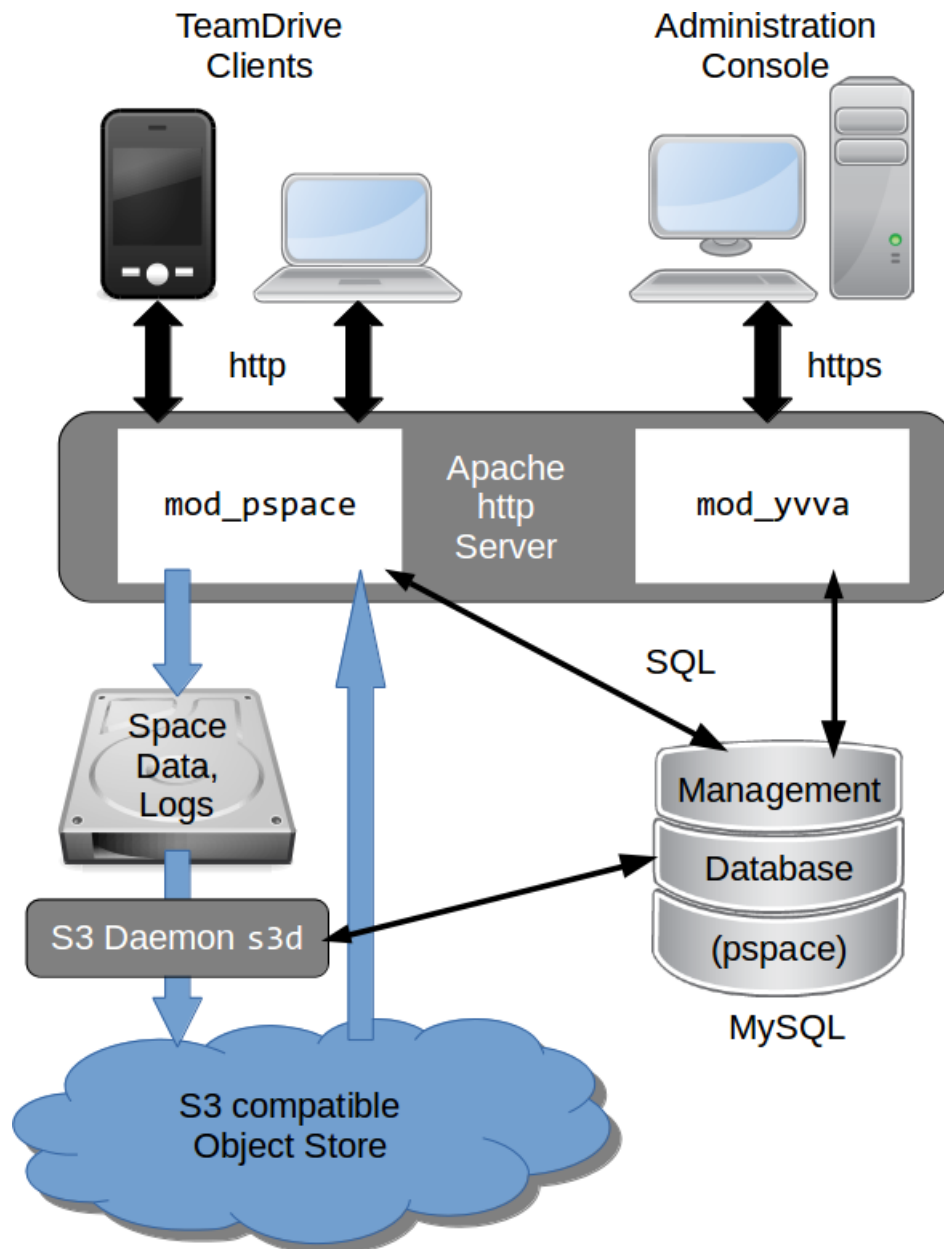


Figure 4.2: TeamDrive Hosting Service using an S3-compatible object store

Afterwards, the files are moved to the object store asynchronously, using the TeamDrive S3 Daemon `s3d`. Once they have been transferred to the object store, `mod_pspace` fetches the objects in question from there before serving them to the Clients, thus acting as a proxy.

Alternatively, the Hosting Service can be configured in such a way that Clients requesting these objects will receive a redirect to the object store by `mod_pspace` for obtaining them directly. This helps to offload network traffic from the Host Server to the object store.

See the chapter *Setting up an Amazon S3 Object Store* in the TeamDrive Hosting Service Administration Guide for details.

A storage system combined with the associated web servers is called a TeamDrive Hosting Service. Externally, i.e. from the Registration Server or user’s perspective, the Hosting Service is referred to as a TeamDrive Host Server. However, in this documentation references to TeamDrive Host Server refer to single host instance running an Apache web server and the TeamDrive Hosting Service software.

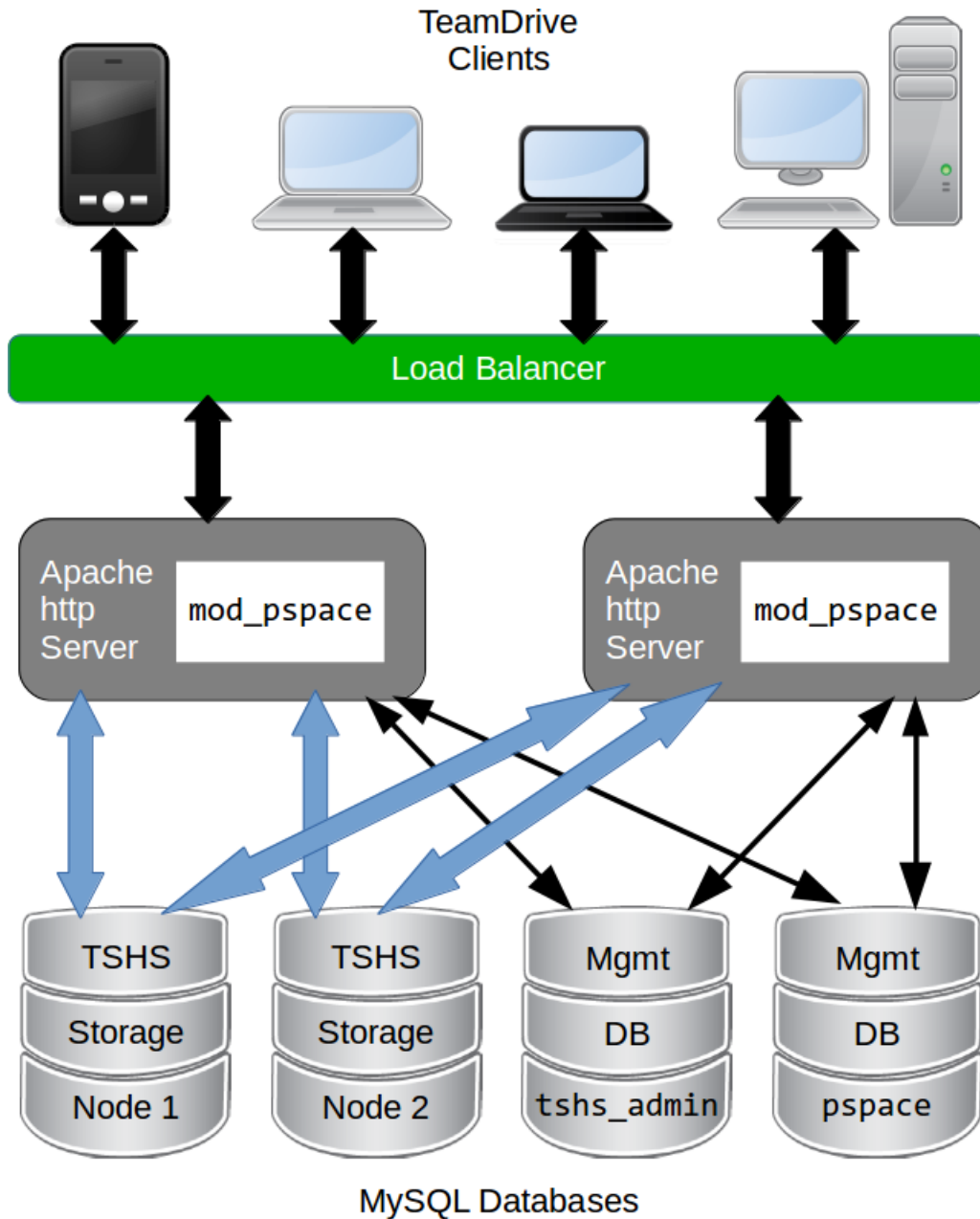


Figure 4.3: TeamDrive Scalable Hosting Storage (TSHS)

The illustration above shows a “scaled-out” solution, with several Apache Webservers attached to a TeamDrive Scalable Hosting Storage (TSHS) cluster. See the chapter *TeamDrive Scalable Hosting Storage* in the TeamDrive Hosting Service Administration Guide for details.

As an alternative to TSHS, a shared file system like NFSv4 or a distributed file system can also be used to store the data.

4.2 TeamDrive Hosting Basics

When using file system based storage, the data is stored on one or multiple volumes. When using the TSHS cluster for storage, the volume component is ignored. When using a file system, Spaces may be created on any volume that is “operational”.

A TeamDrive Hosting Service requires a unique domain name. The domain name becomes part of the Space URL that is returned to the TeamDrive Client when a Space is created on the service. The domain name is also part of the URL used by the clients to create Spaces, and by the Registration Server to create new Space Depots. This URL is stored in the `ServiceHostURL` system setting.

The Same domain name is also used to access Hosting Administration Console Hosting Service API. The default Hosting Administration Console URL is: <https://tdhostserver.yourdomain.com/admin/>

Note: Note that it is not possible to change the domain name of a Host Server, once the TeamDrive Clients have contacted it to create and access Spaces — the location of Spaces is tied to the Host Server’s host name. However, it is possible to change a Host Server’s IP address, if required.

4.3 Directory Structure of Hosted Data

The directory structure for space data stored on local storage is as follows:

```
spacedata
`-- vol101
  |-- 1
  |   |-- protolog
  |   |   |-- last.log
  |   |   |-- last.log.lock
  |   |   `-- 0.log
  |   `-- data
  |       |-- D41D8CD98F00B204E9800998ECF8427E
  |       |-- 7D0F97FC38AE3B2666435D03AA91F352
  |       `-- 253F19AA30D5346662B3EA83CF79F0D7
  `-- 2
      |-- data
      |   |-- 5ACDD4Z000004004U8RGKHSZM2592M8H
      |   |-- F3XG47Z000004004U8RG1214Z2592M80
      |   `-- NYFBTSZ000004004U8RFT7Q8A2592M7Y
      |-- protolog
      |   |-- last.log
      |   `-- last.log.lock
      |-- public
      |   `-- 8CN7S0800000A004UH0Q9TP323BBN28E
      |       `-- Familypicture.jpg
      `-- snapshot
          |-- last.log
          `-- last.log.lock
```

When Spaces are created, they are evenly distributed across individual volumes, based on the relative disk space utilization ratio of each available volume. A Space is identified in the file system by its unique database ID. The TeamDrive Clients store the data for a Space separated according to metadata (`protolog`-directory) and contents (`data`-directory).

Metadata is appended to a log file and reflects the history of the Space by storing all events (invitations of users, creation of directories, files and all modifications, etc.). All data stored on the Hosting Service is encrypted and only the TeamDrive Clients can decrypt it. It is not possible to read the original space data in the log.

New data is continually added to the `data` directory in each Space directory. Existing data is never overwritten, with the exception of data that has not been uploaded fully and where the upload may restart. File names are created using a Global Unique ID algorithm in the TeamDrive Clients that prevents two different clients from

creating the same name. When permanently deleting files (e.g. when emptying the recycle bin of a Space), these files are deleted on the server, to free up storage space.

The `last.log.lock` file in each Space is used internally for providing a reliable locking mechanism to prevent multiple clients from appending data to the `last.log` file at the same time. Hence, the underlying storage or file system needs to support proper file locking (the `mod_space` Apache module depends on `flock(LOCK_EX)` to be reliable).

The `public` folder contains unencrypted files that have been published (uploaded) by the TeamDrive Clients. Published files are read-accessible via HTTP or HTTPS (depending on the server configuration) by anybody, including users who do not have a TeamDrive Client installed. A TeamDrive Professional Client license is required to publish files.

Finally, versions 3.2.0 or later of the TeamDrive client support a so-called “Snapshot” feature, which cuts down the time it takes to enter a Space considerably. The information required to implement this functionality is stored in the `snapshot` subdirectory of a Space.

4.4 Spaces, Owners, and Depots

All Spaces created on a host are allocated to a specific Space Depot. A Space Depot has a storage quota and traffic limit. TeamDrive Client users require the access information of a Depot in order to create a Space.

If enabled, the TeamDrive Registration Server creates the necessary Depot (called the default Depot) required by the TeamDrive Client during registration of a client. For this purpose the TeamDrive Registration Server must have API access to the Hosting Service.

After the Depot has been created on the Hosting Service, the access information is returned to the TeamDrive Client via the Registration Server. The default Depot is linked to the registration of the TeamDrive Client, and cannot be used by any other user.

The Space Owner and Space information is recorded when a Space is created using the TeamDrive Client.

In addition to the default Depot, additional Depots can also be created manually via the Registration Server’s and the Host Server’s Administration Console. See chapter “Manually creating a Depot” in the Host Server Administration Guide for details.

4.5 Background Tasks Performed by `td-hostserver`

The `td-hostserver` process is a service running on a Host Server instance that processes background tasks scheduled by the Hosting Service.

It uses the Yvva daemon `yvvad` to execute the following background tasks at a definable regular interval:

- **Close Session:** Each TeamDrive Client needs a valid session for uploading; the session is held in the database. Since the clients do not necessarily have to log out, this process ensures that old sessions are deleted.
- **Sum Disk Usage:** Sums up traffic and usage of storage space in account Spaces and sets flags where necessary when account limits are exceeded.
- **Reset Traffic :** On the first day of each month the traffic for all Spaces and Depots is reset to 0.
- **Volume Warning :** Automatically sends a warning when a volume exceeds the limits set.
- **Check Spaces with Limit:** When Spaces exceed their storage or traffic limit, this checks whether the Depot has dropped back below the limit.
- **Delete Space:** TeamDrive Clients can request the deletion of a Space by setting its status to “TO-DELETE”. `td-hostserver` automatically detects Spaces with this status and removes all associated folders and files from the file system of the associated Host Server. After deleting all files, `td-hostserver` changes the corresponding Space status to “DELETED”.

- **Create Space statistics:** If the `SpaceStatisticEnabled` configuration setting is set to `True`, a monthly report containing detailed statistics like monthly traffic and disk usage for all existing Depots and Spaces within these depots will be created. See the chapter “Reporting Usage Statistics” in the Host Server Administration Guide for details.

OPERATING SYSTEM CONFIGURATION

5.1 Installing a base operating system

Start by performing a minimal OS installation of a recent 64-bit Red Hat Enterprise Linux 6 (RHEL 6) or derivative Linux distribution (e.g. CentOS 6, Oracle Linux 6), using your preferred installation method (manual install, Kickstart, etc). The details of how to perform this task are out of the scope of this document.

For performing the installation, the system needs to be able to establish outgoing TCP connections (mainly to download additional components).

Boot up the system and log in as the root user, either via the console or via an SSH connection.

5.2 Enable Time Synchronization with NTP

We strongly advise that the clocks of all servers in a TeamDrive installation are synchronized using the Network Time Protocol (NTP). This can be achieved by installing the ntp package and enabling the NTP daemon:

```
[root@hostserver install]# yum install ntp
[root@hostserver install]# service ntpd start
[root@hostserver install]# chkconfig ntpd on
```

Edit and update the configuration file `/etc/ntp.conf`, if necessary for your local environment.

5.3 Disable SELinux

The TeamDrive Host Server currently can not be run when SELinux is enabled. Edit the file `/etc/selinux/config` and set `SELINUX=disabled`.

Reboot the system or change the SELinux enforcing mode at run time using the following command:

```
[root@hostserver install]# echo 0 > /selinux/enforce
```

5.4 Firewall configuration

You should configure a local firewall so the server is protected against remote attacks. The only TCP ports that should be reachable from outside are 22 (SSH, optional for remote administration), 80 (http) and 443 (https).

On a minimal installation, you can install and use the text-based firewall configuration utility to enable access to the following services:

- SSH
- Secure WWW (HTTPS)
- WWW (HTTP)

To configure the firewall, you need to run:

```
[root@hostserver install]# yum install system-config-firewall-tui newt-python
[root@hostserver install]# system-config-firewall-tui
```

Follow the instructions to configure the firewall. Enable additional protections based on your local requirements or security policies.

You can check the result with `iptables -L`:

```
[root@hostserver ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           state
ACCEPT     all  --  anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere              state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere              state NEW tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere              state NEW tcp dpt:https
REJECT     all  --  anywhere              anywhere              reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           reject-with
REJECT     all  --  anywhere              anywhere              reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

INSTALLING THE HOST SERVER COMPONENTS

6.1 Enable the TeamDrive Host Server yum Repository

The TeamDrive Host Server components are available in the form of RPM packages, hosted in a dedicated yum repository. This makes the installation and applying of future updates of the software very easy — you can simply run `yum update` to keep your Host Server software up to date.

To enable the repository, you need to download the `td-hostserver.repo` file and place it into the directory `/etc/yum.repos.d/`, e.g. by using `wget`:

```
[root@hostserver ~]# wget -O /etc/yum.repos.d/td-hostserver.repo \
http://repo.teamdrive.net/td-hostserver.repo
```

This will enable the “TeamDrive Host Server Version 3.0.013” repository, which you can check by running `yum repolist` afterwards:

```
[root@hostserver ~]# yum repolist
Loaded plugins: security
repo id                                repo name                                status
td-hostserver-3.0.013                  TeamDrive Host Server Version 3.0.013    2
base                                    CentOS-6 - Base                          6.367
extras                                  CentOS-6 - Extras                        14
updates                                 CentOS-6 - Updates                       1.094
repolist: 7.477
```

6.2 Download and Install the TeamDrive Host Server Package

Perform the download and installation of the Host Server installation RPM package using the `yum` package manager:

```
[root@hostserver ~]# yum install td-hostserver
```

The TeamDrive Hosting Service depends on the Yvva Runtime Environment version 1.0.0 or later to be installed and configured. It will be installed by `yum` as a dependency on `td-hostserver` automatically.

Once the TeamDrive Host Server software has been installed successfully, you can proceed with the initial configuration.

APACHE HTTP SERVER INSTALLATION AND CONFIGURATION

The Apache http server and the `mod_ssl` Apache module should have already been installed as dependencies for the `td-hostserver` RPM package. You can verify this with the following command:

```
[root@hostserver ~]# yum install httpd mod_ssl
Setting up Install Process
Package httpd-2.2.15-30.0.1.el6_5.x86_64 already installed and latest version
Package 1:mod_ssl-2.2.15-30.0.1.el6_5.x86_64 already installed and latest version
Nothing to do
```

7.1 Update `httpd.conf`

Open the web server configuration file `/etc/httpd/conf/httpd.conf` in a text editor to change the following parameters:

```
KeepAlive On
KeepAliveTimeout 2
ServerName <Your ServerName>
```

For security reasons, we also advise to disable the so-called “Server Signature” - a feature that adds a line containing the server version and virtual host name to server-generated pages (e.g. internal error documents, FTP directory listings, etc):

```
ServerSignature Off
```

By default, the server version and operating system is also displayed in the `Server` response header field, e.g. `Server: Apache/2.2.15 (CentOS)`. To suppress this output, we suggest to update the `ServerTokens` option as follows:

```
ServerTokens Prod
```

7.2 Disable Unneeded Apache Modules

The TeamDrive Registration Server only requires a few Apache modules to be enabled. To reduce the memory footprint, please deactivate unnecessary modules in the apache configuration. Only the following modules should be left enabled in `/etc/httpd/conf/httpd.conf`:

```
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule headers_module modules/mod_headers.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
```

You also need to comment out the following variables in `/etc/httpd/conf/httpd.conf`, to avoid syntax errors caused by the disabled modules:

```
# DirectoryIndex index.html index.html.var
# LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no
pl pt pt-BR ru sv zh-CN zh-TW
# ForceLanguagePriority Prefer Fallback
# BrowserMatch "Mozilla/2" nokeepalive
# BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
# BrowserMatch "RealPlayer 4\.0" force-response-1.0
# BrowserMatch "Java/1\.0" force-response-1.0
# BrowserMatch "JDK/1\.0" force-response-1.0
# BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
# BrowserMatch "MS FrontPage" redirect-carefully
# BrowserMatch "^WebDrive" redirect-carefully
# BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
# BrowserMatch "^gnome-vfs/1.0" redirect-carefully
# BrowserMatch "^XML Spy" redirect-carefully
# BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
```

7.3 Configure `mod_ssl`

The web-based TeamDrive Hosting Service Administration Console should be accessed via an encrypted SSL connection. To facilitate this, add the following to the end of the default `<VirtualHost>` section in `/etc/httpd/conf.d/ssl.conf`:

```
# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

RewriteEngine on
RewriteLogLevel 0
RewriteLog "/var/log/httpd/rewrite.log"
RewriteRule ^/admin$ /admin/ [R]
RewriteRule ^/admin(.*) /yvva/pla$1 [PT]
RewriteRule ^/pbas/pl_as/api/(.*)$ /yvva/api/$1 [PT]
</VirtualHost>
```


MYSQL INSTALLATION AND CONFIGURATION

8.1 Installing MySQL Server

The TeamDrive Hosting Service requires a MySQL database to store its information. This document assumes that the MySQL instance runs on the same host as the Host Server itself, connecting to it via the local socket file.

Alternatively, it's possible to use an external MySQL Server. In this case, you need to make sure that this external MySQL instance is reachable via TCP from the Host Server (usually via TCP port 3306) and that the `teamdrive` MySQL user account is defined correctly (e.g. the MySQL username in the remote database would become `teamdrive@hostserver.yourdomain.com` instead of `teamdrive@localhost`).

Most MySQL installations usually do not allow the `root` user to log in from a remote host. In this case the installation script is unable to create the dedicated `teamdrive` user automatically and you need to perform this step manually before performing the installation of the TeamDrive Hosting Service databases.

Especially the correct definition of the host part is critical, as MySQL considers `username@hostserver` and `username@hostserver.yourdomain.com` as two different user accounts.

To set up the Host Server using a local MySQL Database, install the MySQL Client and Server packages:

```
[root@hostserver ~]# yum install mysql mysql-server
```

For reliability and performance reasons, we recommend placing the MySQL data directory `/var/lib/mysql` on a dedicated file system or storage volume.

Please start the MySQL server, run the secure installation script and follow the recommendations. Make sure to create a password for the MySQL `root` user and take note of it:

```
[root@hostserver ~ ]# service mysqld start
Initializing MySQL database: Installing MySQL system tables...
OK
Filling help tables...
OK
```

To start `mysqld` at boot time you have to copy `support-files/mysql.server` to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

```
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h hostinstalltest.local password 'new-password'
```

Alternatively you can run:
`/usr/bin/mysql_secure_installation`

which will also give you the option of removing the test databases and anonymous user created by default. This is strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

```
Starting mysqld: [ OK ]  
[root@hostserver ~ ]# mysql_secure_installation
```

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current password for the root user. If you've just installed MySQL, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none): <Enter>
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL root user without the proper authorisation.

```
Set root password? [Y/n] <y>  
New password: <mysql_root_pw>  
Re-enter new password: <mysql_root_pw>  
Password updated successfully!  
Reloading privilege tables..  
... Success!
```

By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.

```
Remove anonymous users? [Y/n] <Enter>  
... Success!
```

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

```
Disallow root login remotely? [Y/n] <Enter>  
... Success!
```

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

```
Remove test database and access to it? [Y/n] <Enter>  
- Dropping test database...  
... Success!  
- Removing privileges on test database...  
... Success!
```

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

```
Reload privilege tables now? [Y/n] <Enter>
... Success!
```

```
Cleaning up...
```

All done! If you've completed all of the above steps, your MySQL installation should now be secure.

Thanks for using MySQL!

MySQL is now up and running and you can proceed with creating the `teamdrive` user and the MySQL databases required for the TeamDrive Host Server.

8.2 Creating TeamDrive MySQL User and Databases

The TeamDrive Hosting Service requires two MySQL databases `hostapilog` and `pspace`, which will be accessed using a dedicated `teamdrive` MySQL user.

The Host Server installation package ships with a script that performs the required configuration steps:

- Modify the local configuration file `/etc/my.cnf`, start and enable MySQL Server (only when using a local MySQL Server)
- Create the required MySQL user `teamdrive`, assign the provided password and the required database privileges (requires access to the MySQL `root` account)
- Create and populate the required Hosting Service MySQL databases
- Modify the local Host Server configuration file `/etc/td-hostserver.my.cnf`

The following example assumes that the MySQL database is located on the same system where the TeamDrive Host Server instance is installed.

You need to have the following information available:

- The password of the MySQL `root` user account
- The password that you want to assign to the `teamdrive` user

The script is part of the `td-hostserver` package and is installed in `/opt/teamdrive/hostserver/mysql/mysql_install.sh`. Call it as the `root` user and follow the instructions:

```
[root@hostserver ~]# /opt/teamdrive/hostserver/mysql/mysql_install.sh
```

```
TeamDrive Hosting Service MySQL Database Install Script
```

```
-----
Configuring MySQL database for TeamDrive Hosting Service
version 3.0.013.0
```

This script will perform the following steps:

- Modify the local configuration file `/etc/my.cnf`, start and enable MySQL Server (only when MySQL Server runs locally)
- Create the required MySQL user "teamdrive", assign the provided password and the required database privileges (requires access to the MySQL `root` account)
- Create and populate the required Hosting Service MySQL databases
- Modify the local Host Server configuration file `/etc/td-hostserver.my.cnf`

```
Enter MySQL hostname: localhost
Enter MySQL root password for localhost: <mysql_root_pw>
Enter MySQL password to be set for user teamdrive: <td_pw>

mysqld (pid 7490) is running...
Stopping mysqld: [ OK ]
Changing local MySQL Server configuration...
Backing up existing configuration file /etc/my.cnf...
`/etc/my.cnf' -> `/etc/my.cnf-2014-06-12-17:19.bak'
Starting and enabling MySQL Server...
Starting mysqld: [ OK ]
Trying to connect to the MySQL server as root...
+-----+
| MySQL Version |
+-----+
| 5.1.73        |
+-----+
Creating teamdrive MySQL user on localhost
Trying to connect to the MySQL server as the teamdrive user...
Creating Hosting Service databases...
Updating /etc/td-hostserver.my.cnf...
Backing up existing configuration file ...
`/etc/td-hostserver.my.cnf' -> `/etc/td-hostserver.my.cnf-2014-06-12-17:19.bak'

Finished!
The MySQL configuration for TeamDrive Hosting Service
version 3.0.013.0 is now complete.
```

The MySQL database is now properly configured and populated. As a final test, try logging into the MySQL database from the Host Server system, using the teamdrive user account and the password you defined — you should be able to see and access the TeamDrive Hosting Service databases:

```
[root@hostserver ~]# mysql -u teamdrive -p<password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 51
Server version: 5.1.71 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES;
+-----+
| Database          |
+-----+
| information_schema|
| hostapilog        |
| pspace            |
+-----+
3 rows in set (0.00 sec)

mysql> QUIT
Bye
```

INITIAL HOST SERVER CONFIGURATION

9.1 Mount the Space Storage Volume

The toplevel directory `/spacedata` contains the mount points for all space volumes. By default, the mount point `vol01` has already been created by the `td-hostserver` RPM package. Note that it must be owned by the user that the Apache httpd Server runs under (usually `apache`).

You need to create a dedicated file system that provides the requirements outlined in chapter *storage-requirements*.

Mount the file system and create the respective mount entry in `/etc/fstab` to enable automatic mounting of the file system at bootup. Please consult your Operating System documentation for details on how to perform this step.

9.2 Starting the Host Server Instance

After all configuration steps have been performed, we can start the TeamDrive Services to conclude the initial installation/configuration.

9.2.1 Starting `td-hostserver`

To activate the `yvvad`-based `td-hostserver` background task you have to start the service using the provided init script.

The configuration file `/etc/td-hosting.conf` defines how this process is run.

To start the `td-hostserver` program, use the `service` command as user root:

```
[root@hostserver ~]# service td-hostserver start
Starting TeamDrive Hosting Services: [ OK ]
```

Use the `status` option to the `service` command to verify that the service has started:

```
[root@hostserver ~]# service td-hostserver status
yvvad (pid 2506) is running...
```

You can verify the startup by looking at the log file `/var/log/td-hostserver.log`:

```
[root@hostserver ~]# tail -3 /var/log/td-hostserver.log
140603 10:51:47 [Note] yvvad startup
140603 10:51:47 [Note] Using config file: /etc/td-hosting.conf
140603 10:51:47 [Note] yvvad running in repeat 60 (seconds) mode
```

If `td-hostserver` does not start, check the log file for errors. See chapter *Troubleshooting* (page 35) for details.

9.2.2 Starting the Apache http Server

Now the Apache http Server can be started, which provides the TeamDrive Host Server functionality (via `mod_ospace`) as well as access to the TeamDrive Hosting Service Administration Console and API (via `mod_yvva`).

You can start the service manually using the following command:

```
[root@hostserver ~]# service httpd start
```

Check the log files `/var/log/httpd/error_log` and `/var/log/mod_yvva.log` for startup messages and possible errors:

```
[root@hostserver ~]# cat /var/log/httpd/error_log
[notice] Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured
-- resuming normal operations
[notice] mod_ospace 1.2.83 (118) Loaded; Admin 1.0.0; TSHS 1.0.0; S3 1.0.0;
Build Jun  2 2014 15:09:55
[notice] mod_yvva 1.0.0 (Jun  2 2014 09:36:29) loaded
[notice] Logging (=error) to: /var/log/mod_yvva.log
[notice] [notice] mod_ospace 1.5.03 Loaded; Build Jun  6 2014
12:42:24;Crash-Reporting-Disabled
[notice] Admin API booted: TSHS n/a; S3 n/a; Path: /spacedata
[root@hostserver ~]# cat /var/log/mod_yvva.log
140603 11:06:31 [Note] mod_yvva 1.0.0 (Jun  2 2014 09:36:29) startup OK
```

Please consult chapter [Troubleshooting](#) (page 35) if there is an error when starting the service.

Note: You may observe Admin API Errors like the following ones:

```
[notice] Admin API, WARNING: Host Server Volume Path has not been specified
```

or:

```
[notice] Admin API, WARNING: Host Server setup has not been completed
```

or:

```
[error] Failed to boot Admin API 1.2.77: System parameter ServiceHostURL
setting required
```

or:

```
[error] [client xxx.xxx.xx.xx] (500)Unknown error 500: Admin API Error
-14000: System parameter ServiceHostURL setting required
```

These errors can be ignored at this stage, they are caused by the fact that the Host Server has not been configured and registered with a Registration Server yet. This step will be described in the following chapter.

9.3 Registering and Activating the Host Server

Once the Apache http Server is up and running, open a web browser and point it to the Host Server's Admin Console:

```
https://hostserver.yourdomain.com/admin/
```

If you have not installed a proper SSL certificate yet, your browser might issue a warning about an untrusted certificate.

Alternatively, you can open the Admin Console via an unencrypted HTTP connection. In this case, you will be prompted to proceed using an insecure connection.

When everything is configured correctly, you will see the TeamDrive Host Server Setup page that will guide you through the initial configuration:

Figure 9.1: Host Server Setup Page

Fill out the fields according to your environment and requirements:

Admin Password: The administrator password that you need to provide to login to the Host Server Administration Console. The administrator’s default user name is “HostAdmin”.

Host Domain Name: The domain name of this Host Server. This is the domain name that TeamDrive clients will use to create and access Spaces. The setup tool will try to determine and fill in this name automatically, please ensure that it is a fully-qualified and resolvable domain name.

Registration Server Name: All Host Servers must be registered with a Registration Server. Enter the name of your Registration Server here. **Please contact TeamDrive Systems for the correct value if you don’t manage your own Registration Server.**

Reg. Server Domain Name: Enter the fully qualified domain name of the Registration Server. Setup will ping this domain to ensure that the Registration Server is running and reachable. **Please contact TeamDrive Systems for the correct value if you don’t manage your own Registration Server.**

Provider Code: The Host Server will be assigned to a Provider on the specified Registration Server. The Provider Code (aka Distributor Code) is a 4 character code, consisting of letters A-Z and 0-9. **If you don’t have a Provider Code yet, please contact TeamDrive Systems for obtaining you individual Provider Code. This code can not be changed later on.**

API IP List: Enter a comma separated list of IP addresses of systems that are permitted to access the Host Server API. **This list must include the IP address of the Registration Server’s Admin Console. Please contact TeamDrive Systems for the correct value if you don’t manage your own Registration Server.**

API Salt: The API Salt is a code that allows the Host Server to validate calls to the Host Server’s API. This value must match the value of the `APIChecksumSalt` setting on the Registration Server to avoid “man in the middle”-attacks. Please consult the Registration Server Documentation on how to obtain it or contact TeamDrive Systems for the correct value if you don’t manage your own registration server.

Click on **Setup** to initiate the Host Server configuration and registration process with the Registration Server.

Communication within the TeamDrive network is encrypted with a public-private encryption key pair. During registration, this key pair is generated by the Host Server and the public key is sent to the Registration Server. This will result in the creation of a new user account on the Registration Server, named `tdhosting.<host domain name>`, e.g. `tdhosting.hostserver.yourdomain.com`, and a device associated with that user.

After server registration, you are required to enter an Activation Code. Due to security reasons, you will not receive this code automatically. If you don't run your own Registration Server, you need to request this code from TeamDrive Systems.

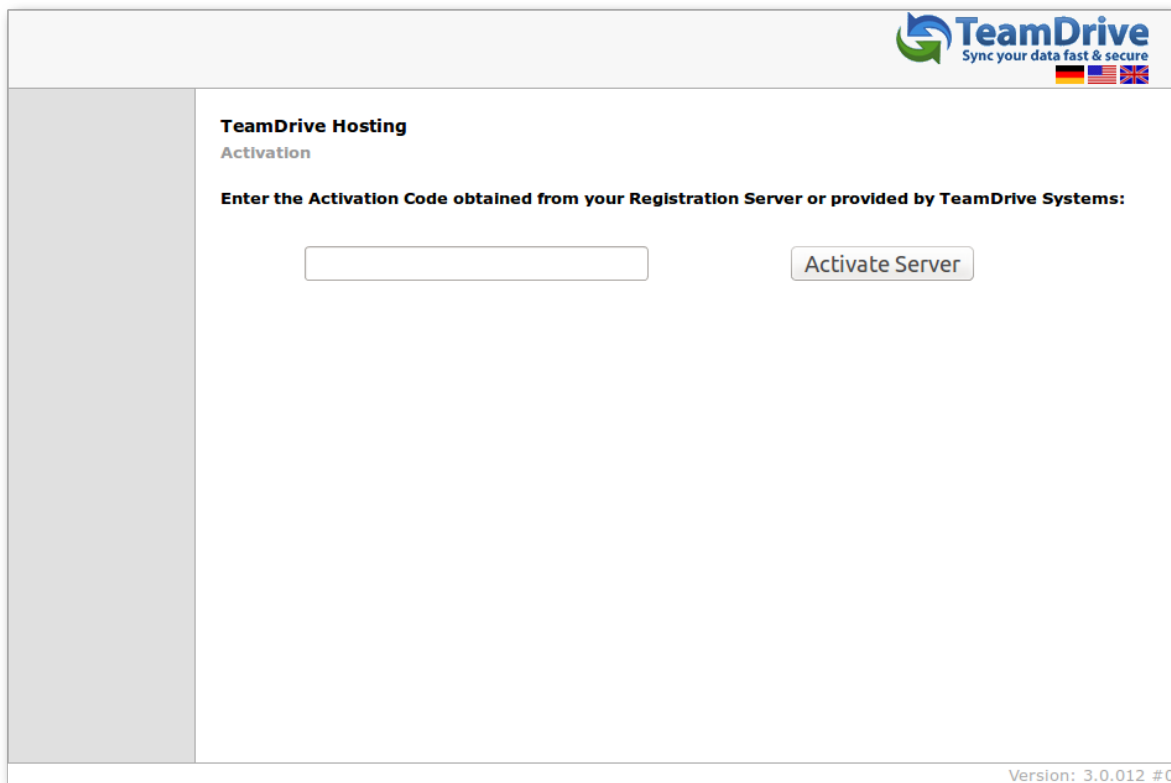


Figure 9.2: Host Server Activation Window

If you manage your own Registration Server, you need to query the Registration Server's MySQL database for the host server's activation code by running the following SQL statement. Starting with version 3.0.018 of the Registration Server Admin Console, the activation code can also be obtained from the "Manage Devices" page.

```
[root@regserver ~]# mysql -u root -p
mysql> SELECT activationcode, name FROM td2reg.TD2Device \
WHERE Name LIKE "tdhosting.hostserver.yourdomain.com";
+-----+-----+
| activationcode          | name                               |
+-----+-----+
| XXXXXXXXXXXXXXXXXXXXXXX | tdhosting.hostserver.yourdomain.com |
+-----+-----+
1 row in set (0.00 sec)
```

Take note of this activation code, enter it into the host server's activation page and click on "Activate server."

Warning: If you had to restart the Registration/Activation process because of incorrectly entered values, it's absolutely necessary to restart the Apache httpd Server to roll back some internal changes:

```
[root@hostserver ~]# service httpd restart
```

9.4 Setup and Administration

Upon successful activation, you will be presented with the Host Server Administration Console Home Screen.

The screenshot shows the Host Server Administration Console Home Screen. The page title is "hostsrv30013.local". The top right corner features the TeamDrive logo with the tagline "Sync your data fast & secure" and flags for Germany, the USA, and the UK. A left sidebar contains a navigation menu with items: Home (selected), Host, Volumes, Depot/Space Owner, Space Depots, Spaces, Settings, and Logout. The main content area is titled "TeamDrive Hosting" and includes sections for "Home", "Host", "Volumes", "Depot/Space Owner", "Space Depots", and "Spaces", each with a brief description of its function.

Figure 9.3: Host Server Admin Console: Home Screen

9.5 Host Servers (Hosts)

9.5.1 Overview

In the overview, you can display the Host Servers, the associated volumes, and some statistical values. The volumes change colour between green, yellow, and red depending on the percentage used.

The values are updated at regular intervals with the "SumUsage" background task. In the process, the associated Depot is updated via the Spaces, as are the volumes and hosts.

Volumes first appear in the view when created as described in the following chapter.

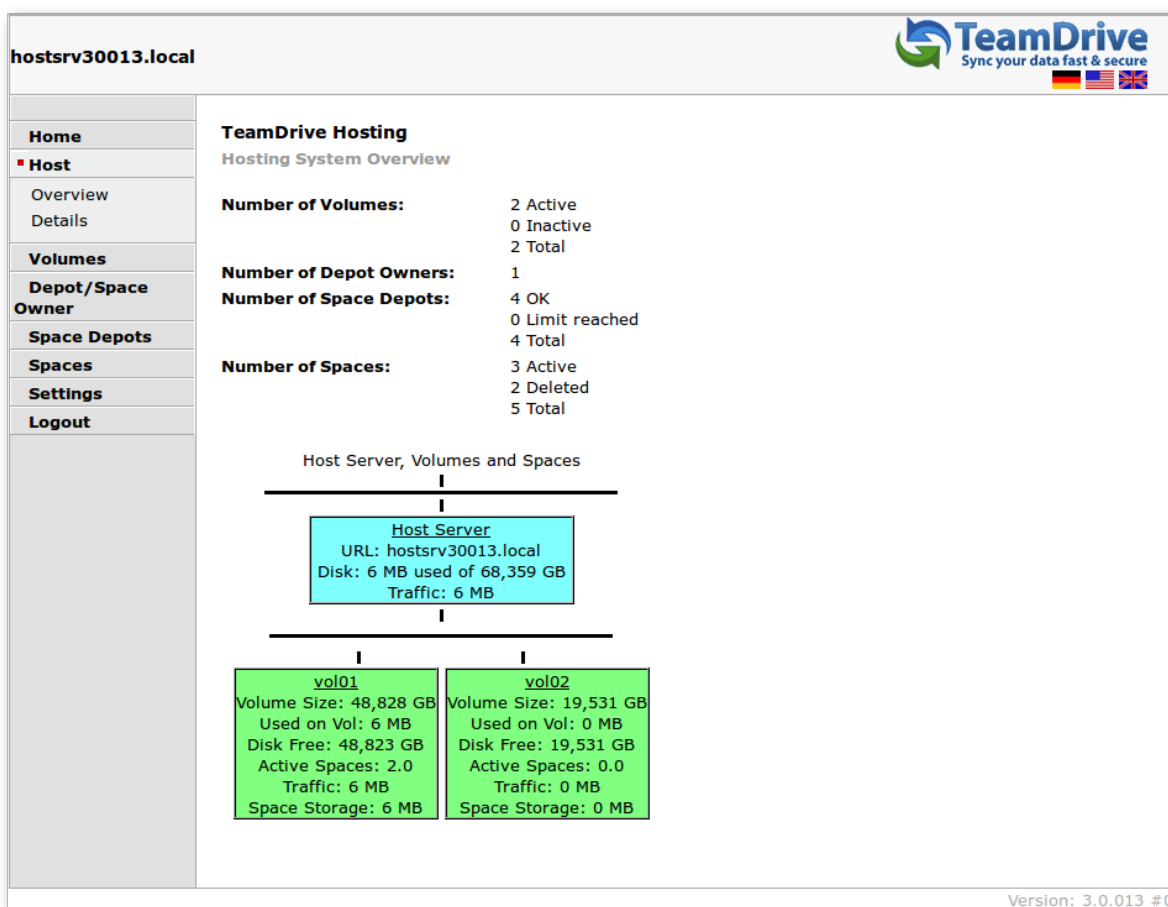


Figure 9.4: Host Server Admin Console: Server Overview

9.6 Volumes

9.6.1 Adding more Volumes

By default, the first volume `vol01` has already been created during the initial installation.

If required, you can add more Volumes using this screen.

The screenshot shows the 'Add New Volume' form in the Host Server Admin Console. The form is titled 'TeamDrive Hosting' and 'Volumes: Add New Volume'. It contains the following fields and values:

- Directory:
- Internal Name:
- State:
- Mounted on Host:
- Max. Disk Space: MB

At the bottom of the form, there are two buttons: 'Back' and 'Create'. The navigation bar on the left includes 'Home', 'Host', 'Volumes', 'Volume List', 'Depot/Space Owner', 'Space Depots', 'Spaces', 'Settings', and 'Logout'. The TeamDrive logo is in the top right corner, and the version '3.0.013 #0' is in the bottom right corner.

Figure 9.5: Host Server Admin Console: Add New Volume

Click on **Volumes -> Add New Volume** in the navigation bar and enter the values as shown in the following example. Make sure to adjust them to match your configuration/environment.

Directory: **vol02** (this is the default and should be kept)

Internal Name: **sda**

State: **Operational (active)**

Mounted on Host: **tdhostsrv001:/spacedata**

Max. disk space (in MB): **10000**

The field **Directory** defines both the Volume Name as well as the name of the mount point in the filesystem below the `/spacedata` directory.

Note: Volume names must be of the form: `volxx`, e.g. `vol01`, `vol02`.

Please don't use blanks in volume names.

The name of a volume cannot be changed later because it becomes part of the Space URL which the TeamDrive Clients use to access these spaces.

The field **Internal Name** is for your reference only, it could contain the name of the volume on your storage system or the local hard disk drive name or partition.

The volume mount point must be created with the corresponding name in the path to the volumes as indicated in the Host Server configuration, e.g. `/spacedata/vol02`. The ownership of the volume must be assigned to the user that runs the Webserver (usually `apache`) using the `chown` command.

Click on “Create” to create the new volume.

Note: When unmounting the volume, the mount point must be removed in the operating system as well.

9.7 Associating the Host Server with a Provider

As a final step, you need to associate your host server with your provider account on the Registration Server. This can be performed via the Registration Server’s Admin Console, which you can usually access via the following URL:

`https://regserver.yourdomain.com/adminconsole/`

Please see the Registration Server Manual for details.

Log in with your provider login and click the tab “Edit Distributor Settings” (Registration Server version 3.0.017 and older) or “Edit Provider Settings” (Registration Server version 3.0.018 and newer).

In the section “Distributor Settings”, click on the Button labelled “HOSTSERVER”.

Change the configuration setting `HAS_DEFAULT_DEPOT` from `False` to `True` and click “Save”.

The `HOST_SERVER_NAME` and related settings should now appear in the list of `HOSTSERVER` settings. Select your host server from the selection list and click “Save” to apply this change.

If required, adjust the other settings from the `HOSTSERVER` category to match your requirements, e.g. `HOST_SERVER_URL`, `HOST_DEPOT_SIZE` and `HOST_TRAFFIC_SIZE`.

9.8 Testing Client Access

The Host Server has now been set up. To test its functionality, start a TeamDrive Client and create or log into a user account belonging to the Provider Code this Host Server has been associated with.

When creating a new space, the Host Server should now be available in the “Server” selection list of the Client’s “Create a Space” dialogue.

After the space has been created, take note of the Server URL and Space ID in the Client’s Space Information panel. The URL should point to the host name of your Host Server.

On the Host Server, a directory with that Space ID as the directory name should have been created in `/spacedata/vol01/`. If you add files to this Space via the TeamDrive Client, the encrypted versions should appear in the respective Space’s `data` directory shortly afterwards.

Also try publishing a file (requires a Professional Client License), the file should be uploaded to the Host Server in unencrypted form and placed into a subdirectory below the `public` directory of that space. Try downloading the file using the URL provided. Again, the URL should point to your new Host Server.

POST-INSTALLATION TASKS

10.1 Starting the Apache http Server at Boot Time

To ensure that Apache http Server starts up automatically at system bootup time, use the following command to enable it:

```
[root@hostserver ~]# chkconfig httpd on
```

10.2 Starting TeamDrive Service at Boot Time

To start the TeamDrive Host Server background service `td-hostserver` at boot time, use the following command to enable it:

```
[root@hostserver ~]# chkconfig td-hostserver on
```

10.3 Installing SSL certificates

The default Apache http Server installation ships with self-signed SSL certificates for testing purposes. We strongly recommend to purchase and install proper SSL certificates and keys and adjust the configuration in file `/etc/httpd/conf.d/ssl.conf` accordingly before moving the server into production. The exact installation process depends on how you obtain or create the SSL key and certificate, please refer to the respective installation instructions provided by your certificate issuer.

10.4 Next steps

This concludes the basic installation and configuration of the TeamDrive Host Server. Please consult the TeamDrive Hosting Service Administration Manual for additional information on advanced administrative tasks and configuration steps.

TROUBLESHOOTING

11.1 List of relevant configuration files

/etc/httpd/conf.d/td-hostserver.httpd.conf: The configuration file that loads and enables the TeamDrive Host Server-specific modules for the the Apache http Server:

- `mod_pspace.so`: this Apache module provides the actual Host Server functionality by accepting incoming data from the TeamDrive clients as well as delivering data to other clients upon request.
- `mod_yvva.so`: this Apache module is responsible for providing the web-based Host Server Administration Console as well as the Host Server API interface.

/etc/logrotate.d/td-hostserver: This file configures how the log files belonging to the TeamDrive Host Service are being rotated. See the `logrotate(8)` manual page for details.

/etc/td-hosting.conf: This file defines how the `td-hostserver` background service is started using the `yvvad` daemon.

/etc/td-hostserver.my.cnf: This configuration file defines the MySQL credentials used to access the `pspace` MySQL database. It is read by the Apache modules `mod_yvva` and `mod_pspace` as well as the `yvvad` daemon that runs the `td-hostserver` background tasks and the `yvva` command line client.

/etc/yvva.conf: This configuration file contains configuration settings specific to the Yvva Runtime Environment that are shared by all Yvva components, namely the `mod_yyva` Apache module, the `yvvad` daemon and the `yvva` command line shell.

/etc/tshs.conf: This configuration file defines a number of maintenance tasks performed by the `tshs` background service.

11.2 List of relevant log files

In order to debug and analyse problems with the Host Server configuration, there are several log files that you should consult:

/var/log/mod_yvva.log: The log file for the Yvva Application Server module which provides the web-based Host Server Administration Console and API. Consult this log file when you have issues with associating the Host Server with the Registration Server, errors when issuing API requests or problems with the Administration Console. You can increase the amount of logging by changing the Yvva setting `log-level` from `error` to `trace` or `debug` in `/etc/httpd/conf.d/td-hostserver.httpd.conf`:

```
<Location /yvva>
  SetHandler yvva-handler
  YvvaSet root-path=/opt/teamdrive/hostserver
  YvvaSet mysql-cnfile=/etc/td-hostserver.my.cnf
  YvvaSet log-level=error
</Location>
```

After changing these values, you need to restart the Apache http Server service using `service httpd restart`.

/var/log/td-hostserver.log: The log file for the `td-hostserver` background task. Check this one to verify that background tasks are being processed without errors. The log file location can be configured by changing the file name passed to the `log-file` option in the configuration file `/etc/td-hosting.conf`. The log level can be increased by changing the default value `error` for the `log-level` option to `trace` or `debug`. Changing these values requires a restart of the `td-hostserver` background process using `service td-hostserver restart`.

/var/log/mod_pspace.log: This log file contains error messages related to the `mod_pspace` Apache module, particularly when using TSHS. It needs to be writable by the user that the Apache http Server runs under (`apache` by default). The log file location is configured by the server setting `ModuleLogFile` and the amount of logging can be changed by adjusting the server setting `ModuleLogLevel` via the Host Server Administration Console. The value defines the maximum level of logging of messages logged: 1 = Protocol, 2 = Error, 3 = Warning, 4 = Trace, 5 = Debug. Changing these value requires restarting the Apache http Server.

/var/log/httpd/: The Apache httpd Server's log files (e.g. `error_log`) might also contain additional relevant error messages (e.g. from `mod_pspace`) that should be checked. The amount of logging is affected by the `ModuleLogLevel` setting described above.

/var/log/tshs.log: This log file contains errors and other messages generated by the `tshs` background service. The log file location and amount of output are defined in file `/etc/tshs.conf`, via the options `log-file` and `log-level`. Possible values in the order of verbosity are `protocol`, `error`, `warning`, `trace`, `debug`. The default is `warning`.

/var/log/s3d.log: This log file is written by the TeamDrive S3 daemon `s3d` and provides log messages and errors specific to the `s3d` background service. The log file location is defined in the init script `/etc/init.d/s3d`.

11.3 Common errors

11.3.1 Errors When Registering the Host Server

If the Host Server Registration fails, check `/var/log/mod_yvva.log` on the Host Server as well as `/var/log/pbt_mod.trace` on the Registration Server for hints. See the Troubleshooting chapter in the Registration Server Installation Manual for details.

11.3.2 MySQL Errors When Upgrading From an Older Host Server Version

If you observe `Access denied` or `Unknown database` errors from the MySQL server like the following ones after starting the updated TeamDrive Host Server using an older MySQL table structure:

```
140618 10:56:37 [Note] DROP DATABASE pbgp;
140618 10:56:37 [Error] -12036 (1044): Access denied for user
'teamdrive'@'localhost' to database 'hostapilog'
140618 10:56:37 [Error] "plsetup.pbt" P1Setup:upgradeSettings (328)
140618 10:56:37 [Error] "plsetup.pbt" P1Setup:setupDatabase (14)
140618 10:56:37 [Error] "plsetup.pbt" (506)
```

Unknown database:

```
140618 10:24:31 [Error] -12036 (1049): Unknown database 'hostapilog'
140618 10:24:31 [Error] "plsetup.pbt" P1Setup:upgradeSettings (328)
140618 10:24:31 [Error] "plsetup.pbt" P1Setup:setupDatabase (14)
140618 10:24:31 [Error] "plsetup.pbt" (506)
140618 10:24:31 [Error] "pl_shared.pbt" (2)
```

Double check that the `hostapilog` database actually exists and that the `teamdrive` user has the required privileges to access it.

Create the database using `CREATE DATABASE hostapilog;` and grant the required privileges using `GRANT ALL PRIVILEGES ON 'hostapilog'.* TO 'teamdrive'@'localhost';`. Restart the TeamDrive Service again using `service td-hostserver restart`, it should now conclude the schema conversion.

If you observe a Can't connect to local MySQL server error like the following one in `/var/log/httpd/error_log`:

```
[Thu Jun 19 16:20:50 2014] [notice] mod_ospace 1.5.04 Loaded; Build Jun 19
2014 13:24:58;Crash-Reporting-Disabled
[Thu Jun 19 16:20:50 2014] [error] Failed to boot Admin API: MySQL 2002:
Can't connect to local MySQL server through socket
'/var/lib/mysql/mysql.sock' (2)
```

or in `/var/log/td-hostserver.log`:

```
140619 16:42:06 [Error] -12036 (2002): Can't connect to local MySQL server
through socket '/var/lib/mysql/mysql.sock' (2)
```

Double check that the MySQL Server is up and running and that the socket configuration setting in the `[mysqld]` group in `/etc/my.cnf` matches the one in `/etc/td-hostserver.my.cnf`.

The default value is `/var/lib/mysql/mysql.sock`. If the value in `my.cnf` is different, e.g. `/tmp/mysql.sock`, we suggest to revert back to the default value there instead of changing it in `td-hostserver.my.cnf` (unless you have an explicit reason to change the default socket path, of course). Restart MySQL and the TeamDrive Hosting Services after changing this value.

11.3.3 Admin Console: Clicking on “Host” Results in a “500 Internal Server Error”

If you observe an error message like the following when clicking on **Host** in the Host Server Administration Console:

```
500 Internal Server Error
ERROR -1: TshsMain: void CSDBConn::connect(CSDB.cc:1116) MySQL 1044: Access
denied for user 'teamdrive'@'localhost' to database 'tshs_admin'
```

Or:

```
500 Internal Server Error
ERROR -1: TshsMain: void CSDBConn::connect(CSDB.cc:1116) MySQL 1049: Unknown
database 'tshs_admin'
```

You likely changed the setting `TSHSEnabled` to `True`, but did not configure the MySQL settings for accessing the `tshs_admin` database in `/etc/td-hostserver.my.cnf`.

If you changed the setting by accident, simply set `TSHSEnabled` back to `False`.

Otherwise, consult the chapter *TeamDrive Scalable Hosting Storage* in the Team Drive Host Server Administration Guide for details on how to enable and configure TSHS properly.

11.3.4 “Duplicate key” MySQL errors when updating the database

If you observe “Duplicate key” errors in the `Traffic` or `Owner` tables when upgrading these to the latest schema version, you first need to manually remove the duplicates via the MySQL client or another tool like MySQL Workbench. Older versions of the Host Server database schema did not have `UNIQUE` constraints on some columns, which caused the creation of duplicate entries. For the `Traffic` table, this usually only affects older traffic accounting information that can safely be removed.

Duplicates in the `Owner` table are likely caused by user names or email addresses that refer to the same user account, but using different capitalization. In this case it helps to cross-reference the affected users with their

information in the Registration Server Database - likely one of these accounts has not been actively used and can be deleted. Please contact support@teamdrive.net if you need assistance in resolving these conflicts.

11.3.5 Admin API Error: MySQL 1040: Too many connections

On a busy server, you might observe one of the following error messages in the Apache http Server's error log file from time to time:

```
[error] Failed to boot Admin API: MySQL 1040: Too many connections
[error] [client xxx.xxx.xxx.xxx] (500)Unknown error 500: Admin API Error:
MySQL 1040: Too many connections
```

In `/var/log/mod_yvva.log` you might observe a similar error:

```
141107 12:11:44 [Error] -12036 (1040): Too many connections
141107 12:11:44 [Error] "startup.yv" (80)
```

This error indicates that the number of child processes spawned by the Apache http Server (e.g. when many TeamDrive Clients attempt to connect to the Host Server concurrently), causes the MySQL Server to run out of threads for handling the incoming database connections.

By default, the MySQL Server is configured to accept 151 concurrent connections. Each Apache child process can establish up to two MySQL connections (one for `mod_pspace` and one for `mod_yvva`, depending on what kind of requests it needs to serve). Therefore, the maximum number of connections should be adjusted to be at least 1.5 times the maximum number of child processes spawned by the Apache http Server (defined by the `MaxClients` directive in the Apache http Server configuration file `/etc/httpd/conf/httpd.conf`).

The value can be changed by adding the system variable `max_connections` to the `[mysqld]` configuration group in the MySQL Server configuration file `/etc/my.cnf`, e.g.:

```
[mysqld]
datadir=/var/lib/mysql
max_allowed_packet=4M
max_connections=350
socket=/var/lib/mysql/mysql.sock
user=mysql
```

You need to either restart the MySQL server in order to apply this change, or change the value at run-time, by running the following SQL statement as the MySQL root user:

```
mysql> SET GLOBAL max_connections=350;
```

Keep in mind that increasing the maximum number of connections also increases the memory requirements of the MySQL Server. For more details, please consult the MySQL Server and Apache http Server documentation:

<https://dev.mysql.com/doc/refman/5.6/en/too-many-connections.html>

https://httpd.apache.org/docs/2.2/mod/mpm_common.html#maxclients

<http://fuscata.com/kb/set-maxclients-apache-prefork>

12.1 Abbreviations

PBAC Prime Base AutomationClient

PBAS Prime Base ApplicationServer

PBT Prime Base Talk is an object oriented language specifically designed for the programming of “server-side” functionality common to intra- and internet Web sites. A large share of the TeamDrive Host and Registration Server functionality is implemented in PBT. The code is parsed and executed by the Yvva application server components.

SAKH Server Access Key HTTP for TeamDrive 2.0 Clients

TDES Team Drive Enterprise Server

TDNS Team Drive Name Service

TDRS Team Drive Registration Server

TDSV Same as **SAKH**, but for TeamDrive 3.0 Clients: Team Drive Server

TSHS Team Drive Scalable Hosting Storage.

RELEASE NOTES - VERSION 3.0.013

Host Server Version 3.0.013 is the next major release following after version 3.0.011 (Version 3.0.012 was an internal release that has not been published).

Version 3.0.013 contains the following features and notable differences to version 3.0.011:

- The TeamDrive Host Server installation can now be performed via RPM on Red Hat Enterprise Linux 6 and derivative distributions, which significantly improves the installation procedure and the process of applying updates.
- The initial setup and registration of a Host Server is now fully web-based. It's no longer necessary to provide a `hosting.txt` or `properties` file. Instead, all the required information can be entered in a web form.
- The entire Host Server configuration is now stored in the MySQL database. This includes configuration settings for S3 daemon and TSHS.
- The web-based TeamDrive Hosting Service Administration Console has been improved significantly, by simplifying the work flows for common administration tasks and fixing several usability issues.
- TSHS, the TeamDrive Scalable Hosting Storage and the TeamDrive S3 Daemon provide additional scalability options to expand the storage capabilities of a TeamDrive Hosting Service.
- It's now possible to generate a monthly report that contains detailed statistics about all existing Depots and Spaces within these depots, including the monthly traffic and disk usage.
- The Host Server no longer depends on the PrimeBase Application Environment. Instead, it now uses the Yvva Runtime Environment, which replaces the following components:
 - `mod_yvva` replaces `mod_pbas` for providing the web-based Administration Console and API. The stand-alone `pbas` instance is no longer required. As a consequence, the `pbur` MySQL database which was used by PBAS to manage user accounts and privileges is no longer required and has been removed.
 - `yvvad` replaces `pbac` for running background tasks. The former `p1_autotask` background task PBAC instance is now provided by the service `td-hostserver`, which uses `yvvad`.
 - `yvva` replaces `pbac` for command line operations that involve executing PBT code on the shell.
- The installation location of the TeamDrive PBT code has been changed from `/home/teamdrive/pbas` to `/opt/teamdrive/hostserver/`.
- The `sakgen` binary that used to be installed in `/home/teamdrive/sakh` is no longer required. Instead, the functionality to encrypt Space Depot access keys is now provided by the `tshs` binary.
- All TeamDrive Host Server processes now run under the user ID used by the Apache http Server (`apache`). A dedicated `teamdrive` user account is no longer required.
- By default, the MySQL databases are now installed in the default location `/var/lib/mysql` instead of `/spacedb`, which made it difficult to enable SELinux on the MySQL instance.
- For security reasons, the MySQL credentials required for accessing the MySQL Database are no longer stored in the default MySQL configuration file `/etc/my.cnf`. Instead, the `[p1db]` options group has now been moved into a dedicated configuration file `/etc/td-hostserver.my.cnf`, only readable by the `apache` user.

- The Apache httpd Server configuration file has been renamed from `teamdrive.conf` to `td-hostserver.httpd.conf`.
- The overall robustness of the TeamDrive Host Server has been improved by issuing more meaningful error messages and performing more safety and consistency checks.
- Each Space Volume now contains a file `teamdrive-volume-id` that contains a unique global volume ID, to ensure that multiple volumes are mounted to the correct location.

Table 13.1: Release Notes - Version 3.0.013

Build Date	Version	Comment
YYYY-MM-DD	3.0.013.7	
2014-12-09	3.0.013.6	<ul style="list-style-type: none"> • Fixed possible upgrade error from 3.0.011 when the MySQL database <code>pbpg</code> still existed, but the <code>Keys</code> table was already moved to the <code>pspace</code> database (REGSERVER-427) • Fixed bug in which failed Auto Tasks were not executed anymore (HOSTSERVER-407) • <code>mod_pspace</code>: fixed possible crash when system settings are NULL (e.g. in an upgrade scenario from 3.0.011 to 3.0.013, when httpd was started before <code>yvvd</code> performed the required schema updates) • <code>mod_pspace</code>: Fixed possible “Admin API: AES decode error- corruption detected” error when updating from older versions (timing issues could result in the generation of duplicate private keys) (HOSTSERVER-420, HOSTSERVER-422) • Increased the size of the <code>S3Options</code> settings field from 200 to 2000 chars, to accommodate longer option strings required for certain OpenStack environments (HOSTSERVER-425) • Installation: updated <code>RewriteRule</code> sets in the httpd configuration files (removed obsolete <code>/depot</code> rule, HOSTSERVER-424)
2014-09-26	3.0.013.5	<ul style="list-style-type: none"> • <code>mod_pspace</code>: fixed a Space corruption bug that could occur when updating from a previous Host Server version to version 3.0.013 and Space Volumes were using a non-standard naming scheme (not “volxxx”) • Admin Console: added “Repair” button that allows performing an automatic repair of Volumes affected by the corruption bug. Clients will be notified to perform a Space Restore operation on affected Spaces.
2014-09-18	3.0.013.4	<ul style="list-style-type: none"> • Admin Console: fixed 404 errors when opening the Admin URL without a trailing slash (HOSTSERVER-398) • Admin Console: the input focus is now automatically set to the password field (HOSTSERVER-392) • <code>s3d</code>: Fixed bug in path deletion on S3: if the path ended with ‘/’ it wasn’t being deleted. • <code>s3d</code>: exceptions are now logged in <code>/var/log/s3d.log</code>
Continued on next page		

Table 13.1 – continued from previous page

Build Date	Version	Comment
2014-09-05	3.0.013.3	<ul style="list-style-type: none"> • mod_pspace: Replaced the previously used MD5 implementation with calls to the MD5 routines provided by OpenSSL (yielding a 70% performance improvement when calculating MD5 checksums on large files) (HOSTSERVER-355) • mod_pspace: consolidated brand-specific settings into one place and disabled multi-part uploads for OpenStack • mod_pspace: Fixed bug where failed uploads (resulting in MD5 checksum failures) would still be accounted for as bytes written in the Space usage statistics (HOSTSERVER-352) • Fixed autotask <code>resetTraffic()</code> to properly reset the traffic for Spaces that had the <code>SPACE_TRAFFIC_FULL</code> status flag enabled. (HOSTSERVER-353) • Installation: security enhancement: set <code>ServerTokens</code> to <code>Prod</code> and <code>ServerSignature</code> to <code>Off</code> in <code>httpd.conf</code> to disable displaying the Apache Server version and OS version in the HTTP headers and on error pages (HOSTSERVER-357) • mod_pspace: Disabled unnecessary buffering of files fetched from S3 object store and passed back to the client. (HOSTSERVER-356) • tshs: <code>add-s3-host</code> will ping the S3 service before actually adding the host details. • Admin Console: security enhancement: don't display the version and build number on the login page and https redirection page (HOSTSERVER-359) • Security enhancement: disabled unneeded HTTP methods in <code>td-hostserver.httpd.conf</code> (only allow GET, POST, PUT, disable HEAD, OPTIONS, TRACE) (HOSTSERVER-361) • Virtual appliance security enhancement: set <code>ServerTokens</code> to <code>Prod</code> and <code>ServerSignature</code> to <code>Off</code> in <code>httpd.conf</code> to disable displaying the Apache Server version and OS version in the HTTP headers and on error pages (HOSTSERVER-357)
2014-07-14	3.0.013.2	<ul style="list-style-type: none"> • To avoid confusion, the S3-related configuration option <code>openStackAuthURL</code> was renamed to <code>openStackAuthPath</code>
2014-07-11	3.0.013.1	<ul style="list-style-type: none"> • Initial Release

RELEASE NOTES - VERSION 3.0.011 AND OLDER

Table 14.1: Release Notes - Version 3.0.011 and older

Build Date	Version	Comment
YYYY-MM-DD	3.0.011.6	<ul style="list-style-type: none"> • HOSTSERVER-228: Add settings for ClientPollFrequency and StatisticPollFactor • HOSTSERVER-241: Moved [pldb] group from my.cnf to a dedicated configuration file /etc/td-hostserver.my.cnf to improve security and packaging.
2014-04-22	3.0.011.5	<ul style="list-style-type: none"> • HOSTSERVER-224: Added SpaceStatisticEnabled and SpaceStatisticExportPath • Updated teamdrive.conf Apache configuration file: wrapped long lines and updated s3daemon file locations to match the defaults suggested in the Installation Manual • HOSTSERVER-191: Fixed Magic Username problem with sakgen by enclosing them with single quotes to avoid the shell from expanding them as variables. Fixed “bad file descriptor error”
2014-03-12	3.0.011.4	<ul style="list-style-type: none"> • Fixed HOSTSERVER-99: created database migration script mysql/v3.0.010_to_v3.0.011.sql to update the table structures, move the Keys table from database pbpg to pspace and renamed database td2apilog to hostapilog. • Removed default API_SALT in sql script. • Improved hosting.txt value validation.
2014-03-03	3.0.011.3	<ul style="list-style-type: none"> • Updated version number in pbstab from “4546” to “4547” • Fixed HOSTSERVER-172: The default MySQL table definition file mysql/plspace_schema.sql contained a wrong value for the configuration variable PathToSAKConverter. Instead of /home/teamdrive/sakh/sakgen it should have been /home/teamdrive/sakh/.
Continued on next page		

Table 14.1 – continued from previous page

Build Date	Version	Comment
2014-02-07	3.0.011.2	<ul style="list-style-type: none"> • Updated sample <code>hosting.txt</code> file: no trailing slash after <code>REGSERVERURL</code> • Updated and completed Translation files (grammar, typos, obsolete terms) • Set <code>PathToSAKConverter</code> configuration variable to <code>/home/teamdrive/sakh/sakgen</code> by default • Added <code>S3Daemon</code> config and script files to the installation package • Fixes to object store access log processing
2014-02-04	3.0.011.1	<ul style="list-style-type: none"> • Added parsing and error handling for <code>API_IP_LIST</code> and <code>API_SALT</code> from the <code>hosting.txt</code>. • <code>pbstab</code>: changed log file from <code>/home/teamdrive/pbas/setup/pbac.log</code> to <code>/var/log/pl_autotask.log</code> (Jira-Issue <code>HOSTSERVER-145</code>) • <code>pbstab</code>: fixed wrong path to <code>p1ctl.dal</code> • Fixed setting space status bit • Fixed autotask debug output • Fixed typos and obsolete reference to <code>p1ctl</code> from the translation files • Changed configuration variable 340 “Protocol Log File” in <code>pbas.env</code> from “<< Default Log >>” to <code>/var/log/pbas.log</code> - note that this file needs to be created and assigned to the user running the PBAS instance (<code>touch /var/log/pbas.log ; chown teamdrive:teamdrive /var/log/pbas.log</code>) • Fixed <code>HOSTSERVER-150</code>: removed reference to <code>td2apilog</code> database
2014-01-28	3.0.011.0	<ul style="list-style-type: none"> • First build of the 3.0.011 branch, using the scripted build
2012-08-22	3.0.009	<ul style="list-style-type: none"> • Fixed traffic <code>LastReset</code> bug
2012-08-03	3.0.008	<ul style="list-style-type: none"> • MySQL plugin with new reconnect; Fixed MySQL result set handling

DOCUMENT HISTORY

Date	Version	Name	Description
2011-12-06	1.0	Thomas Hess	Start
2012-02-28	1.2	JG	Corrections and enhancements. Added PBAC for background task (P1ctl, 7). Update screenshots.
2012-02-29	3.0.1	JG	Adding chapter Restore, minor additions.
2012-03-01	3.0.2	JG	Adding chapter 13.2 Some minor changes.
2012-03-01	3.0.3	EP	Added MySQL appendix
2012-03-05	3.0.4	EP	Modified LD_LIBRARY_PATH pbvm + pbas parameters added yum install libstdc++.i686
2012-05-21	3.0.5	EP	Added symbolic link for new mysql lib: libmysqlclient.so.18 -> libmysql.so.16.0.0 Added Charset=utf8; in connect.def
2012-05-22	3.0.6	EP	Fixed several instruction errors in the documentation
2012-06-18	3.0.7	EP	Fixed wrong documentation of the docs.tar.gz, setup.tar.gz and sakh.tar.gz in chapter "Update PBAS modules". Added hint not to use blanks in Volume names Changed PBAS to 4530 Added mysql password hint to use not more than 15 chars
2012-06-29	3.0.8	EP	Fixed admin URL (must end with "/")
2012-08-29	3.0.9	EP	Update to PBAS 4.5.33
2012-12-17	3.0.10	EP	Added UseHTTpsForPublishFiles Added hint to free memory Added setting to disable storing space names Added API_ReturnSpaceNames Added ForceHTTpsUsage

Date	Version	Name	Description
2013-01-28	3.0.10	EP	Added hint for swap file usage
2013-05-06	3.0.11	Paul McCullagh	Added TSHS documentation Improved consistency of terminology Improved introduction and added graphic
2013-05-21	3.0.12	Barry Leslie	Corrected some minor errors and reworded a few things.
2013-05-22	3.0.12	Barry Leslie	Added s3daemon documentation.
2014-01-27	3.0.011	Lenz Grimmer	Updated installation instructions to reflect packaging changes the new Hosting Server package (<code>HostingServer-3.0.011.x.tar.gz</code>) and latest PBAS package (<code>PrimeBase_TD.4546.tar.gz</code>). Re-arranged installation instructions to improve the workflow. Split TSHS documentation into a separate document.
2014-04-02	3.0.011	Lenz Grimmer	Converted documentation to reStructuredText/Sphinx Re-arranged content to support multiple documents sharing some chapters Created separate Virtual Appliance Installation Manual