TASSTA

ENGLISH

Document revision: **2407.01-1905**

T.Lion

Best Practices

Last revised: July 1, 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

Best practices 4
Network segmentation and capacity planning 4
Isolate teams on a single server 4
Limit the number of users per channel 5
Limit the number of users per server 5
Limit the number of users per node 5
Restarting servers 6
Mitigating DoS attacks 6
What you will need 6
Checking the network load 6
Finding out IP addresses connected to your server 7
Blocking the attacker address 7

Best practices

This document provides basic recommendations and outlines usage scenarios to improve your experience with TASSTA communications solution and increase system stability and reliability.

Network segmentation and capacity planning

To ensure smooth and efficient operations of the TASSTA communication platform, maintaining an optimal distribution of users across servers is crucial. While the maximum number of concurrent online users and active communications has the most significant impact on performance, the total number of users, including those offline, also plays a very important role.

- Server management will become too complicated.
- Restarting the server (for example, after adding a channel) will affect too many users at once.
- The amount of data transmitted to each client increases as the number of users grows. This can lead to significant increases in overall server traffic, impacting service communication performance and costs, especially on mobile networks.
- Rules and policies may become too complicated.
- End-users will have to look for colleagues in a long list of users wasting the valuable time.
- When the "Hide offline users" setting is disabled on a server with a large number of users, it can become difficult to find and interact with the specific users you need. This can lead to confusion when trying to communicate via PTT, send messages, make direct calls, and the like.
- Displaying the last known positions of offline users on the map can significantly increase data traffic and slow down map rendering performance.
- Certain operations such as making snapshots of server state and restoring from snapshots will take longer.
- Backups will require significantly more storage space.

While the actual limits will vary depending on your hardware, network speed, and usage patterns, consider these recommendations when segmenting your users:

Isolate teams on a single server

Access policies (rules) are very flexible and powerful instruments for limiting access to channels and establishing a segregation of duties. They control all aspects of channel access, user behavior, and membership. By limiting the list of channels available for individual teams, you can eliminate the interference between users while keeping the ability to coordinate common operations through a central dispatcher. For example, you can:

- Isolate internal communication of geographically distributed fire brigades, but handle all distress calls from a single dispatch center.

- Ensure clear coordination and safety at the construction site by providing a dedicated communication channel for each team, with the ability to broadcast emergency messages to every worker from the dispatcher console.
- Prevent volunteers from accessing internal police channels.

See T.Commander Administrator's Guide for technical details and practical examples of configuring isolated teams.

Limit the number of users per channel

The recommended number of users per channel should not exceed 200.

> NOTE:
>
> When the user logs in to the system, it is added to the *Main* channel by default.

If you need more users to communicate with each other on the ad hoc basis, you can use dynamic groups or use multi listening feature.

Limit the number of users per server

T.Commander allows for using more than one server on a single T.Lion node. Try to divide your users into functional groups that perform completely different tasks and do not need to communicate with each other directly. Such groups can be kept on different servers with unique settings.

The recommended number of users per server (both online and offline) should not exceed 1,000.

For example, consider creating dedicated servers for each district. This way, you can group ambulance brigades by location on their respective servers, improving overall performance and efficiency.

This segmentation will not hinder the intercommunication when needed. Cross-server communication feature will allow the dispatchers to easily join the channels from different server into a single communication unit.

Limit the number of users per node

In large, geographically dispersed deployments, consider deploying multiple T.Lion nodes, each managing several servers. This strategic placement distributes processing power and optimizes network traffic by locating nodes closer to your users. This can significantly improve overall performance and responsiveness for your users.

The recommended number of users per node (both online and offline) should not exceed 5,000.

Even if channels and users reside on different nodes, the transparent ad-hoc communication is still possible. Cross-server communication feature will allow the dispatchers to easily join the channels from different nodes and servers into a single communication unit.

Restarting servers

When the server is restarted, all clients and dispatcher consoles are disconnected from it. It will temporary stop ongoing voice and video communication for all users on the server.

Typically, the restart only takes a few seconds and all active users are automatically reconnected to it. However, the more users you have on the server, the longer it takes to restart and reconnect.

It is recommended to follow the best practices:

- Only restart the server during non-working hours.
- Use multiple servers to isolate users into smaller teams.

Mitigating DoS attacks

Denial of service (DoS) is a very common type of attacks that can render a server inaccessible or severely limit the connectivity until the issue is mitigated. Typical DoS attack is performed by flooding the target server with traffic from a single IP address. Though it rarely results in the theft or data loss, this attack can result in mobile clients and dispatchers being unable to communicate with each other.

This topic describes a basic DoS attack detection and mitigation scenario. The commands below must be run on the server where T.Lion and related services are deployed.

> IMPORTANT:
>
> You will need root privileges on the server.

What you will need

To find out what IP addresses are currently connected to your T.Lion server, use **netstat** tool, which is a part of **net-tools** utilities package. To install **netstat** on Debian 9, issue the following command:

```
sudo apt install net-tools
```

To check the network traffic and bandwidth usage, use **nload** utility. To install **nload** on Debian 9, issue the following command:

```
sudo apt install nload
```

Checking the network load

Simply run `nload` command. You should see details on incoming and outgoing network load. You you find out unexpectedly high incoming load, you might be under attack.

Finding out IP addresses connected to your server

Use netstat tool:

```
netstat -ntu|awk '{print $5}'|cut -d: -f1 -s|sort|uniq -c|sort -nk1 -r
```

The output of this command will list each IP address connected to the server and the number of instances from each address. If you see an IP address with an extremely large number of instances, the chances are pretty high that the address is your culprit.

Blocking the attacker address

If you suspect that the IP address found in the previous step belongs to an attacker, ban it with the following command:

```
sudo route add <IP address> reject
```

Then re-check network load and connected IP addresses. If the attack is mitigated, it is recommended to permanently block this IP address on the firewall.

TASSTA

All-in.

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

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