TeamDrive Host Server Installation and Configuration

Release 3.5.2.0

Lenz Grimmer, Barry Leslie, Paul McCullagh, Eckhard Pruehs

2015

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 `td-hostserver` . . . 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
5.5 Installing the Postfix MTA (optional) . . . 16

6 Installing the Host Server Components **17**
6.1 Enable the TeamDrive Host Server `yum` Repository . . . 17
6.2 Download and Install the TeamDrive Host Server Package . . . 17
6.3 Installing the Host Server HTML Documentation (optional) . . . 17

7 Apache HTTP Server Installation and Configuration **19**
7.1 Update `httpd.conf` . . . 19
7.2 Disable Unneeded Apache Modules . . . 19
7.3 Configure `mod_ssl` . . . 20

8 MySQL Installation and Configuration **21**
8.1 Installing MySQL Server . . . 21
8.2 Creating TeamDrive MySQL User and Databases . . . 23

9 Pre-Installation Tasks **25**
9.1 Mount the Space Storage Volume . . . 25
9.2 Installing SSL certificates . . . 25
9.3 Starting the Host Server Instance . . . 25

10 Initial Host Server Configuration **27**
10.1 Registering and Activating the Host Server . . . 27

10.2 Setup and Administration . . . 30
10.3 Associating the Host Server with a Provider . . . 32
10.4 Testing Client Access . . . 32

11 Post-Installation Tasks **33**
11.1 Startup Sequence / Dependencies . . . 33
11.2 Starting the Apache HTTP Server at Boot Time . . . 33
11.3 Starting TeamDrive Service at Boot Time . . . 33
11.4 Next steps . . . 33

12 Troubleshooting **35**
12.1 List of relevant configuration files . . . 35
12.2 List of relevant log files . . . 35
12.3 Enable Logging with Syslog . . . 36
12.4 Tracing Client Accesses to a Single Space . . . 37
12.5 Common errors . . . 37

13 Appendix **41**
13.1 Abbreviations . . . 41

14 Release Notes - Version 3.5 **43**
14.1 Key features and changes . . . 43
14.2 Change Log - Version 3.5 . . . 45

15 Release Notes - Version 3.0.013 **49**
15.1 Change Log - Version 3.0.013 . . . 50

16 Release Notes - Version 3.0.011 and older **55**

17 Document History **57**

CHAPTER

ONE

COPYRIGHT NOTICE

TeamDrive Systems GmbH
https://www.teamdrive.com
Max-Brauer-Allee 50
22765 Hamburg, Germany
Email: info@teamdrive.com

CHAPTER

TWO

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.

CHAPTER

THREE

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 1.2 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.

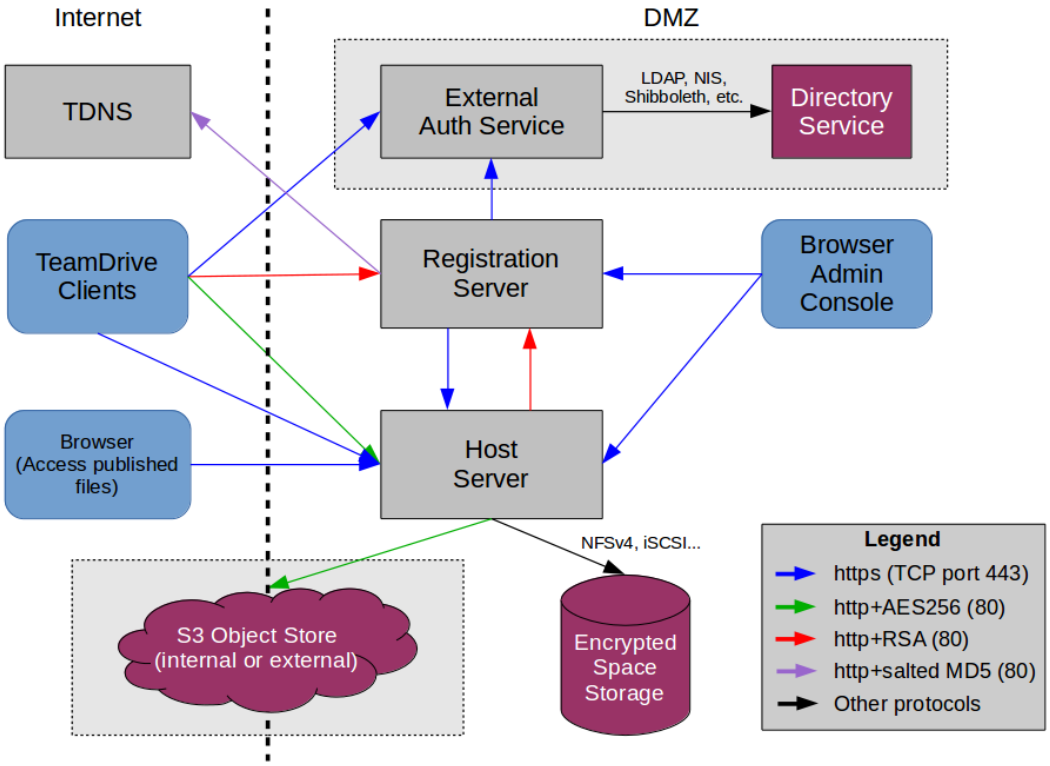

Fig. 3.1: TeamDrive Hosting Service Networking Overview

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.

CHAPTER

FOUR

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:

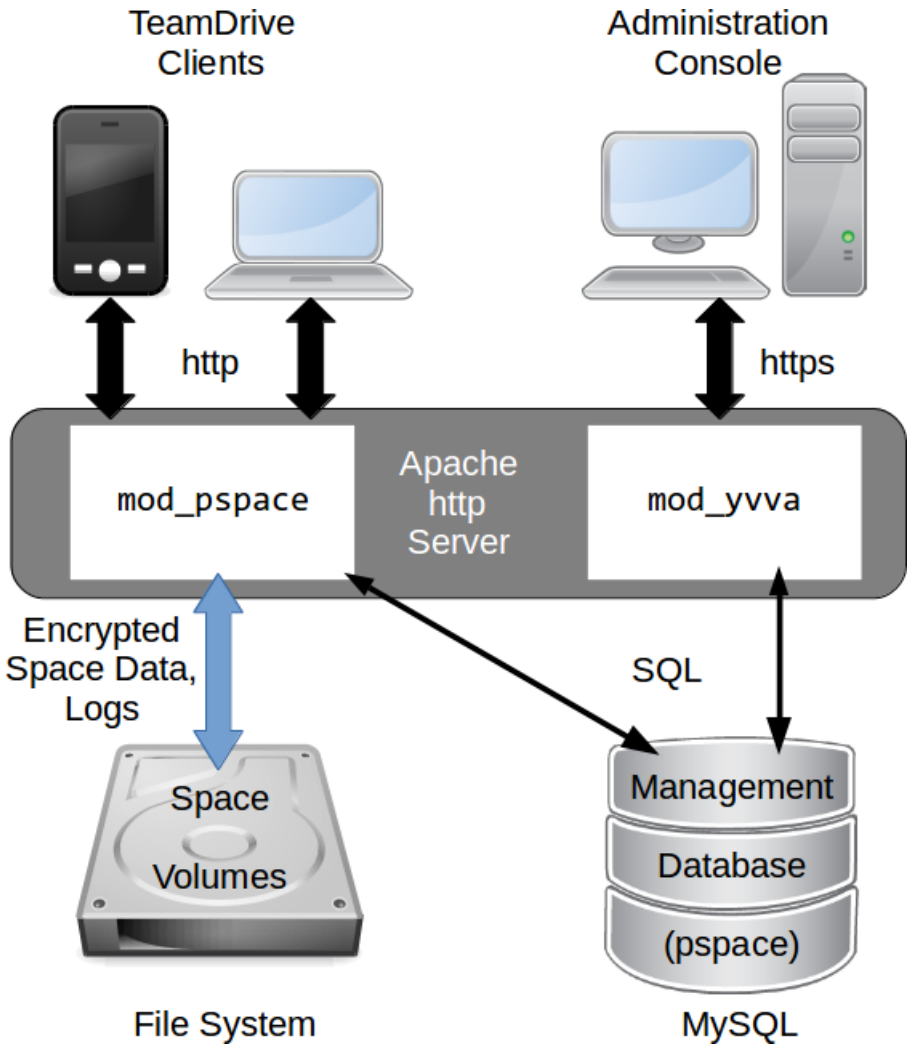

Fig. 4.1: TeamDrive Hosting Service Overview

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.

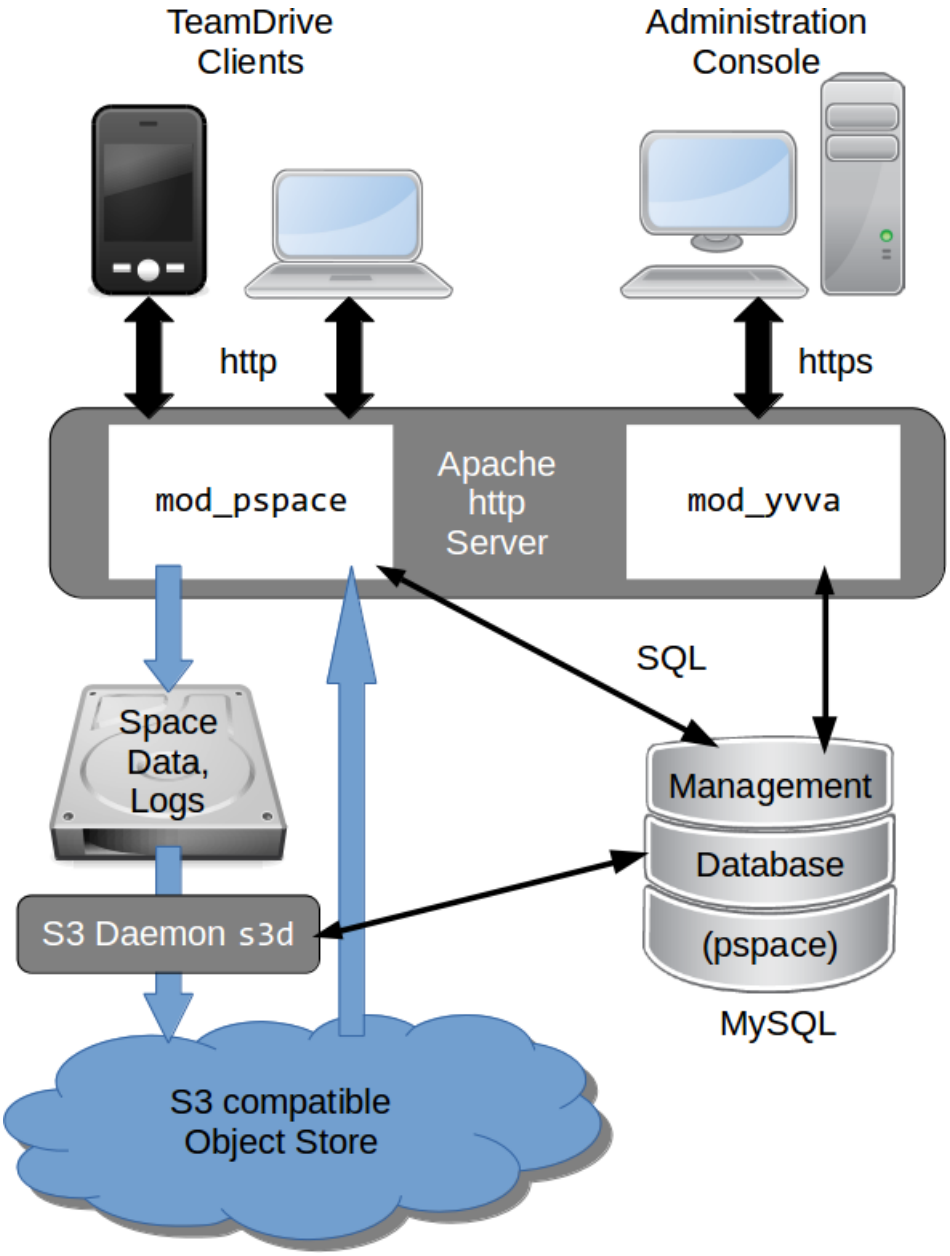

Fig. 4.2: TeamDrive Hosting Service using an S3-compatible object store

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-Compatible 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.

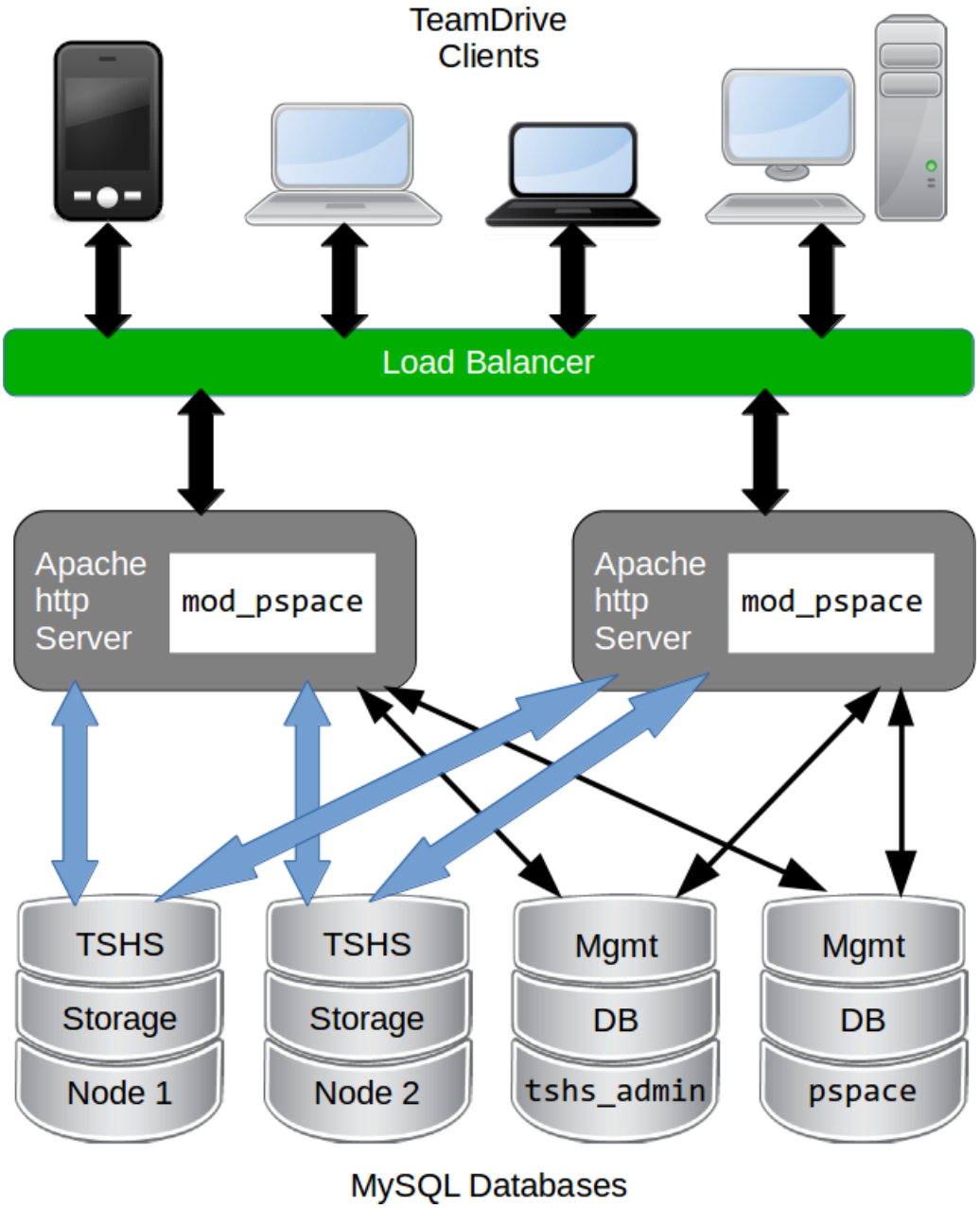

Fig. 4.3: TeamDrive Scalable Hosting Storage (TSHS)

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
`-- vol01
    |-- 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
        |   `-- 8CN7S0800000A004UH0Q9TP323BBNZ8E
        |       `-- 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 Sessions**: 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. 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.
- **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".

- **Process S3 Logs**: Background task to calculate the traffic usage on an object store as described in the chapter "Enabling Object Store Traffic Usage Processing" in the Host Server Administration Guide for details.
- **Notify Volume**: Checks the disk utilization of Space Volumes and sends out a notification email if the usage exceeds a configurable level.
- **Clean up API log**: Removes entries from the API log table older than 30 days.
- **Delete Public Files**: Remove published files that have reached their expiry time.

CHAPTER

FIVE

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
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     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

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

5.5 Installing the Postfix MTA (optional)

If you intend to use the email-based two-factor authentication for accessing the Host Server Administration Console, or if you want to be notified about Space Volumes running out of disk space via email, the TeamDrive Host Server needs to be configured to send out these notifications via SMTP.

The Yvva Runtime Environment that provides the foundation for the Host Server is only capable of sending out email using plain SMTP via TCP port 25 to a local or remote MTA.

If your mail server requires some form of authentication or transport layer encryption like SSL/TLS, you need to set up a local MTA that relays all outgoing email from the TeamDrive Host Server to your mail server using the appropriate protocol and credentials.

We recommend configuring a local Postfix instance to perform this duty. The following packages need to be installed:

```
[root@regserver ~]# yum install postfix mailx cyrus-sasl-plain
```

The detailed configuration of the local Postfix instance depends heavily on your local environment and how the remote MTA accepts remote submissions and is out of the scope of this document.

See the Postfix SMTP client documentation at http://www.postfix.org/smtp.8.html for details on how to configure Postfix to use a relay server and make sure to test the correct operation by sending local emails using the `mail` command line utility and watching the Postfix log file `/var/log/maillog` for errors.

Once the Postfix service has been configured correctly, ensure that it will be started automatically upon system boot:

```
[root@regserver ~]# chkconfig postfix on
```

CHAPTER

SIX

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 3.5" repository, which you can check by running yum repolist afterwards:

```
[root@hostserver ~]# yum repolist
Loaded plugins: security
repo id                              repo name                                  status
td-hostserver-3.5                    TeamDrive Host Server Version 3.5          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 1.2 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.

6.3 Installing the Host Server HTML Documentation (optional)

Beginning with Host Server version 3.0.013.10, the documentation (in HTML format) can be installed locally, so you can access it directly from the Host Server (or any other host running an Apache HTTP Server).

To install the HTML Documentation, install the following package via yum from the "TeamDrive Host Server" repository:

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

The HTML documents will be installed in directory `/var/www/html/td-hostserver-doc`. From your web browser, open the following URL to access the documentation:

http://hostserver.yourdomain.com/td-hostserver-doc/

Note: This step is optional. If you leave the documentation installed when the Host Server goes into production and is accessible from the public Internet, you should ensure to restrict access to this URL to trusted hosts or networks only. This can be achieved by adding the appropriate access control rules to the file `/etc/httpd/conf.d/td-hostserver-doc.httpd.conf`.

CHAPTER

SEVEN

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/p1a$1 [PT]
RewriteRule ^/pbas/p1_as/api/(.*)$ /yvva/api/$1 [PT]
RewriteRule ^/pbas/p1_as/p1a/(.*)$ /primespace/admin/$1 [PT]
</VirtualHost>
```

CHAPTER

EIGHT

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 reliablility 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:

```
[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!

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

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 ~ ]# 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 at system bootup (only when using a local MySQL Server)
- Create the MySQL user account `teamdrive`, assign the provided password and assign the necessary 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 you defined while running `mysql_secure_installation`
- 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 3.5.x.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-2015-05-19-17:19.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-2015-05-19-17:19.bak'

Finished!
The MySQL configuration for TeamDrive Hosting Service
version 3.5.x.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
```

CHAPTER

NINE

PRE-INSTALLATION TASKS

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 HTTP 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.

> **Warning:** The space volume's file system **must** be mounted to `/spacedata/vol01`, not `/spacedata`, to make it possible to mount additional volumes underneath the `/spacedata` directory, if required.

9.2 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 to 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.

9.3 Starting the Host Server Instance

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

9.3.1 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. You usually don't have to modify these settings.

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...
```

If `td-hostserver` does not start (process `yvvad` is not running), check the log file `/var/log/td-hostserver.log` for errors. See chapter Troubleshooting for details.

9.3.2 Starting the Apache HTTP Server

Now the Apache HTTP Server can be started, which provides the TeamDrive Host Server functionality (via `mod_pspace`) 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
```

Warning: At this point, the Host Server's web server is answering incoming requests from any web client that can connect to its address. For security purposes, you should not make it accessible from the public Internet until you have concluded the initial configuration, e.g. by blocking external accesses using a firewall.

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

```
[notice] mod_yvva 1.2.0 (May  5 2015 11:06:52) loaded
[notice] Logging (=error) to: /var/log/mod_yvva.log
[notice] Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured
-- resuming normal operations
[notice] mod_pspace 1.6.17 Loaded; Build May  6 2015 12:42:39;
Crash-Reporting-Disabled
```

Please consult chapter troubleshooting if there is an error when starting the service.

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

```
Admin API, Error loading parameters: Host Server setup has not been completed
```

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.

CHAPTER

TEN

INITIAL HOST SERVER CONFIGURATION

10.1 Registering and Activating the Host Server

From a desktop system that can connect to the Host Server via HTTPS, start a web browser like Mozilla Firefox, Google Chrome (or any other modern web browser) and start the configuration process by opening the following URL in your browser:

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

This should open the Host Server Setup page. If you get an error message like "500 Internal Server Error", check the log files for any errors. See chapter web installation 500 internal server error for details.

Note: If you haven't replaced the server's self-signed default SSL certificate yet, your web browser most likely will complain about an untrusted/insecure connection. Either replace the SSL certificate with an appropriate one before you proceed, or ignore this message.

Alternatively, you can access the Setup Page 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:

Fill out the fields according to your environment and requirements:

Admin Username The name of the user account with full administrative privileges.

Admin Password The adminstrator password that you need to provide to login to the Host Server Administration Console.

Admin Email The email address of the Administrator. This field is optional. This email address is used for 2-factor authentication (if enabled).

Host Server 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.

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.**

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.**

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.**

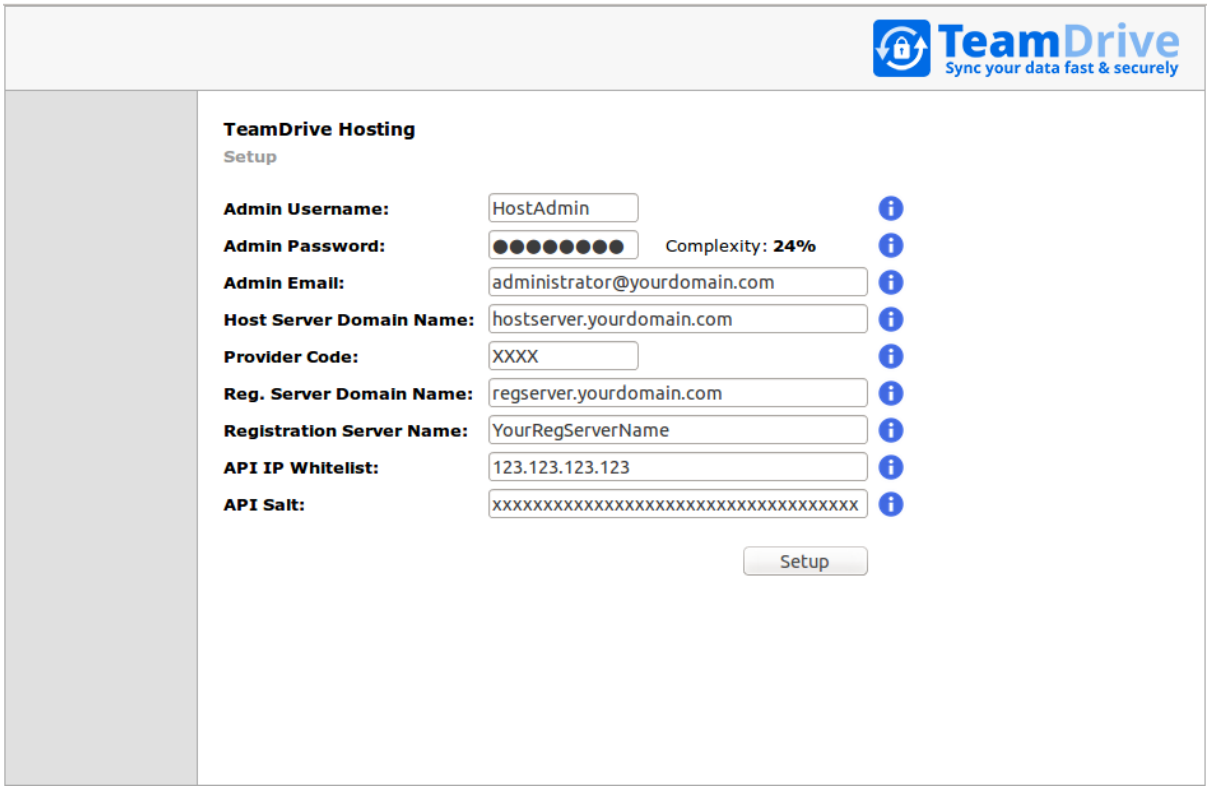

Fig. 10.1: Host Server Setup Page

API IP Whitelist 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.

After you have entered all the required details, click **Setup** to initiate the Host Server configuration and registration process with the Registration Server. After performing some initial checks, the setup process will summarize the information that it will use to perform the registration with the selected Registration Server.

Click **Register Server** to proceed with the registration, **Reset** to abort and return to the setup page.

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

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

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 and license associated with that user.

Befor the Host Server registration can be concluded, you are required to enter an Activation Code. For 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 your Registration Server operator (usually TeamDrive Systems).

If you manage your own Registration Server (version 3.0.018 or later), the activation code can be obtained from the Registration Server's Administration Console via the the **Manage Devices** page (**Manage Clients -> Manage**

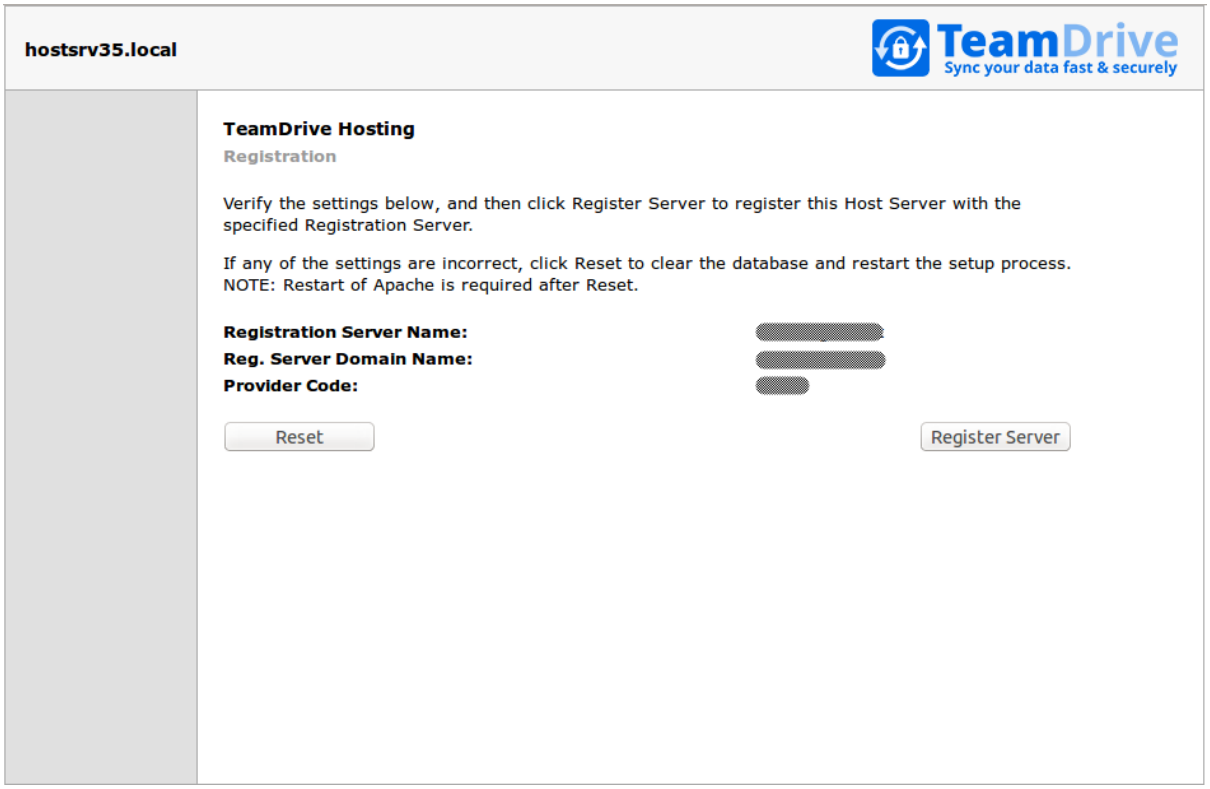

Fig. 10.2: Host Server Registration Confirmation

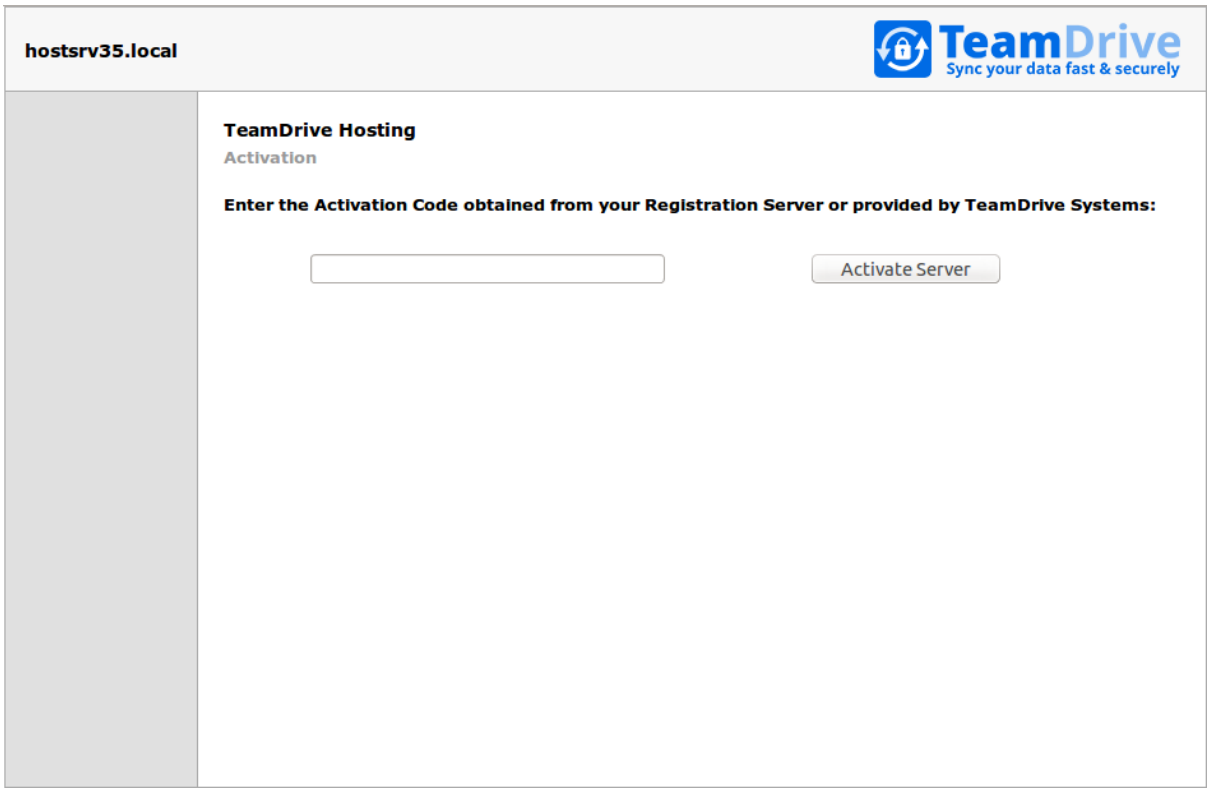

Fig. 10.3: Host Server Activation Window

Devices on Registration Server version 3.5 and up).

On older versions of the 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:

```
[root@regserver ~]# mysql -u teamdrive -p
Enter password:
mysql> SELECT activationcode, name FROM td2reg.TD2Device \
WHERE Name LIKE "tdhosting.hostserver.yourdomain.com";
+----------------------------------+-------------------------------------+
| activationcode                   | name                                |
+----------------------------------+-------------------------------------+
| XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | 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 **Activate server**.

10.2 Setup and Administration

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

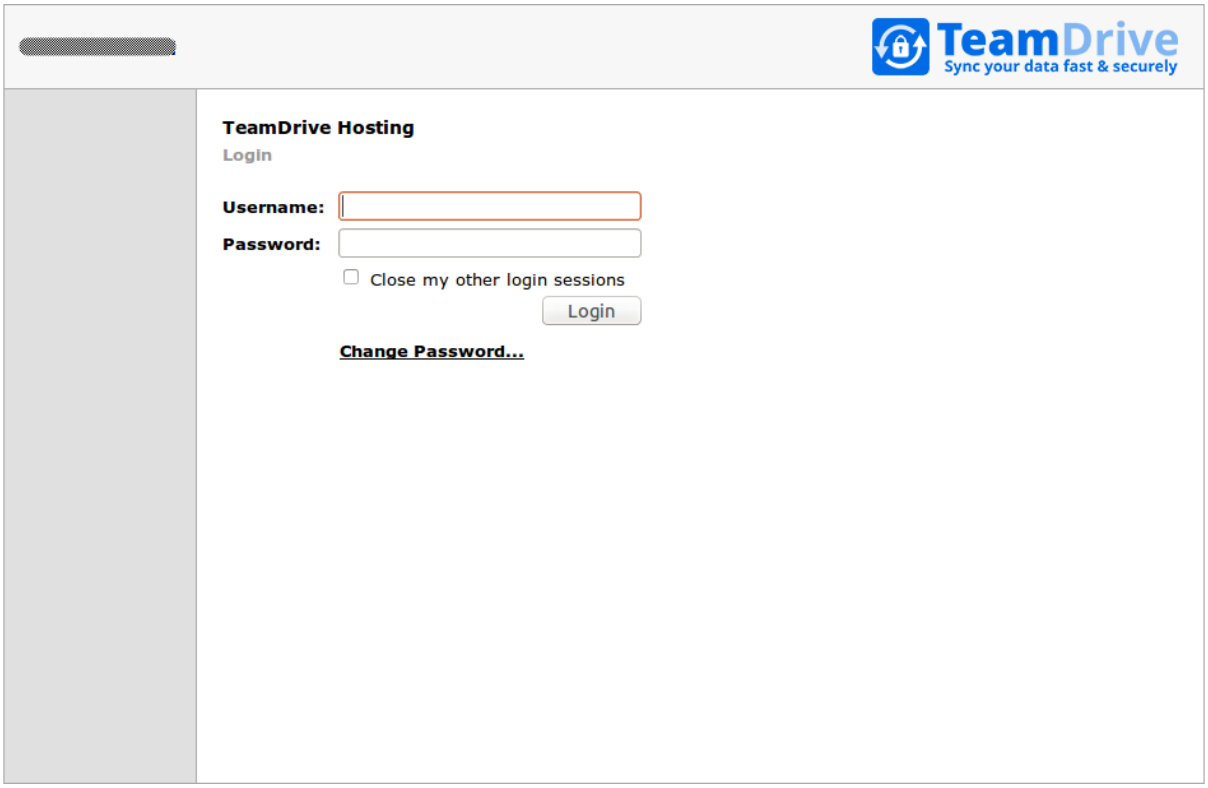

Fig. 10.4: Host Server Admin Console: Login Screen

Enter the username and password you defined during the initial setup to log in.

Upon successful login, you will see the Host Server's Administration Console Home Screen.

At this point, you have concluded the Host Server's basic configuration and registration. See the *TeamDrive Host Server Administration Guide* for more details on how to use the Administration Console and how to accomplish other configuration tasks.

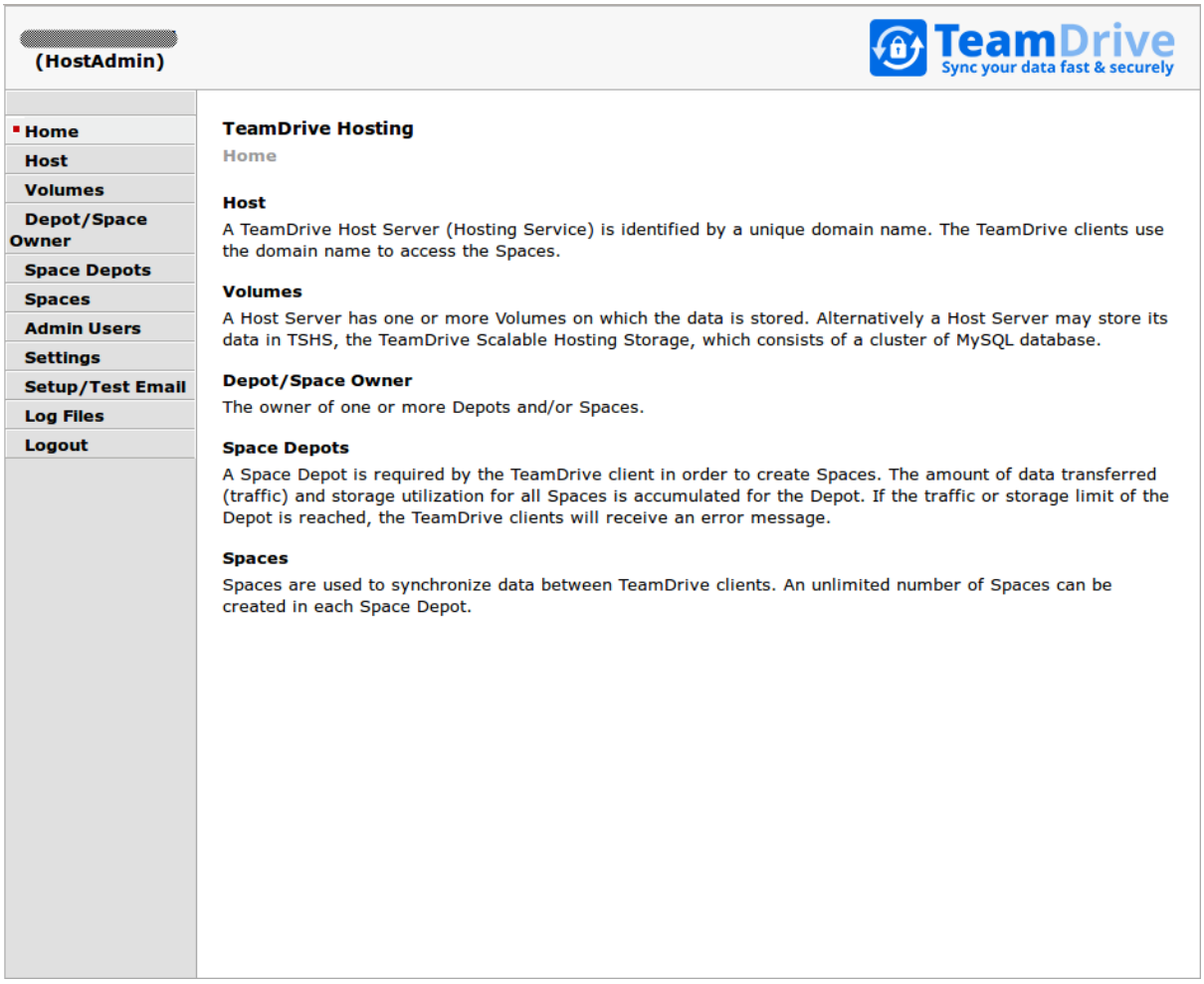

Fig. 10.5: Host Server Admin Console: Home Screen

10.3 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), **Edit Provider Settings** (Registration Server version 3.0.018) or **Server Management -> Provider Settings** (Registration Server 3.5).

In the section **Provider Settings**, click the Button labelled **HOSTSERVER**.

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

The `HOST_SERVER_NAME` setting and related options 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`.

10.4 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.

CHAPTER

ELEVEN

POST-INSTALLATION TASKS

11.1 Startup Sequence / Dependencies

To ensure a proper service start and to minimize error messages on the TeamDrive Client side, the following startup sequence of the TeamDrive Enterprise Server components and services should be observed.

1. Start the TeamDrive Host Server services in the following order:
   (a) Mount the Space Volumes (e.g. NFSv4, local/virtual disks)
   (b) Start the Host Server MySQL database service
   (c) Start the `td-hostserver` background service
   (d) Start the Apache HTTP Server
2. Start the TeamDrive Host Server services as outlined in the *TeamDrive Host Server Installation Guide*.

11.2 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
```

11.3 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
```

11.4 Next steps

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

CHAPTER

TWELVE

TROUBLESHOOTING

12.1 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.

12.2 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/td-hostserver.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-cnf-file=/etc/td-hostserver.my.cnf
  YvvaSet log-file=/var/log/td-hostserver.log
  YvvaSet log-level=error
</Location>
```

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

This log file is also used by 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 an S3 compatible object store or 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 = Error, 2 = Warning, 3 = Notice, 4 = Trace, 5 = Debug. Changing these values requires restarting the Apache HTTP Server.

`/var/log/httpd/`: The Apache HTTP 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`.

12.3 Enable Logging with Syslog

As outlined in list of relevant log files, the TeamDrive Host Server logs critical errors and other notable events in various log files by default.

Starting with Host Server version 3.5 and Yvva 1.2, it is now possible to redirect the log output of some server components to a local `syslog` instance as well.

Note: Please note that other components of the TeamDrive Host Server, e.g. `mod_pspace`, `s3d` or `tshs` currently do not provide syslog support. This limitation may be lifted in future versions of the TeamDrive Host Server software.

Syslog support is an essential feature for auditing, security and/or compliance reasons, as it allows you to funnel all log messages into a centralized syslog server.

This makes it easier to monitor the logs for critical events or errors and prevents tampering with the log files in case of a security breach. It also helps to maintain control over the disk space utilization on the server, as growing log files can't accidentally fill up the file system.

To enable syslog support, the log file name in the `log-file` setting has to be replaced with the keyword `syslog`. Optionally, a custom process identifier can be supplied, by appending it to the `syslog` keyword, using a colon as the separator, e.g. `log-file=syslog:my_process_identifier`. If not used, the default process identifier will be used, which is the name of the program executable.

To enable syslog support for the Yvva-based `td-hostserver` backround service, edit the `log-file` setting in file `/etc/td-hosting.conf` as follows:

```
log-file=syslog:td-hostserver
```

You need to restart the `td-hostserver` background service via `service td-hostserver restart` in order to activate this change. If the `log-level` is set to `debug` you will now see log messages appearing in `/var/log/messages`:

```
Jun 23 11:57:33 localhost td-hostserver: notice: yvvad startup
Jun 23 11:57:33 localhost td-hostserver: notice: Using config file:
/etc/td-hosting.conf
Jun 23 11:57:33 localhost td-hostserver: notice: No listen port
Jun 23 11:57:33 localhost td-hostserver: notice: yvvad running in repeat 60
(seconds) mode
```

To enable syslog support for the Host Server API and Administration Console, edit the `YvvaSet log-file` setting in file `/etc/httpd/conf.d/td-hostserver.httpd.conf`:

```
YvvaSet log-file=syslog
```

You need to restart the Apache HTTP Server via `service httpd restart` in order to activate this change. If the `log-level` is set to `debug` you will now see log messages appearing in `/var/log/messages`:

```
Jun 23 12:06:04 localhost mod_yvva: notice: mod_yvva 1.2.1 (May 21 2015
11:00:12) startup OK
```

12.4 Tracing Client Accesses to a Single Space

For debugging issues with a specific Space, it might be useful to enable more verbose tracing of activity between the Host Server and the TeamDrive Clients accessing this Space.

For this purpose, access to that Space can be traced by providing the Space's ID to the option `watched_space_id` in `/etc/httpd/conf.d/td-hostserver.httpd.conf` as follows:

```
<Location /primespace>
      SetHandler pspace-handler
      MySQLCnf /etc/td-hostserver.my.cnf

      watched_space_id <space ID>

      # Necessary to ignore the extra Range-header
      # (see Range-header note in the documentation)
      RequestHeader unset Range
</Location>
```

Restart the Apache HTTP Server with `service httpd restart`. Any activity on the selected Space will now be logged into the log file `/var/log/mod_pspace.log`.

Note: Remove this option and restart the Apache HTTP Server once you've finished analyzing the problem, to avoid uncontrolled growth of the log file.

12.5 Common errors

12.5.1 Web Installation: "500 Internal Server Error"

This error can be triggered by several error conditions. Check the log file `/var/log/td-hostserver.log` for details.

Some common errors include:

```
[Error] -12036 (2002): Can't connect to local MySQL server through socket
'/var/lib/mysql/mysql.sock' (25)
[Error] "startup.yv" (80)
```

The local MySQL Server's socket file can't be opened. This could either be a permission problem, or the MySQL Server is simply not available. Check that MySQL is actually up and running (e.g. by running `service mysqld status`) and restart it, if necessary. If the error persists, check the MySQL error log file (usually `/var/log/mysqld.log`) for hints.

Similarly, an error like the following one indicates that a remote MySQL Server might not be answering (e.g. because of a firewall rule or because it's not running):

```
[Error] -12036 (2003): Can't connect to MySQL server on
'mysql.yourdomain.com' (107)
[Error] "startup.yv" (80)
```

If you see `Access denied` errors like the following one:

```
[Error] -12036 (1045): Access denied for user 'teamdrive'@'localhost' (using
password: YES)
[Error] "startup.yv" (32)
```

Either the username or password used to connect to the MySQL Server are wrong. Double check that the MySQL username and password provided in `/etc/td-hostserver.my.cnf` are correct, e.g. by trying to connect to the MySQL server using these credentials with the `mysql` command line client.

If you see the following error when connecting to a remote MySQL Server:

```
[Error] -12036 (1130): Host 'regserver.yourdomain.com' is not allowed to
connect to this MySQL server
[Error] "startup.yv" (80)
```

Check the TeamDrive MySQL user's privileges on the remote MySQL server, e.g. by running `SHOW GRANTS FOR 'teamdrive'@'regserver.yourdomain.com';` and make sure that this user is allowed to connect to the MySQL server from the Registration Server's host.

12.5.2 Errors When Registering the Host Server

If the Host Server Registration fails, check `/var/log/td-hostserver.log` on the Host Server as well as `/var/log/td-regserver.log` on the Registration Server for hints (`/var/log/pbt_mod.trace` for Registration Server versions before version 3.5) . See the Troubleshooting chapter in the Registration Server Installation Manual for details.

12.5.3 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:

```
[Note] DROP DATABASE pbpg;
[Error] -12036 (1044): Access denied for user 'teamdrive'@'localhost' to
database 'hostapilog'
[Error] "p1setup.pbt" P1Setup:upgradeSettings(328)
[Error] "p1setup.pbt" P1Setup:setupDatabase(14)
[Error] "p1setup.pbt" (506)
```

`Unknown database`:

```
[Error] -12036 (1049): Unknown database 'hostapilog'
[Error] "p1setup.pbt" P1Setup:upgradeSettings(328)
[Error] "p1setup.pbt" P1Setup:setupDatabase(14)
[Error] "p1setup.pbt" (506)
[Error] "p1_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`:

```
[notice] mod_pspace 1.6.17 Loaded; Build May  6 2015 12:42:39;
Crash-Reporting-Disabled
[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`:

```
[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.

12.5.4 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.

12.5.5 "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.

12.5.6 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/td-hostserver.log` you might observe a similar error:

```
[Error] -12036 (1040): Too many connections
[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

CHAPTER

THIRTEEN

APPENDIX

13.1 Abbreviations

PBAC **P**rime **B**ase **A**utomation**C**lient

PBAS **P**rime **B**ase **A**pplication**S**erver

PBT **P**rime **B**ase **T**alk 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 **S**erver **A**ccess **K**ey **H**TTP for TeamDrive 2.0 Clients

TDES **T**eam **D**rive **E**nterprise **S**erver

TDNS **T**eam **D**rive **N**ame **S**ervice

TDRS **T**eam **D**rive **R**egistration **S**erver

TDSV Same as **SAKH**, but for TeamDrive 3.0 Clients: **T**eam **D**rive **S**er**v**er

TSHS **T**eam **D**rive **S**calable **H**osting **S**torage.

CHAPTER

FOURTEEN

RELEASE NOTES - VERSION 3.5

14.1 Key features and changes

TeamDrive Host Server Version 3.5 is the next major release following after version 3.0.013.

Note: Please note the the version numbering scheme for the Host Server has been changed starting with version 3.5. The first two digits of the version string now identify a released version with a fixed feature set. The third digit, e.g. "3.5.1" now identifies the patch version, which increases for every public release that includes backwards-compatible bug or security fixes. A fourth digit identifies the build number and usually remains at zero, unless a rebuild/republishing of a release based on the same code base has to be performed (e.g. to fix a build or packaging issue that has no effect on the functionality or feature set).

Version 3.5 contains the following features and notable differences to version 3.0.013. See releasenotes-3.0.013 for a detailed description of the change history for that version.

14.1.1 Host Server Functionality

- Security enhancement: Files can now be published with an expiration date after which an auto task on the Host Server will automatically remove the published files again. Additionally, published files can now be protected by a password. This functionality requires support on the TeamDrive Client side, which is implemented in versions 4.1 of the TeamDrive Client. For entering the password in a html page, a few templates were added. The templates could be customized and will not overwritten when updating to a newer Host Server version.
- Security enhancement: A request for a published file no longer returns the actual file directly, except in the case where the request comes from tools like `wget` or `curl`. Instead, the document returned is an HTML file containing JavaScript calls that load the actual file using a temporary URL. This solves a potential security problem in which URLs of published documents can be inadvertently disclosed to unintended recipients in the following scenario: A TeamDrive user publishes a document that contains URLs pointing to a third-party website (e.g. a PDF or office document). The user, or an authorized recipient of the published URL, clicks on a hyperlink embedded in the document. At that point, the referrer header discloses the document's publish URL to the third-party website. Someone with access to that header, such as the webmaster of the third-party website, could then access the link to the published document. (HOSTSERVER-316)
- A new Client/Server protocol, supporting parallel polling of Spaces for increased throughput/performance, batched delete operations (e.g. emptying the Trash) and "soft" locking of files. These features require support on the TeamDrive Client side, which is scheduled to be implemented in future versions of the TeamDrive Client.
- Performance improvement: The Host Server now uses a database table instead of action files in the Space Volume's file system for signalling actions like uploading or deleting files to the object store. As a result, `s3d` no longer has to perform a full scan of all Space Volumes to look for new or changed files. (HOSTSERVER-284) Additionally, the MD5 digest of a file is also stored in this table, so `s3d` does not need to perform a recalculation of the checksum before uploading the file to the object store. During an upgrade from a previous version, any remaining action tag files in the file system will be imported into the database. Afterwards, the server setting `ImportS3tagFiles` should be set to `False`.

- The S3 daemon `s3d` now only performs a full scan of all Space Volumes once per day by default, looking for old files to be transferred to the object store. The age of these files is set via the settings variable `MaxFileAge`. The maximum file age should be set long enough to ensure that no file that may still be in the process of being uploaded by a Client will be sent to the Object Store, otherwise the Client would have to restart the upload from scratch.

14.1.2 Administration Console

- Security improvement: Added support for managing multiple user/administrator accounts. There are 2 types of users: Superuser and Administrator. Only the Superuser may manage other users. The Administrator may view all users and only update his own user account. (HOSTSERVER-366)
- Security improvement: Disabled auto completion on the login form. (HOSTSERVER-379)
- Security improvement: The complexity of entered passwords is now indicated. (HOSTSERVER-374)
- Security improvement: it is now possible to enable two-factor authentication via email. If enabled, the user is required to enter a security code provided via email in addition to his username and password.
- Security improvement: On login, the user will get an error if he has another logged in session. To proceed, the user must check the checkbox titled: "Close my other login sessions". (HOSTSERVER-376, HOSTSERVER-377)
- Security improvement: The following events are now logged at the "notice" level: login, logout, failed login attempts and changes to user accounts.
- Security improvement: the amount of search results (e.g. Spaces, Depots or users) is now limited to a maximum defined by the `MaxRecordsDisplayed` setting, which can only be changed by the Superuser.
- Administration: It is now possible to change a Depot's status (e.g. enabled, disabled, deleted)
- Administration: Added support for viewing selected server log files and the Host Server API log. (HOSTSERVER-348, HOSTSERVER-243)
- Administration: It is now possible to track and display modifications made to Space Depots (e.g. via API calls coming from the Registration Server or via the Host Server Admin Console). (HOSTSERVER-388)
- Administration: When creating a new Space Volume via the Administration Console, the system now checks if the directory actually exists on the file system before creating the Volume. (HOSTSERVER-349)
- Usability: References like Depot Names, Volume names and owners in the Space list are now clickable, to improve the quick navigation between pages. (HOSTSERVER-390)
- Usability: Objects like Spaces or Depots that have been marked as deleted are now hidden in result lists by default. They can be made visible again by changing the setting `ShowDeletedObjects` from `false` to `true`. (HOSTSERVER-442)
- Usability: Administration Console now better visualizes errors like missing Space Volumes.
- Usability: Units displayed for disk space or traffic usage now use the correct units (e.g. MiB, or GiB), to avoid confusion caused by conversions between different units. Space and traffic levels are now displayed in percent instead of absolute units.

14.1.3 Administration / Installation

- Administration: The Host Server's log levels have been aligned with the ones used by the Registration Server and the Yvva Runtime Environment. Valid log levels are: 1 (Error), 2 (Warning), 3 (Notice), 4 (Trace), 5 (Debug). In production mode the default log level is 3 (Notice). Setting the log file name to `syslog` will now send log output to the local syslog service. You can add an optional "Log Identity after a colon in the log file name, for example: `syslog:my-log-id`. The default Log Identity is name of the program, e.g. `s3d` or `tshs`.

- Administration: The central log file `/var/log/td-hostserver.log` is the central log location for all Yvva-based components (e.g. the Host Server API, Administration Console or `td-hostserver` background service); the log files used in previous versions (e.g. `/var/log/mod_yvva.log`, `/var/log/p1_autotask.log`, `/var/log/pbvm.log`) will no longer be used.
- Administration: TSHS now supports the additional commands `disable-s3-host`, `enable-s3-host` and `delete-s3-host` that allow for disabling/removing the synchronization of objects to an S3-compatible object store. Calling `disable-s3-host` marks a host entry as "disabled". Calling `delete-s3-host` deletes a host entry unless the entry is referenced by a file. In this case the entry will be marked as deleted. If an entry is marked as disabled or deleted, no further data will be uploaded to the object store. However, accessing existing objects from the object store will continue to work. Calling `enable-s3-host` will re-enable the synchronization of objects to the object store, including the upload of all objects that have been uploaded to TSHS while the object store was marked as disabled. If a disabled or deleted host is marked as current, then TSHS will generate an error on each write attempt.
- Administration: Added an auto task that can be enabled to send out notification emails if a Space Volume's disk utilization reaches a configurable level.
- Administration: Added an auto task that removes published files that have reached their expiry time.
- Administration: Added an auto task that can be enabled to delete API log entries older than 30 days from the `hostapilog` table.
- Installation: TSHS now supports reading options from a configuration file. The default is `/etc/tshs.conf`. The default options that were previously stored in the TSHS init script `/etc/init.d/tshs` have now been moved to the configuration file instead. (HOSTSERVER-303)
- Installation: Optionally configure email support (required when using two-factor authentication). (HOSTSERVER-437)
- Installation: The initial Host Server setup process now asks for both a user name and password for the Superuser account. (HOSTSERVER-438)
- Installation: Host Server 3.5 now requires Yvva Runtime Environment version 1.2 or later. This version is included in the Host Server's yum package repository and will be installed automatically.
- Installation: The distribution now contains the tool `mys3`, which can be used to interact with an S3 compatible object store.

14.1.4 API

- Changes to a Space Depot performed by the API functions `addusertodepot` and `deleteuserfromdepot` are now added to the Depot's change log.
- The MD5 checksum value calculated over API requests no longer needs to be passed in lowercase when submitting the request. (HOSTSERVER-426)
- For debugging purposes, erroneous API requests are now logged to the API requests table as well. (REGSERVER-465)

14.2 Change Log - Version 3.5

14.2.1 3.5.2 (2015-12-08)

14.2.2 Host Server Functionality

- Fixed bug in schema definition for FileSize column in PublicFile table
- Fixed bug with comparison of timestamp to DATE value in the database because of daylight savings time corrections (HOSTSERVER-578).
- Fixed TD3 Protocol crash in loadSpaces() (HOSTSERVER-580).

- Fixed return of .tdsv files
- Fixed disk usage calculation error in case of host server is connected to an object store (HOSTSERVER-576).
- Fixed duplicate object store log files processing in case of identical or missing S3ToProcessPath and S3ProcessedPath (HOSTSERVER-586)
- Fixed adding external traffic in API-call "getspacedata" (HOSTSERVER-587)
- Fixed retrieval of public file where name comtains reservied URL characters (HOSTSERVER-581)
- Correctly log last.log.lock when reading and writing log files and if no maximum len is given, return the entire log
- Fixed error when adding MOVE action to database –> Illegal mix of collations (HOSTSERVER-589)
- Fixed TD3Protocol: Empty reply for getblob (HOSTSERVER-595)
- Fixed exclude "Error getting size from ..." in case of zero download for object store access log processing (HOSTSERVER-593)
- Corrected RepositoryChanges table duplicate constants
- S3Daemon: Fixed error 'The Content-MD5 you specified did not match what we received.' It was possible that the checksum value stored in the database did not match that of the actual file (HOSTSERVER-591).
- S3Daemon: Fixed problem with multipart uploads. If an attempt to transfer a zero length file to S3 it would fail but would try again later so it was stuck in an endless loop (HOSTSERVER-588).
- Added Functionality to move space from one depot to another. The host Admin Console now provides a "Move..." button which can be used to move Spaces to a selected Depot. A new API function, movedepotspaces(), allows the same function to be performed via the API (HOSTSERVER-546). Client version 4.1.2 required to update the new space owner correctly.

14.2.3 3.5.1 (2015-10-09)

14.2.4 Documentation

- Fixed description of Background Tasks
- Added ssl configuration hint in case of upgrading a server to version 3.5
- Added description for the html templates for password protected published files

14.2.5 Host Server Functionality

- Usability: Added a default html template folder to avoid conflicts with customized html templates (HOSTSERVER-572)
- Administration: Fixed divide by zero error in case of depot size and traffic limit are zero (HOSTSERVER-570)
- Administration: German translation is disabled. Only english web interface is supported (HOSTSERVER-569)
- Administration: The new background task for API log cleanup will be created with status enabled instead of disabled. The usage could be controlled using the setting "APILogEntryTimeout" (HOSTSERVER-568)
- Usability: Added html template "url-invalid.html" for expired or invalid token in case of access a published file (HOSTSERVER-567)
- Security improvement: Limit access to allowed log files (HOSTSERVER-564)
- S3 daemon: Added bandwidth limitation for the S3 daemon (HOSTSERVER-563)
- Administration: Added filter (<, >, =) for Space-IDs and Depot-IDs (HOSTSERVER-562)

- Administration: Added setting "APILogEntryTimeout" to define a period in days for deleting api logs (HOSTSERVER-561)
- Administration: Fixed truncated "Add New Admin User"-Button (HOSTSERVER-560)
- Administration: Fixed access to ping.xml (HOSTSERVER-558)
- Administration: Fixed s3d.log file name for log file display (HOSTSERVER-557)
- S3 daemon: Fixed crash in case of multipart upload (HOSTSERVER-556)
- Administration: Fixed displaying info text for "TimeDiffTolerance" setting (HOSTSERVER-553)

14.2.6 3.5.0 (2015-09-21)

- Initial public release

CHAPTER

FIFTEEN

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.

15.1 Change Log - Version 3.0.013

15.1.1 3.0.013.16 (YYYY-MM-DD)

15.1.2 3.0.013.15 (2015-08-17)

- S3: Fixed bug with high IO, upload could not proceed and other uploads will be blocked. (HOSTSERVER-529)

15.1.3 3.0.013.14 (2015-06-04)

- S3: Fixed bug in parsing S3 access log entries for traffic calculation (resolves `Error getting spaceid` errors in `td-hostserver.log`). Additionally, the S3 log analyser script now only downloads and processes objects from the log bucket that contain the string `access_log-`. (HOSTSERVER-500)
- mod_pspace: Added support for calculating traffic from S3-compatible object stores that do not support access logging via log buckets in the way that Amazon S3 does it. Now, if a redirect to S3 is performed and `S3LogBucketName` has not been specified, the request length will be logged as bytes sent. (HOSTSERVER-499)
- s3d: The S3 daemon has now been split into two processes, a worker process and a watchdog process. If the worker process dies, the watchdog will restart it. Killing the watchdog process will also kill the worker process. The watchdog will always try to restart the worker, but depending on the frequency with which the worker is dying the watchdog will wait before trying to restart it. The minimum wait is 3 seconds, the maximum is 30 minutes. (HOSTSERVER-508)

15.1.4 3.0.013.13 (2015-05-11)

- mod_pspace/s3d: Added workaround to handle a deviation in the Ceph 0.8 Object Store S3 API: the "list multipart upload parts" API request returns `ListMultipartUploadResult` instead of `listpartsresult` (see BUG#11494 in the Ceph bug tracker for details). (HOSTSERVER-484)
- mod_pspace: Added missing call to `s3d_delete()` when an "Upload to file that has already been transfered to S3" is detected. Due to the missing call, Clients could end up in an endless loop, showing a "wrong md5" error in the log file. (TDCLIENT-2045)
- mod_pspace: Added new module option `watched_space_id` that can be used to trace Client accesses to a specific Space for debugging purposes. See tracing_client_accesses_to_a_single_space for details. (HOSTSERVER-486)

15.1.5 3.0.013.12 (2015-04-14)

- s3d: Uploading the `last.log` file failed with a checksum error if the log was written to before the upload was complete. `s3d` now only transfers the data size used when calculating the checksum. This will allow the `last.log` file to grow while being uploaded to S3. (HOSTSERVER-474)
- s3d: Fixed unsafe object references during multi-part uploads which may have lead to `s3d` crashes. (HOSTSERVER-454)

- Installation: The `td-hostserver` RPM package will no longer reset the permissions and ownerships of the `/spacedata` and `/spacedata/vol01` directories to `700` and `apache:apache` during an update, if they had been changed by the administrator after the initial installation. Depending on how the Space Volume is mounted, the RPM installation could fail with an error like `error: unpacking of archive failed on file /spacedata`. A new installation will still create the directories using these permissions/ownerships by default. (HOSTSERVER-401)
- Host Server: Converted the type of the `StatisticRest` setting from `INT` to `DATE`, to avoid an error that could occur when updating from very old Host Server Versions (the `resetTraffic()` auto task failed with an `Invalid integer literal` error). This also fixes a potential issue that could result in the reset routine being run multiple times on the day the traffic is reset. (HOSTSERVER-478)
- Documentation: Fixed link structure in the HTML documentation so that clicking **Next** and **Previous** within a document works as expected. (HOSTSERVER-471)

15.1.6 3.0.013.11 (2015-03-30)

- Administration Console: Updated logo and favicon.
- Host Server: Updated some error messages by replacing "Repository" with "Depot". Ensure that a Space Depot that has been marked as "Deleted" no longer allows the creation of new Spaces. (HOSTSERVER-456)
- mod_pspace: Reduced logging of errors by only logging Client accesses to deleted Spaces as an error if the Space status is zero. (HOSTSERVER-449)
- mod_pspace: Fixed a crashing bug that could occur in rare situations. (HOSTSERVER-457)
- s3d: Fix unsafe access to the thread pool that may have caused `s3d` to crash in certain situations. (HOSTSERVER-454)
- s3d: Fixed a problem that caused a crash if a multipart upload was interrupted before completion and then restarted again. The parts list could have holes in it for the parts that were successfully uploaded in the first try.
- Documentation: Added section that instructs the user to perform a `yum update` after installing the VM image. Reformatted the 3.0.013 release notes and replaced the table with regular sections for improved readability.
- Documentation: Added Failover and Scalability chapter to the Administration Guide, added description of the startup sequence/dependencies to the Installation Guides. (HOSTSERVER-431)

15.1.7 3.0.013.10 (2015-01-26)

- s3d: Fixed a problem that caused a crash from time to time. The crash would occur if a request for an object's header timed out or was interrupted.
- Host Server: Fixed bug in the calculation of `DiskUsed` for Space Volumes that did not contain any Spaces. (HOSTSERVER-452)
- Administration Console: The Volume repair button now only appears if a repair is actually required (previously it appeared whenever there was an error on the volume).
- Installation: added a new RPM package `td-hostserver-doc-html` that contains the Host Server documentation in HTML format, installed in the Host Server's Apache document root `/var/www/html/td-hostserver-doc/`. Access to the documentation can be restricted by editing `/etc/httpd/conf.d/td-hostserver-doc.httpd.conf`. (HOSTSERVER-450)
- Installation: fixed bug in upgrading from older versions and the `hostapilog` database did not get created. (HOSTSERVER-446)

15.1.8 3.0.013.9 (2015-01-14)

- mod_pspace/s3d: fixed `unexpected object "vol01/..." starting with 'vol' was found in the bucket...` error , which prevented the Apache module from starting. This error could occur after updating from a previous version if S3 was already enabled, and the old object format (prefixed by volume name) was used on an S3 compatible object store. (HOSTSERVER-447)

15.1.9 3.0.013.8 (2015-01-13)

- API: Added missing `activatedepot` API command and added new tag `<changeinfo>` to add a free form comment to the change history of the following API commands: `activatedepot`, `assignusertodepot`, `createdepotwithoutuser`, `deactivatedepot`, `deletedepot`. Updated API version to 3.0.004. (HOSTSERVER-337)
- Installation: fixed typo in the installation script that adds the RewriteRules to `ssl.conf`. Added RewriteRule in preparation for accepting Client requests for Space data via SSL/TLS (not supported yet).
- Installation: the binary tarball distribution now includes debug versions of the Host Server binaries (`s3d-debug` and `tshs-debug`) and Apache module (`mod_pspace-debug.so`, to better support analyzing possible crashing bugs. (HOSTSERVER-445)
- Installation: fixed possible upgrade error from previous versions: moving the MySQL table `pbpg.Keys` to the `pspace` database failed if an empty `pspace.Keys` table already existed. (HOSTSERVER-441)

15.1.10 3.0.013.7 (2014-12-12)

- Fixed error in creating an index during the initial MySQL table creation (HOSTSERVER-440)

15.1.11 3.0.013.6 (2014-12-09)

- Installation: fixed possible upgrade error from 3.0.011 when the MySQL database `pbpg` still existed, but the `Keys` table was already moved to the `pspace` database (HOSTSERVER-427)
- Fixed bug in which failed Auto Tasks were not executed anymore (HOSTSERVER-407)
- mod_pspace: 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 yvvad performed the required schema updates)
- mod_pspace: Fixed possible "Admin API: AES decode error- curruption 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 `S3Options` settings field from 200 to 2000 chars, to accommodate longer option strings required for certain OpenStack environments (HOSTSERVER-425)
- Installation: updated `RewriteRule` sets in the httpd configuration files (removed obsolete `/depot` rule, HOSTSERVER-424)

15.1.12 3.0.013.5 (2014-09-26)

- mod_pspace: 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.

15.1.13 3.0.013.4 (2014-09-18)

- 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)
- s3d: Fixed bug in path deletion on S3: if the path ended with '/' it wasn't being deleted.
- s3d: exceptions are now logged in `/var/log/s3d.log`

15.1.14 3.0.013.3 (2014-09-05)

- 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 `resetTraffic()` to properly reset the traffic for Spaces that had the `SPACE_TRAFFIC_FULL` status flag enabled. (HOSTSERVER-353)
- Installation: security enhancement: set `ServerTokens` to `Prod` and `ServerSignature` to `Off` in `httpd.conf` 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: `add-s3-host` 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 unneded HTTP methods in `td-hostserver.httpd.conf` (ony allow GET, POST, PUT, disable HEAD, OPTIONS, TRACE) (HOSTSERVER-361)
- Virtual appliance security enhancement: set `ServerTokens` to `Prod` and `ServerSignature` to `Off` in `httpd.conf` to disable displaying the Apache Server version and OS version in the HTTP headers and on error pages (HOSTSERVER-357)

15.1.15 3.0.013.2 (2014-07-14)

- To avoid confusion, the S3-related configuration option `openStackAuthURL` was renamed to `openStackAuthPath`

15.1.16 3.0.013.1 (2014-07-11)

- Initial public release

CHAPTER

SIXTEEN

RELEASE NOTES - VERSION 3.0.011 AND OLDER

Table 16.1: Release Notes - Version 3.0.011 and older

Build Date	Version	Comment
YYYY-MM-DD	3.0.011.6	• HOSTSERVER-228: Add settings for `ClientPollFrequency` and `StatisticPollFactor` • HOSTSERVER-241: Moved `[p1db]` 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	• 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	• 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	• Updated version number in `pbstab` from "4546" to "4547" • Fixed HOSTSERVER-172: The default MySQL table definition file `mysql/p1space_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 16.1 – continued from previous page

Build Date	Version	Comment
2014-02-07	3.0.011.2	• Updated sample `hosting.txt` file: no trailing slash after `REGSERVERURL` • Updated and completed Translation files (grammar, typos, obsolete terms) • Set `PathToSAKConverter` configuration variable to `/home/teamdrive/sakh/sakgen` by default • Added S3Daemon config and script files to the installation package • Fixes to object store access log processing
2014-02-04	3.0.011.1	• Added parsing and error handling for `API_IP_LIST` and `API_SALT` from the `hosting.txt`. • pbstab: changed log file from `/home/teamdrive/pbas/setup/pbac.log` to `/var/log/p1_autotask.log` (Jira-Issue HOSTSERVER-145) • `pbstab`: fixed wrong path to `p1ctl.dal` • Fixed setting space status bit • Fixed autotask debug output • Fixed typos and obsolete reference to p1ctl from the translation files • Changed configuration variable 340 “Protocol Log File” in `pbas.env` from “<< Default Log >>” to “/var/log/pbas.log” - note that this file needs to be created and assigned to the user running the PBAS instance (`touch /var/log/pbas.log ; chown teamdrive:teamdrive /var/log/pbas.log`) • Fixed HOSTSERVER-150: removed reference to td2apilog database
2014-01-28	3.0.011.0	• First build of the 3.0.011 branch, using the scripted build
2012-08-22	3.0.009	• Fixed traffic LastReset bug
2012-08-03	3.0.008	• MySQL plugin with new reconnect; Fixed MySQL result set handling

CHAPTER

SEVENTEEN

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 (`HostingServer-3.0.011.x.tar.gz`) and latest PBAS package (`PrimeBase_TD.4546.tar.gz`). 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