TASSTA

ENGLISH

Document revision: **2408.15-1221**

T.Lion 5.6

Preparing for Deployment

Last revised: August 15, 2024

This document is not warranted to be error-free. If you find any problems in the documentation, please report them to us in writing.

Due to ongoing product improvements and revisions, TASSTA GmbH cannot guarantee the accuracy of printed or soft material after the publishing nor can it accept responsibility for errors or omissions. Updates to this document and other documentation can be downloaded at TASSTA Documentation Center.

Contents

Overview

T.Lion is the central component of the TASSTA communications network. It manages users, provides communication between clients, records calls and activities, stores and processes geolocation information, calculates indoor positioning, handles lone worker protection, and provides many other services.

T.Lion suite includes a communication server, services that perform specific tasks (authentication, positioning, and the like), and Recorder Server that keeps the history of calls and messages.

T.Lion can be further extended with T.Brother – a backup communication server, which ensures an uninterrupted communication flow, even if the primary (T.Lion) server fails. T.Brother is an exact copy of the T.Lion; as such it should have the same hardware configuration.

TASSTA remotely installs, configures, and upgrades T.Lion and the related services on your on-premises hardware or in the cloud, so you do not have to worry about complicated technical details. All you need is to coordinate business details with TASSTA Sales, prepare the environment according to these instructions and grant access to our engineers.

Once T.Lion server is deployed, you can configure the communication network, deploy Android and iOS clients, and set up dispatcher workplaces.

This document provides detailed instructions on preparing your environment for deploying T.Lion.

Required hardware

- x86 or x64 processor; dual-core or better.
  A dedicated quad-core CPU with support for the Intel® AVX instruction set is required for correct operation of all modes of the Indoor Localization feature set (up to 600 users). Without this instruction set, some of the modes will be unavailable.

> NOTE:
>
> To verify that your CPU of choice supports the technology, use the Intel advanced search web page. Alternatively, to check the AVX support status of a running CPU, use the following command:
> `lscpu | grep avx`

- Gigabit Ethernet adapter.
- Free USB port (for dongle license).
- To improve performance, it is recommended to use a solid state drive (SSD) for T.Lion installation.

T.Lion

Number of users	CPU	RAM	Disk space
100	Intel® Core™ i7-6700 Quad-Core Skylake	8 GB	500 GB
500	Intel® Core™ i7-8700 Hexa-Core Coffee Lake	16 GB	1 TB
1000	Intel® Core™ i9-9900K Octa-Core	32 GB	2 TB
3000	Intel® Xeon® E-2176G Hexa-Core	64 GB	4 TB
5000	Intel® Xeon® E-2176G Hexa-Core	128 GB	10 TB

The actual hardware requirements may vary depending on product features and usage scenarios. The numbers above are only given for reference sake.

Arbitrator Server

This optional service monitors T.Lion server availability and automatically switches all communication flow to backup server (T.Brother) if the primary server experiences problems.

- Intel® Core™ i7-6700 Quad-Core Skylake or better CPU.
- At least 2 GB of RAM.
- Minimum of 120 MB hard disk space.

Operating system

T.Lion works on Debian GNU/Linux 9 "Stretch" (x86 or x64), Debian 10 "Buster" and Debian 12 "bookworm". The operating system is installed and configured by the customer.

> IMPORTANT:
>
> Installation under Debian 10 and Debian 12 requires additional configuration from TASSTA Support. When requesting a deployment, be sure to specify the target operating system.

Refer to **Debian Installation Guide** for detailed deployment instructions, along with downloadable files. Consider the following guidelines:

- Choose **Guided - use entire disk** partitioning method and **All files in one partition** (a single `/` partition with `var`, `tmp`, and `home` directories) partitioning scheme.
  Alternative partitioning may result in free space issues.
- Do not install a desktop environment. It consumes resources and can lead to server instability.
- Linux Kernel Security (SElinux or AppArmor) must be disabled or set to permissive mode.

> IMPORTANT:
>
> We do not recommend installing any feature updates (except for security patches) or additional software packages on T.Lion servers.
> Contact us to clarify the warranty terms and conditions.

Packages

- SSH server.
- Standard system utilities.
- BASH version 4 or later is recommended.

Time zone

All T.Lion / T.Brother servers should work in the same time zone and their time must be synchronized. Verify the configuration by executing `date` command:

```
$ date

Mon Jan 12 22:59:24 UTC 2020
```

To change the time zone, for example from UTC to Pacific time, run:

```
$ rm /etc/localtime
```

```
$ ln -sf /usr/share/zoneinfo/US/Pacific localtime
```

Configure NTP client for each host to avoid time drift. To immediately sync a server's time with a time server, run:

```
$ ntpdate -u [NTP server, e.g europe.pool.ntp.org]
```

Debian 10 and Debian 12 support

T.Lion can work on Debian 10 "Buster" and Debian 12 "bookworm". However, there are some specifics in deployment:

- TASSTA Services require Docker containers to run.
- Occasional issues may arise during deployment and operations still need to be addressed.

Before deploying, be sure to indicate that you want to install the system on Debian 10 or above, and be aware that additional time and effort will be required from the TASSTA Support team.

> IMPORTANT:
>
> Debian 10 and Debian 12 support is still undergoing extensive testing. To ensure maximum stability, use Debian 9 Long Term Support (LTS).

Network configuration

The following network-related settings are recommended for smooth and secure operation of T.Lion and the related services.

Firewall and security groups

Make sure all servers and the database/cluster are properly secured. It is recommended that you isolate the infrastructure from the Internet and whitelist only known hosts or networks.

Due to the way network sockets work, when a client connects to a server, the operating system allocates a port number at random. In some situations, a firewall on the client side may disallow outgoing connections on the resulting port number. TASSTA software has no knowledge about the sockets which clients connect from, so if you need to prevent port blocking, you should adjust your firewall rules to ensure access to the ports listed in this topic.

Configure your firewall so that instead of blocking traffic based on port number on the client side, all traffic should be blocked on on the server on all ports that are not required by TASSTA software.

Connections to allow on the server

Open the following ports on a firewall:

Port	Protocol	Direction	Use
20	TCP/UDP	Outgoing	File Transfer Protocol (FTP) data transfer
21	TCP/UDP	Outgoing	File Transfer Protocol (FTP) control (command)
22	TCP/UDP	Incoming	Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding
80	TCP/UDP	Outgoing	Hypertext Transfer Protocol (HTTP)
443	TCP/UDP	Outgoing	Hypertext Transfer Protocol Secure (HTTPS)

Stand-alone servers

Port	Protocol	Purpose	Alternative port	Security	Notes
22	TCP	SSH Console	Can be changed with Linux CLI	Trusted hosts/networks only	
80	TCP	Local Map tile server	Not supported	Unrestricted	In case of using local Map tile server
3306	TCP	MySQL	Not supported	No external connections	
4000	TCP	TASSTA Proxy	Not supported	Unrestricted	
4321	TCP	T.Commander	Can be reassigned		
8082	TCP	T.Recorder	Not supported	Unrestricted	T.Recorder client connections
60xxx	UDP/TCP	Recorder server	Not supported	Unrestricted	Unencrypted connection between T.Lion and Recorder server version 3.001 and newer. xxx depends on the server ID.
65xxx	UDP/TCP	T.Lion	Can be reassigned	Unrestricted	xxx depends on the server ID

NOTE:

Port 65xxx and the matching 60xxx are opened for each server on T.Lion node. Last 3 digits are equal to the server ID.

Additional ports for T.Mugen client

Allow inbound connections to the following ports in addition to standard T.Lion server ports:

Port	Protocol	Use
3036	TCP	TL Proxy service
5349	TCP/UDP	Interactive Connectivity Establishment (ICE) server
3478	UDP	TURN/STUN server
49152 to 65535	UDP	TURN relay media

HTTP and HTTPS traffic must also be allowed. If you prefer default ports for accessing T.Mugen web interface:

Port	Protocol	Use
80	TCP/UDP	Hypertext Transfer Protocol (HTTP)
443	TCP/UDP	Hypertext Transfer Protocol Secure (HTTPS)

Additional ports for high-availability cluster

Port	Protocol	Purpose	Alternative port	Security	Notes
4444	TCP	Cluster SST	Not supported	Source, destination firewall defined	Port for all other State Snapshot Transfer. Should be opened on T.Lion and T.Brother servers.
4567	UDP/TCP	Cluster	Not supported	Source, destination firewall defined, SSL	Reserved for Database Cluster replication traffic. Multicast replication uses both TCP and UDP transport on this port. Should be opened on T.Lion and T.Brother servers.

Port	Protocol	Purpose	Alternative port	Security	Notes
4568	TCP	Cluster IST	Not supported	Source, destination firewall defined	Port for Incremental State Transfer. Should be opened on T.Lion and T.Brother servers.
13000	TCP	Cluster Arbitrator	Can be reassigned	Source, destination firewall defined	Should be opened on Arbitrator server.
27017	TCP	Mongo Database replication	Not supported	Should be opened on T.Lion and T.Brother servers.	
n/a	IP protocol 112 (VRRP)	Virtual Router Redundancy Protocol	Not supported	Source, destination firewall defined	The Unicast Virtual Router Redundancy Protocol (VRRP) provides a way for multiple hosts to communicate so that one of them at a time can hold a virtual IP address. Should be opened on T.Lion and T.Brother servers.

TASSTA Central Licensing Server (RMP)

Domain or IP address	Port
central.tassta.com	55555
116.203.164.16	55555
central1.tassta.com	55555
167.233.13.223	55555

Host names

Consider giving your servers informative names:

- `tls1234` for T.Lion Server.
- `tbs1234` for T.Brother Server.
- `arb1234` for Arbitrator Server.
- `trs1234` for Recorder Server (in case of standalone deployment).

Where `1234` is the license/dongle ID.

Supported cloud platforms

T.Lion can be deployed on almost any cloud platform. The following cloud providers have been tested:

- Amazon Web Services (with Elastic IP for high availability cluster)
- Microsoft Azure
- Hetzner Online (natively supports floating IP for high availability cluster)
- OVH
- Alibaba Cloud
- Telefónica Cloud (natively supports floating IP for high availability cluster)
- Private Virtual Data Centers based on VMware Platform (natively supports floating IP for high availability cluster)

T.Lion is deployed on the cloud instance with the hardware configuration and operating system described in the corresponding topics. The instance is created and pre-configured by the client.

High-availability deployment (T.Lion with T.Brother) requires a floating IP address. The configuration depends on the specific platform.

Configuring Amazon Web Services

Collect the following information before initiating deployment of T.Lion/T.Brother on AWS EC2:

- Elastic IP ID (*eipalloc-dbxxxx*).
- Elastic IP address. This address will serve as a single point of contact for a high-availability cluster.
- Master node (*i-xxxxxxccc*).
- Master node private IP address.
- Shadow node (*i-yyyyyyyyyy*).
- Shadow node private IP address.
- Availability zone, for example *eu-west-2*.
- AWS API username.
- AWS API access key.

AWS user should be created and the appropriate access policies applied:

- Log in to your AWS account
- Open Identity and Access Management: https://console.aws.amazon.com/iam/home#/home
- Create a group: https://console.aws.amazon.com/iam/home#/groups
- Create a user, assign it to the group, and get a key: https://console.aws.amazon.com/iam/home#/users

> NOTE:

> The above-mentioned links to AWS Console will only work if you are signed in to AWS.

Public server DNS should be bound to Elastic IP. Refer to AWS documentation for more information: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html

Recorder Server

This service records audio/video calls and messages and provides access to recordings for TASSTA clients: (T.Flex, T.Rodon, T.Recorder). Additionally, Recorder Server exposes a public API for accessing and managing recordings.

Due to the large amount of storage space required for media data, TASSTA offers 2 deployment scenarios for Recorder Server:

- Recorder Server is installed on the same machine where T.Lion is installed (default).
- Recorder Server is installed on a dedicated server.

Integrated deployment

By default, Recorder Server is deployed on the same machine where T.Lion is installed. In addition to standard T.Lion prerequisites, make sure the machine meets the following requirements:

- Intel® Core™ i7-6700 Quad-Core Skylake or better CPU.
- At least 4 GB of RAM.
- Minimum of 1 TB free disk space for storing recorded audio and video. It is highly recommended to use a solid state drive (SSD) for better performance.

Standalone deployment

Unlike other TASSTA services, Recorder Server can be deployed on a dedicated computer. This reduces the load on {VAR (lion)} server and significantly lowers its storage space requirements.

If you choose to deploy Recorder Server as a standalone machine:

1. Coordinate the deployment scenario with TASSTA service team.
2. Prepare a computer or a cloud instance that meets the following requirements:
    - Intel® Core™ i7-6700 Quad-Core Skylake or better CPU.
    - At least 4 GB of RAM.
    - Minimum of 1 TB hard disk space. It is highly recommended to use a solid state drive (SSD) for better performance.
    - Gigabit Ethernet adapter.
3. Deploy and configure Debian (x86 or x64) on the computer / cloud instance.

Refer to **Debian GNU/Linux Installation Guide** for detailed deployment instructions and distributives. Consider the following guidelines:

- Choose **Guided - use entire disk** partitioning method and **All files in one partition** (a single `/` partition with `var`, `tmp`, and `home` directories) partitioning scheme. Alternative partitioning may result in free space issues.
- Do not install a desktop environment.

4. Install the following packages:
   - SSH server.
   - Standard system utilities.
   - BASH version 4 or later is recommended.
5. Synchronize the time zone with T.Lion machine. You can verify the current configuration by executing `date` command. To change the time zone, for example from UTC to Pacific time, use the following commands:

   ```
   $ rm /etc/localtime
   $ ln -sf /usr/share/zoneinfo/US/Pacific localtime
   ```

   NOTE: Configure NTP client to avoid time drift. To immediately sync with a time server, run `$ ntpdate -u [NTP server in the same geographic region as your machine]`.

6. Once the environment if fully set up, grant access to the server / cloud instance for TASSTA engineers.

Granting access to TASSTA engineers

Once the environment if fully set up, grant access to the servers / cloud instances for TASSTA engineers:

- Provide a direct SSH access to the servers where T.Lion and the related services will be deployed. If that is not possible due to security or technical reasons, we would require additional time for alternative access routines (such as on-site professional services). Contact TASSTA sales to request a price quote.
  TIP: To improve the security, restrict access to SSH port for the dedicated IP address of TASSTA engineering team. Contact us to get more details.
- Grant TASSTA engineers root access to the servers on which deployment will be done. If necessary, it can be revoked once the deployment is complete.

Upgrade procedures require the same access level.

TASSTA

All-in.

+49 30 57710674
hello@tassta.com
tassta.com

tasstaworld
t-a-s-s-t-a
TASSTAGmbHHannover
tassta_now
tassta_gmbh