



Intel® Education Theft Deterrent server Load Balance Deployment Guide

July 2016

Legal Notices

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright © 2011 Intel Corporation.

* Third party names and brands may be claimed as the property of others.

Table of Contents

1.	Introduction	1
1.1	Document purpose and scope	1
1.2	Terminology	1
1.2.1	Abbreviations	1
1.2.2	Terms	1
1.3	Revision History	1
1.4	Reference Document	2
2.	Theft Deterrent server Load Balance Overview	3
2.1	Nginx Servers	4
2.2	TD Web Servers	4
2.3	TD Database server	4
2.4	Database Gate Servers	5
2.5	Database Cache Servers	5
2.6	Monitor server	5
2.7	How High Available works?	5
3.	Deployment Workflow	7
3.1	Deployment Procedure	7
3.2	Deployment Preparation	7
3.3	Typical Deploy Scenario for 1M Active Devices	8
3.4	Typical Deploy Scenario for 3M Active Devices	10
4.	Basic Infrastructure's Installation	13
4.1	Database Part Deployment	13
4.1.1	Install TD Database servers	13
4.1.2	Install PGGate servers	15
4.1.3	Configure Master PGGate server	16
4.1.4	Configure Slave PGGate server	16
4.1.5	Configure TD Database server	16
4.1.6	Append TD Database server and PGGate server	17
4.1.7	Install Database Cache server	17
4.2	TD webserver and Nginx Deployment	18
4.2.1	First Node Setup	18
4.2.2	Install TD Webserver Other Node	20
4.2.3	Configure TD Webserver Role	22
4.2.4	Configure Database Cache server	23
4.2.5	Install and Configure Nginx server	24
4.2.6	Append/Remove TD Webserver	25
4.3	Server Webpage Configuration	25
5.	Monitor Server Setup and Monitor	27
5.1	Install Monitor server	27
5.2	Regular Monitor	27
5.2.1	Adjust Database server	27
5.2.2	Adjust TD web server	27
5.2.3	Adjust TD Nginx server	27

1. Introduction

1.1 Document purpose and scope

This document introduces the procedures on how to deploy Intel® Education Theft Deterrent server load balance solution for based on TDserver 4.7.3x.x.

The document contains the following information:

- Introduction to the Theft Deterrent server load balance
- Load Balance Architecture
- Load Balance Deployment Procedure
- Installation Steps
- Monitor and Infrastructure's Adjustment

1.2 Terminology

1.2.1 Abbreviations

<i>Abbreviation</i>	<i>Description</i>
server	Theft Deterrent server
client	Theft Deterrent client

1.2.2 Terms

<i>Term</i>	<i>Description</i>
device	Intel® classmate PC or Intel® Education Tablet
online devices	The devices that are connected with the server network and their clients are activated and communicating with the server.

1.3 Revision History

<i>Revision</i>	<i>Date</i>	<i>Comment</i>
0.6	2015/12	First version for Q4'15 Load Balance Phase I
0.7	2016/06	Update for for Q2'16 Load Balance Phase II

1.4 Reference Document

<i>Document</i>	<i>Date</i>
Intel® Education Theft Deterrent server Deployment Guide	2016-06
Intel Education Theft Deterrent server Monitor Deployment Guide	2015-12

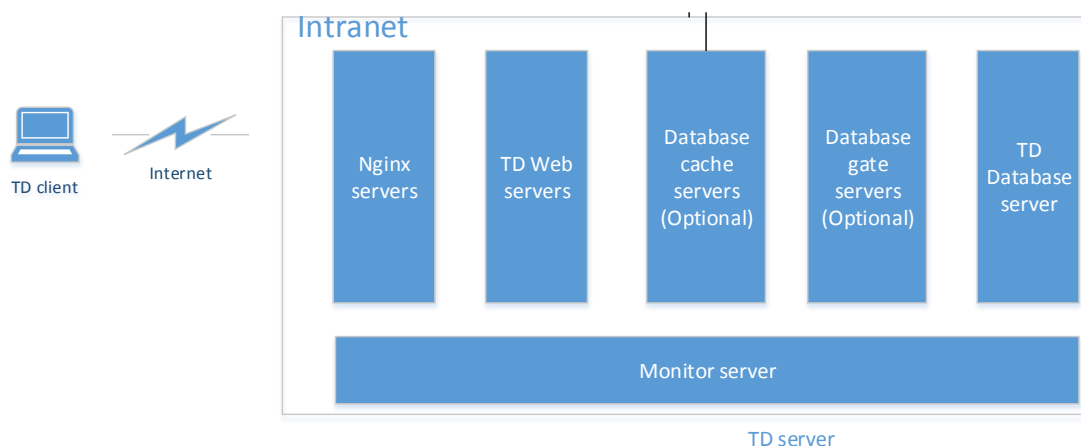
2. Theft Deterrent server Load Balance Overview

As part of the Intel® Education Software suite, Theft Deterrent provides a complete physical security management solution for your Intel® Education Tablet and Intel® classmate PC devices.

In general, it is recommend deploy the TD server in cloud for central management of the devices. As the increasing of client devices volume, several TD servers may be required to extend the client volume for one TD server's design target is support up to 200K devices. While several parallel, external accessible TD server requires more management effort, like different server's URL, different database, different servers to access the device's information, how to extend the server with more client required added etc.

Load balance is a solution for distributing incoming web request traffic through different roles of servers. It is a common technology used for any website with huge customers or data. The architecture is easily to extend, more stable and has better management capability.

For TD server, the high level load balance architecture will like below:



- TD client connect to the TD servers with one or several entries through the Internet
- TD server load balance solution has several components
 - Nginx servers
 - TD Web servers
 - TD Database server
 - Database gate servers (Optional)
 - Database cache servers (Optional)
 - Monitor server

Below is detail description for each of the components

2.1 Nginx Servers

NGINX is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server. NGINX is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption.

For TD, Nginx server act as entry server: TD client sends request to one Nginx server, and Nginx server select one TD web server from the backend server pool, and forward the request to the server, and forward its response to TD client afterward.

For one deployment, main need several Nginx servers according to the client quantity, and we suggest:

1. Only one domain name. All Nginx servers share the domain name.
2. Each Nginx server has its public IP address and private IP address.
3. The domain name and all public IP address can be pre-set in the client side. (Refer to detail description on how to configure the address)

Note: You can choose other load balance solution, such as some hardware based load balance solution to replace Nginx solution.

2.2 TD Web Servers

TD web server is used for is used for process the request sent from TD client. User can login to the webpage to manage the device. There should have several TD Web servers for one deployment and each server has its private IP address used to connect to Nginx and other servers.

There are 3 kinds of TD web server:

1. Load Balance Manage Node:
 - a. Only one manage node in one deployment.
 - b. It will run some activities background, like backup, setting up search keywords etc.
 - c. It will support all operations in the webpage.
2. Load Balance Manage-backup Node
 - a. It is Optional and can have one or several mange-backup node.
 - b. It will run some background activities, just like manage server did. When manage node is crashed, it will switch to manage node automatically.
 - c. It has limited function in the Setting webpage.
3. Load Balance General Node
 - a. There will have one or several general nodes in one deployment.
 - b. It will not run the background activities and it both manage and mange-backup node are down, it will switch to manage node automatically after several minutes.
 - c. It has limited functions in the Setting webpage.

2.3 TD Database server

One TD database server is required for a deployment. If customer want to have database hot-standby and auto fail over feature, then he need setup several TD database server with database gate server. If master database server is down, the database gate server will switch one slave server to master server.

All the database servers should located in the same subnet.

2.4 Database Gate Servers

The Database gate server is an optional component and it is required if want to have the database hot-standby and automatically fail over feature. Gate server are installed in the database server. Each database server install a gate server. Otherwise, we suggest customer regularly backup the database and have a separately hardware machine to save the backup file.

Each database server has different IP address, and web servers use a shared IP address as database server. Gate server will check whether its database server can act as master server, and add the shared database IP address if act as master server. So the master database server will have two IP addresses.

2.5 Database Cache Servers

The Database cache server is an optional component and it is required when want to enlarge the scalability. Redis is selected as the Cache Server solution for TD.

Currently one cache server can support 5M devices.

2.6 Monitor server

The monitor server is a separated machine to monitor the TD load-balance components. Monitor server can monitor the CPU usage, memory usage, hard disk usage, network throughput, HTTP/HTTPS connections, how many requests etc. According the monitor result, you can detect whether server has down or network is disconnect, and make the decision of add more servers or adjust the server hardware configuration.

In one deployment, it is required to setup the monitor server in the same IDC, and it is better add a remote monitor server in other city through check the internet connection with the Nginx server.

2.7 How High Available works?

In the whole system, one single node's problem will not cause total system down because once any single node is down, the system will switch to another similar node automatically.

1. TD client support several TDserver address and will try next address if previous one meet connection error. So we suggest the TDserver address pre-set in TDclient can include a domain name and several public IP addresses of the Nginx, so even DNS request failed or one Nginx server is down, the TD client still can access the infrastructure with the other Nginx server's Public IP address.
2. For TD Webserver, if one Webserver is down, Nginx server will forward the request to other web servers then automatically; if the Webserver is recovered, Nginx server will forward to this server automatically. And even if several TD Webserver are down, and make the alive TD Webserver receive large requests, the TD Webserver will simple return 'server busy' and keep the server will not crash because of huge overload.
3. For PGGate server, if master PGGate server is down, then the slave PGGate server will detect it and switch itself to master PGGate server automatically.
4. For Cache server, if cache server is down, then the web server still connect to database server. But the performance will drop. If the cache server up after a while, the web server can still use cache server.

5. For Database server, the several Database servers will synchronization automatically under the control of PGGate server. If master Database server is down, then the PGGate will detect it and switch slave database server master database server automatically.

3. Deployment Workflow

3.1 Deployment Procedure

The general deployment workflow is split several phases:

1. Preparation. Calculate how many servers are needed, prepare hardware, OS and network for external and internal etc.
2. Deployment. Deployment the basic infrastructure of TD servers.
3. Self-test. After deployment, use several TD client to do self-test at first.
4. Producing. If self-test passed, then allow all TD clients connect to TD server.
5. Monitor. Continuous monitor the system.
6. Adjust deployment. According the monitor result, add or remove TD servers, adjust the hardware configuration or TD server setting.

3.2 Deployment Preparation

1. A rough estimation on how many servers are needed.
 - a. Understand the total volume of the TDclient.
 - b. If there has TD system deployed, you can refer to the current system's performance to calculate how many servers required. For example, if current system can support total number of 250K device with one TDserver, then can use this number to estimate the machine number.
 - c. While the total 'active TD clients' is hard to calculate, especial for a pure new deployment. And it is also hard to deploy a large scale system in a short time. So we suggest can deploy a basic infrastructure with 2 servers for each components at first, then add new servers with TD clients increasing.
2. Hardware Preparation.

It is recommend using virtual machine system instead of a hardware server. Because its hardware configuration is easier to be modified. In general, one TD Nginx server and one TD web server with 8CPU and 16G memory can support about 400K active TD clients.
3. OS Preparation.

Currently the TD load balance solution can only support Linux with Debian/Ubuntu 64 bits platform.
4. Networking Preparation.
 - Public IP: Each Nginx server requires a public IP address.
 - Public IP or NAT: Each server need connect to internet require Public IP or NAT.
 - Domain name: One infrastructure need one domain name. The domain name and Nginx Public IP addresses can be pre-set in the client image and configured to Server Settings, so that will be applied to the client automatically if client support remote address setting feature.
 - Private IP: Each server need a private IP address for the whole infrascture are located in intranet. Nginx and TD web servers must be located in one class subnet with less than 256 IPs, such as 10.1.1.x or 172.16.1.x or 192.168.1.x.
 - Network bandwidth in the DMZ zone: 1Gbps is preferred.

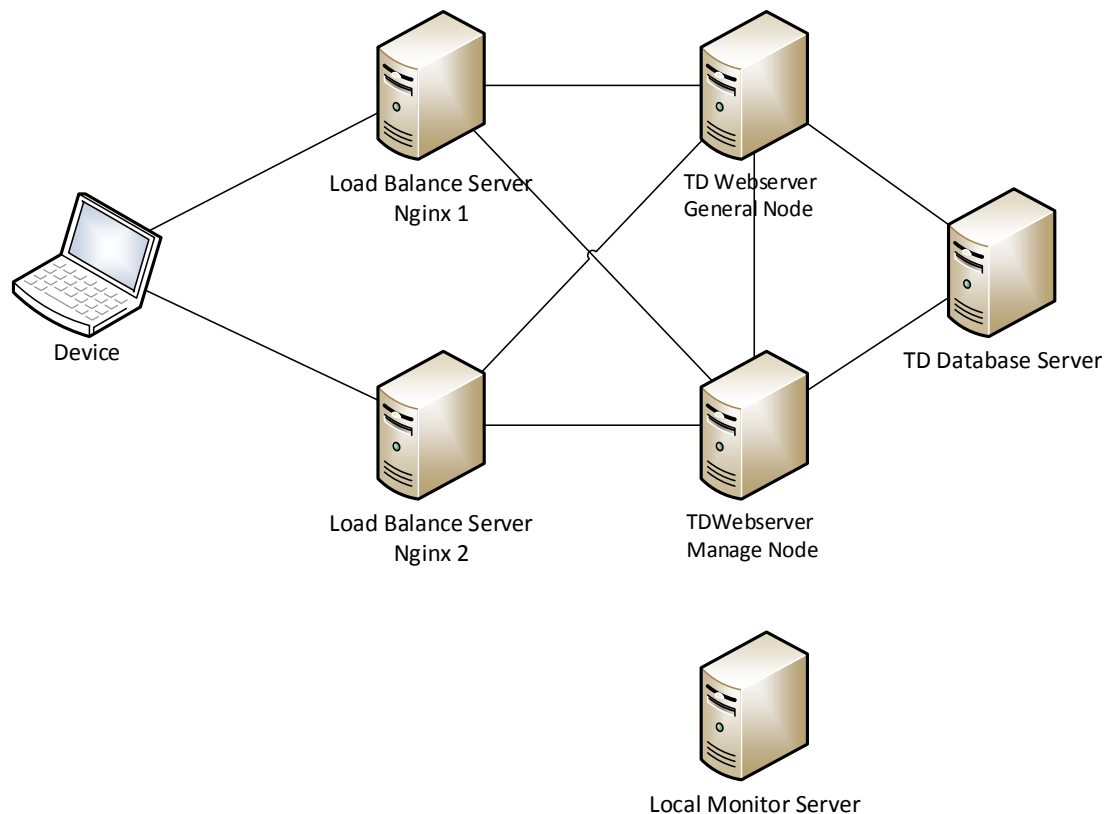
- Network bandwidth of internet connection: refer to network bandwidth suggest in 'Theft Deterrent Deployment Guide'. And it is recommend to monitor network bandwidth and adjust the network bandwidth according to real situation.

5. System Time synchronization

All the servers should keep the system time synchronization. It is recommended to use NTP to synchronize the server time.

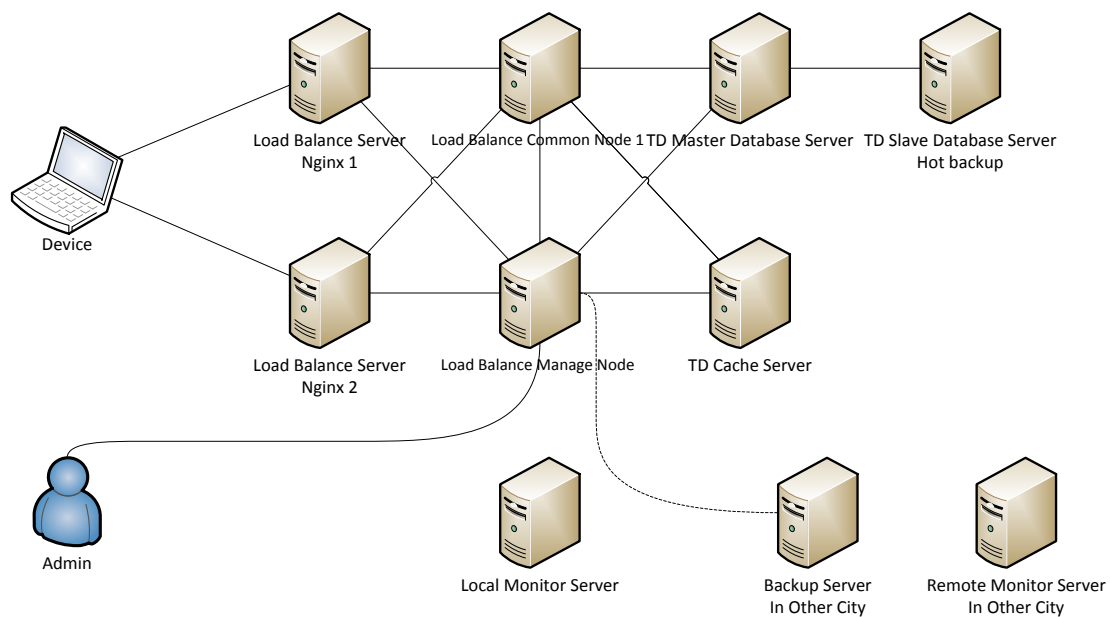
3.3 Typical Deploy Scenario for 1M Active Devices

The basic deployment infrastructure:



Below is a more complex deployment infrastructure with the following feature added:

1. Support database hot-standby with PGGate.
2. Support cache server.
3. Support directly login to manage node from internet with its Public IP address.
4. Support monitor Nginx internet connection.
5. Support remote backup in other city and it can be used for recovery in case of disaster happened for the infrascture.



Server list and its suggested configuration:

	Public IP	Private IP	CPU cores	Memory
TD_Nginx1	50.1.1.2	192.168.1.2	10	2G
TD_Nginx2	50.1.1.3	192.168.1.3	10	2G
TD_Webserver1 (Manage Node)	50.1.1.4*	192.168.1.4	8	16G
TD_Webserver2 (Command Node 1)		192.168.1.5	8	16G
TD_Cache server		192.168.1.6	2	6G
TD_Database server1 (Master)		192.168.1.7 192.168.1.100 (Database IP)	12	8G
TD_Database server2 (Hot backup)		192.168.1.8	12	8G
TD_Monitor1		192.168.1.9	2	2G
TD_Backup1 (Backup in other city)	50.2.2.2	172.16.1.2	2	2G
TD_Monitor_Remote (Monitor in other city)		172.16.1.3	2	2G

* **Note:** The TDwebserver manage node can also use port map or NAT, instead of Public IP so the backup server can access TDwebserver manage node through SSH port, copying the regular backup file from the manage node's hard disk out.

Firewall rule:

Allow TD clients connect the HTTP and HTTPS port:

```
ALLOW 0.0.0.0 CONNECT TCP 50.1.1.2:80
```

```
ALLOW 0.0.0.0 CONNECT TCP 50.1.1.2:443
```

```
ALLOW 0.0.0.0 CONNECT TCP 50.1.1.3:80
```

```
ALLOW 0.0.0.0 CONNECT TCP 50.1.1.3:443
```

Optional, allow admin connect the HTTP and HTTPS port of the manage node:

```
ALLOW x.x.x.x CONNECT TCP 50.1.1.4:80
```

```
ALLOW x.x.x.x CONNECT TCP 50.1.1.4:443
```

Replace the x.x.x.x with the public IP address of admin.

Optional, allow the backup server use SCP to copy the backup file from manage node.

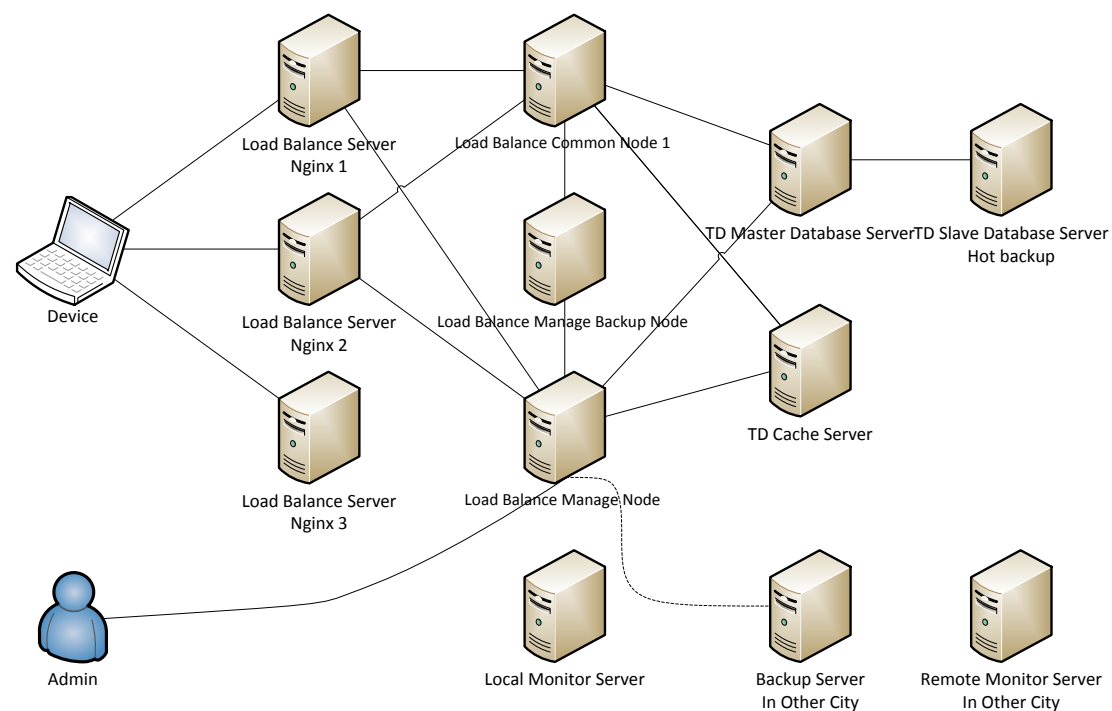
Or set port map or NAT, let the manage node SSH port can be access from backup server.

```
ALLOW 50.2.2.2 CONNECT TCP 50.1.1.4:22
```

DNS setting:

td.xxx.com 50.1.1.2, 50.1.1.3

3.4 Typical Deploy Scenario for 3M Active Devices



Server list and its suggested configuration:

	<i>Public IP</i>	<i>Private IP</i>	<i>CPU cores</i>	<i>Memory</i>
TD_Nginx1	50.1.1.2	192.168.1.2	10	2G
TD_Nginx2	50.1.1.3	192.168.1.3	10	2G
TD_Nginx3	50.1.1.4	192.168.1.4	10	2G
TD_Webserver1 (Manage Node)	50.1.1.5*	192.168.1.5	8	16G
TD_Webserver2 (Manage Backup Node)		192.168.1.6	8	16G
TD_Webserver3 (Command Node 1)		192.168.1.7	8	16G
TD_Cache server		192.168.1.8	2	6G
TD_Database server1 (Master)		192.168.1.9 192.168.1.100 (Database IP)	12	8G
TD_Database server2 (Hot backup)		192.168.1.10	12	8G
TD_Monitor1		192.168.1.11	2	2G
TD_Backup1 (Backup in other city)	50.2.2.2	172.16.1.2	2	2G
TD_Monitor_Remote (Monitor in other city)		172.16.1.3	2	2G

* **Note:** The TDwebserver manage node can also use port map or NAT, instead of Public IP so the backup server can access TDwebserver manage node through SSH port, coping the regular backup file from the manage node's hard disk out.

Firewall rule:

Allow TD clients connect the HTTP and HTTPS port:

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.2:80

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.2:443

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.3:80

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.3:443

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.4:80

ALLOW 0.0.0.0 CONNECT TCP 50.1.1.4:443

Optional, allow admin connect the HTTP and HTTPS port of the manage node:

ALLOW x.x.x.x CONNECT TCP 50.1.1.5:80

ALLOW x.x.x.x CONNECT TCP 50.1.1.5:443

Replace the x.x.x.x with the public IP address of admin.

Optional, allow the backup server use SCP to copy the backup file from manage node.

Or set port map or NAT, let the manage node SSH port can be access from backup server.

ALLOW 50.2.2.2 CONNECT TCP 50.1.1.5:22

DNS setting:

td.xxx.com 50.1.1.2, 50.1.1.3, 50.1.1.4

4. Basic Infrastructure's Installation

The overall installation step for setup the basic infrastructure are:

Database components: If you want have database hot-standby feature, install the TD database server and Database Gate server, configure the hot-standby. If do not want have database hot-standby feature, just install the TD database server directly.

To get better performance and support larger scale of devices (For Load Balance Phase II):

1. Database and PGGate server need be installed in same image.
2. Database cache server need be installed and configured

Webserver and Nginx components: Install TD Webserver nodes, Install Nginx server for load balance and configure these servers

Note: only Linux 64bits is supported for all kinds of servers. Debian 8 64 bits is suggested OS for all these servers.

4.1 Database Part Deployment

4.1.1 Install TD Database servers

1. Install 2+ Linux server, get the IP address for this server
2. Change to root account and input password when needed:

```
su -
```

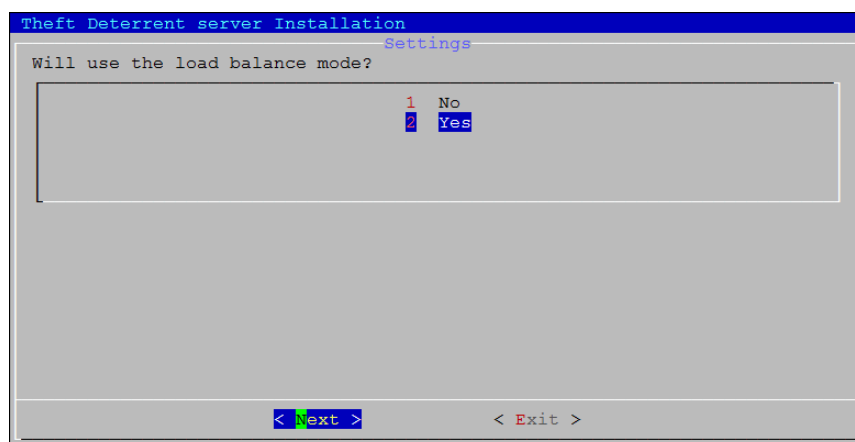
3. Change the file permission of the installation package:

```
chmod +x Theft_Deterrent_server_v4.x.3010X.[version]
```

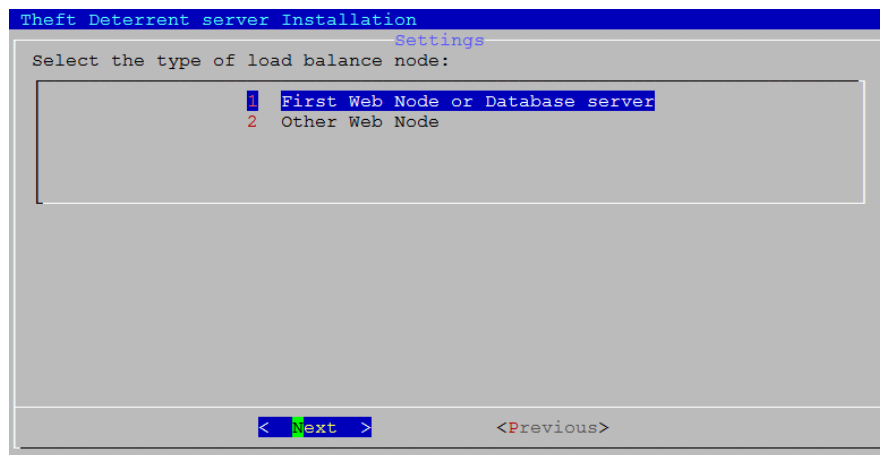
4. Run the installation package to open the install wizard:

```
./Theft_Deterrent_server_v4.x.3010X.[version] install
```

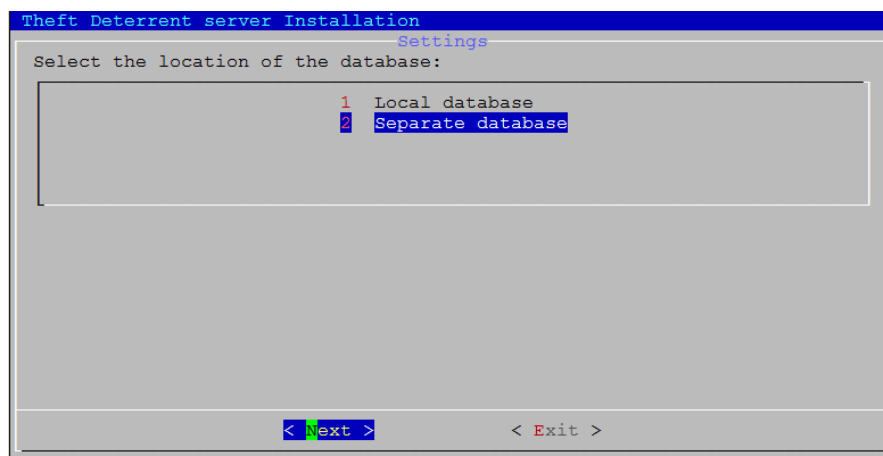
5. Select the Load Balance Mode as **Yes**



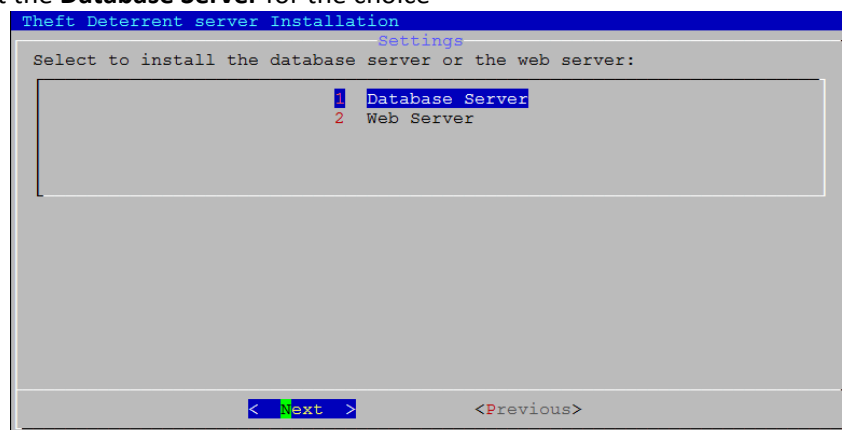
6. Select the **Database server** for the type of Load balance node.



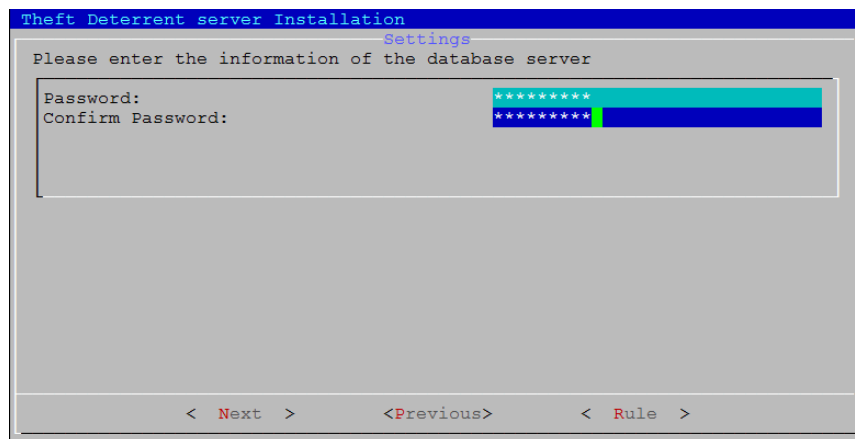
7. Select the **Separate Database** for the database location.



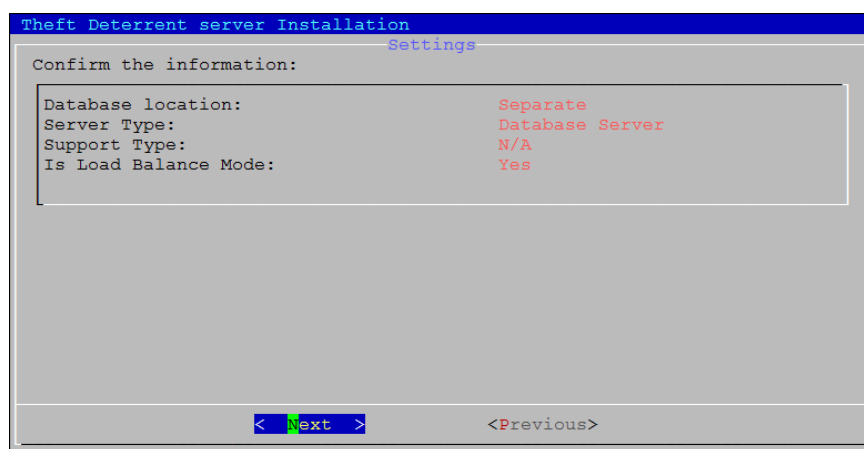
8. Select the **Database Server** for the choice



9. Input the database password and it will be required to input when install TD Webserver.



10. After summary, you can confirm your selection and Next and complete the database install in several minutes.



4.1.2 Install PGGate servers

Install the PGGate server in the same machine of Database server to get better performance.

- For each server, change to root account and input password when needed, change the pggate installer file's permission and run the installer:

```
su -
chmod +x Theft_Deterrent_pggate_v4.x.3010x.[version]
./Theft_Deterrent_pggate_v4.x.3010x.[version] install
```

```
root@kyang12x-debian7:~/td# ./Theft_Deterrent_pggate_v4.7.30103.13828 install
Selecting previously unselected package theftdeterrentpggate.
(Reading database ... 32695 files and directories currently installed.)
Preparing to unpack .../theftdeterrentpggate.deb ...
Unpacking theftdeterrentpggate (4.7.30103.13828) ...
Setting up theftdeterrentpggate (4.7.30103.13828) ...

Initialization configure manually, run the following command:
/usr/local/theftdeterrentpggate/initconf
Add database node manually, run the following command:
/usr/local/theftdeterrentpggate/uptconf
Get configure package manually, run the following command:
/usr/local/theftdeterrentpggate/getconf

Start server manually, run the following command:
/usr/local/theftdeterrentpggate/service_start
Stop server manually, run the following command:
/usr/local/theftdeterrentpggate/service_stop
Check server status, run the following command:
/usr/local/theftdeterrentpggate/service_status
```

4.1.3 Configure Master PGGate server

1. Select one PGGate as the Master PGgate server
2. Run the command

```
/usr/local/theftdeterrentpggate/initconf
```

- 1) Input the TD database server's database password
- 2) Input host/IP address for database unified entrance, it will be used for TDwebserver to connect with.
- 3) Select one network card need bind with

```
root@kyang12x-debian7:~/td# /usr/local/theftdeterrentpggate/initconf
#####
### Please input the following initialization information ###
#####
Database Password: Intel!123
Entrance Address: 192.168.1.210

/usr/local/theftdeterrentpggate/initconf: 75: printf: Illegal option -I
1.      eth0          192.168.1.122
2.      eth1          192.168.0.122
Select: 1
```

3. Run the command to restart the PGGate service

```
/usr/local/theftdeterrentpggate/service_start
```

```
root@kyang12x-debian7:~/td# /usr/local/theftdeterrentpggate/service_start
root@kyang12x-debian7:~/td#
```

4. Run the command to get the Master PGGate server's activate package:

```
/usr/local/theftdeterrentpggate/getconf
```

The activate package file pggate_conf.run will be generated under accordingly folder.

```
root@kyang12x-debian7:~/td# /usr/local/theftdeterrentpggate/getconf
Package is saved successfully under: /root/td/pggate_conf.run
root@kyang12x-debian7:~/td#
```

4.1.4 Configure Slave PGGate server

1. For Slave PGGate server, copy the Master PGGate server's activate package, run the package:

```
chmod +x pggate_conf.run
./pggate_conf.run
```

Select one network card need bind with in the other PGGate server

```
root@kyang12x-debian6:~/td# ./pggate_conf.run
Configure database hot-standby...
/var/lib/dpkg/info/theftdeterrentpggate.funcui: line 75: printf: -I: invalid op
tion
printf: usage: printf [-v var] format [arguments]
1.      eth0          192.168.1.123
2.      eth1          192.168.0.123
Select: 1
root@kyang12x-debian6:~/td#
```

2. Run the command to restart the PGGate service in the slave server

```
/usr/local/theftdeterrentpggate/service_start
```

4.1.5 Configure TD Database server

For Master TD Database server, run command to configure:

```
td database maxwebserver webserver_number
```

webserver_number: mean the estimation number of the TD Webserver. If the real number bigger than this estimation number, need configure the max number again.

```
root@kyang12x-debian10:~/td# td database maxwebserver 2
Optimization completed
Starting the Theft Deterrent database server ... done.
root@kyang12x-debian10:~/td#
```

4.1.6 Append TD Database server and PGGate server

If you want to add the TD database server to improve the performance, you can follow the steps:

1. Install the new TD Database server
2. Install the new PGGate server in the same machine of Database server.
3. For new PGGate server(new TD database server), copy the Master PGGate server's activate package, run the package, then restart the PGGate service

```
chmod +x ppgate_conf.run
./pggate_conf.run
/usr/local/theftdeterrentppgate/service_start
```

4.1.7 Install Database Cache server

The Database cache server is used when want to improve the database performance. Now one cache server is required to satisfy the target performance criteria.

1. Install 1 Linux servers
2. For each server, change to root account and input password when needed, change the cache installer file's permission and run the installer:

```
su -
chmod +x Theft_Deterrent_redis_v4.x.3010x.[version]
./Theft_Deterrent_redis_v4.x.3010x.[version] install
```

```
root@kyang12x-debian7:~/td# ./Theft_Deterrent_redis_v4.8.30103.14299 install
Selecting previously unselected package theftdeterrentredis.
(Reading database ... 32695 files and directories currently installed.)
Preparing to unpack .../theftdeterrentredis.deb ...
Unpacking theftdeterrentredis (4.8.30103.14299) ...
Setting up theftdeterrentredis (4.8.30103.14299) ...
Setting up the redis service...
Configure:
Port          : 16379
Config file   : /etc/redis/16379.conf
Log file      : /var/log/redis_16379.log
Data dir      : /var/lib/redis/16379
Executable    : /opt/TheftDeterrentredis/utils/./bin/redis-server
Cli Executable : /opt/TheftDeterrentredis/utils/./bin/redis-cli
Copied /tmp/16379.conf => /etc/init.d/redis_16379
Installing service...
Success!
Starting Redis server...
Installation successful!
```

The cache server configuration steps will be address in next section after TD Webservers setup successfully.

4.2 TD webserver and Nginx Deployment

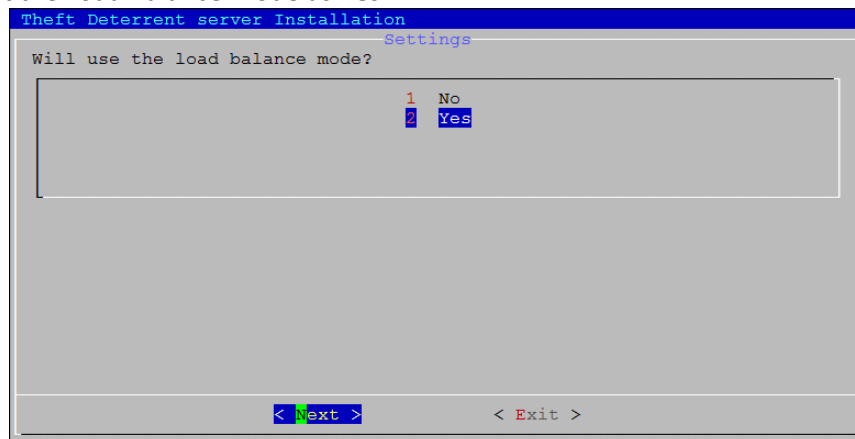
Install 4+ Linux servers: 2+ for TD Webserver and 2+ for Nginx server.

4.2.1 First Node Setup

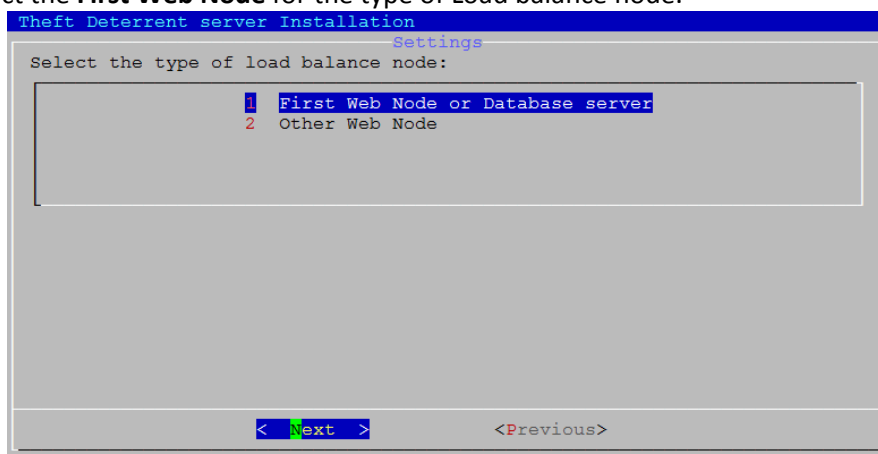
1. Run the installation package to open the install wizard:

```
su -  
chmod +x Theft_Deterrent_server_v4.x.3010X.[version]  
./Theft_Deterrent_server_v4.x.3010X.[version] install
```

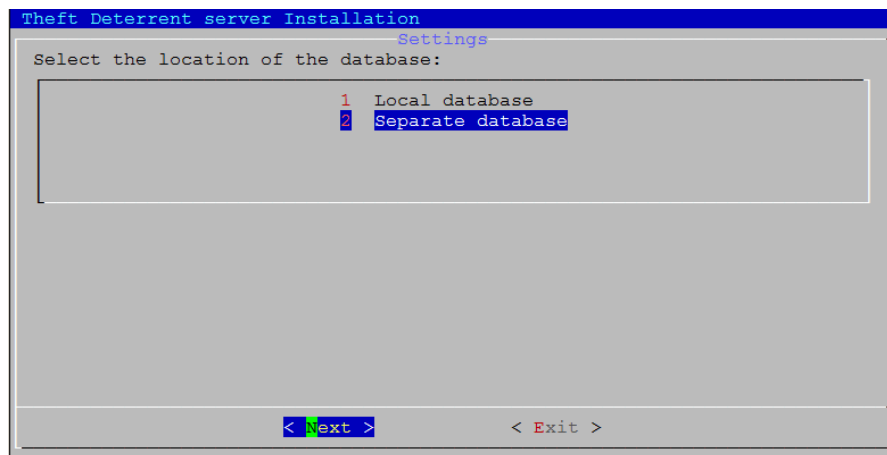
2. Select the Load Balance Mode as **Yes**



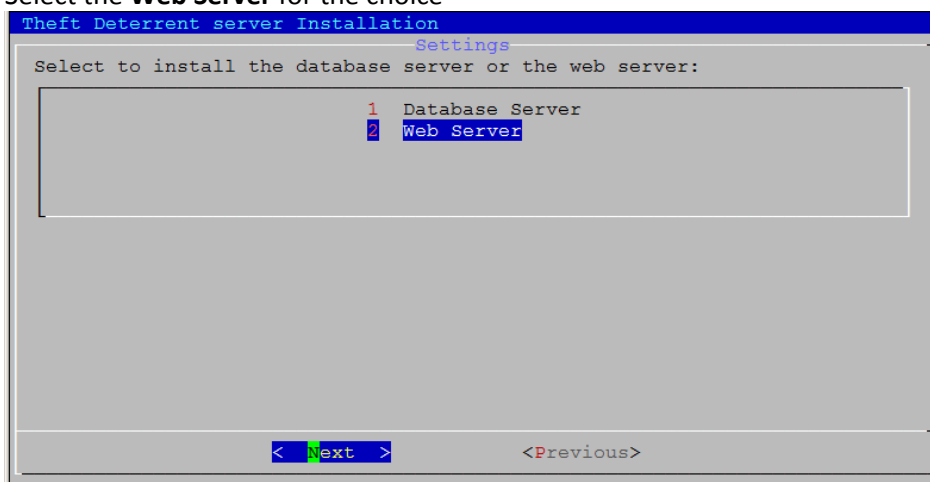
3. Select the **First Web Node** for the type of Load balance node.



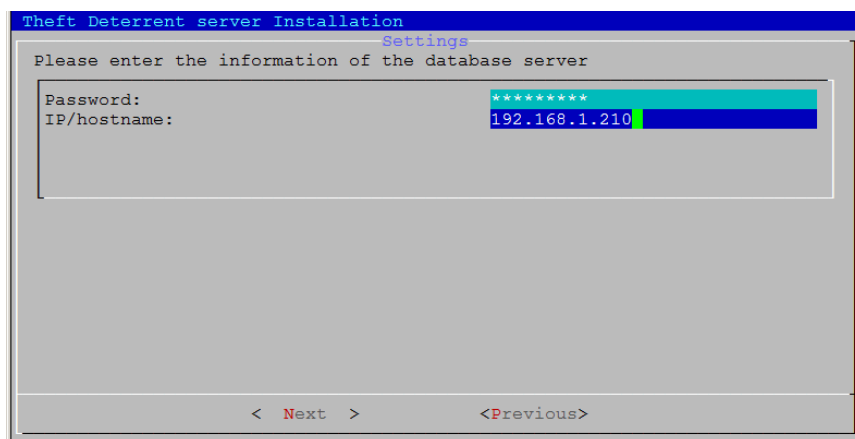
4. Select the **Separate Database** for the database location.



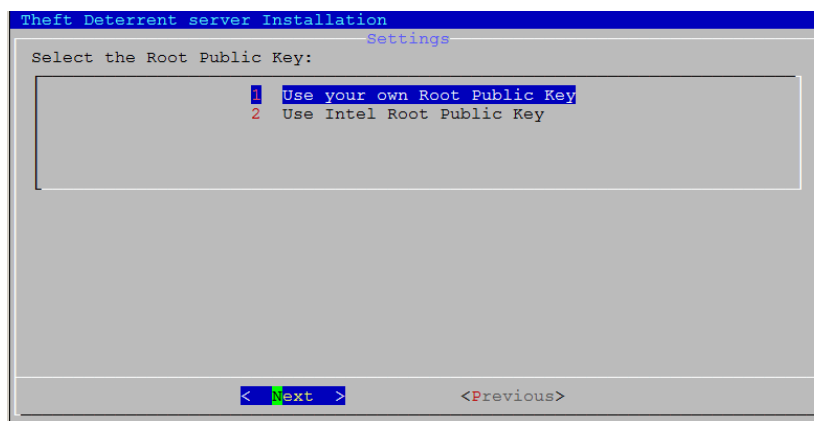
5. Select the **Web Server** for the choice



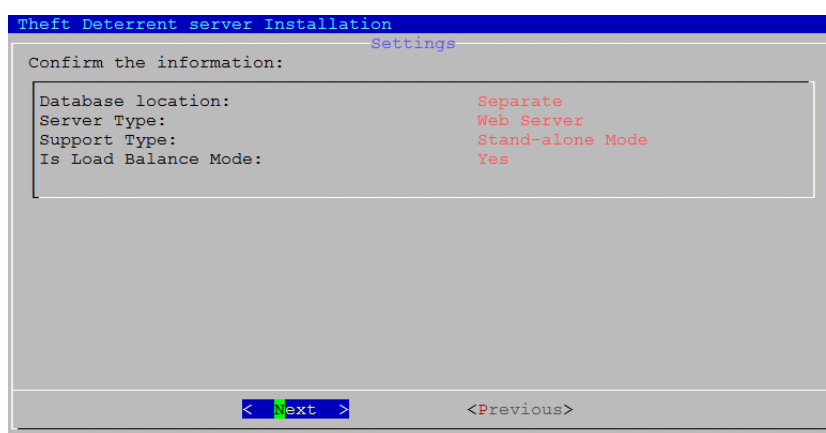
6. Input the shared database server's IP address/hostname and Password for the PGGate entrance address.



7. Select the Root Public key you will use for the infrastructure



8. After summary, you can confirm your selection and Next and complete the first Webservice Node's install in several minutes.



9. After the First Node install successfully, the image backup package will be created under /opt/TheftDeterrentserver/loadbalancedpkg.tdsbackup. If you cannot find the file, you can create the file through the command:

```
td setting backup
```

```
root@kyang12x-debian2:/opt/TheftDeterrentserver# td setting backup

-----
Theft Deterrent server backup/restore offline tool (4.7.0.13828)
Copyright (c) Intel Corporation. All rights reserved.
-----

Select language:
1. English
2. Espa?ol (N/A)
3. Portugu?o 茂驴茂驴茂驴 (N/A)
4. T 茂驴茂驴茂驴rk?e (N/A)
5. Vi?t Nam (N/A)
Input (1|2|3|4|5) [default:1]: 1
Set a password for the backup package:
Input:

Information:
> Server backup finished at /opt/TheftDeterrentserver/e3823476-89f6-4d37-98a3-f1
8dcb5c9be0.backup.tdspackage <
root@kyang12x-debian2:/opt/TheftDeterrentserver#
```

Input the password used to protect the backup package, then the relative file will be generated under /opt/TheftDeterrentserver/[UUID].backup.tdspackage

4.2.2 Install TD Webserver Other Node

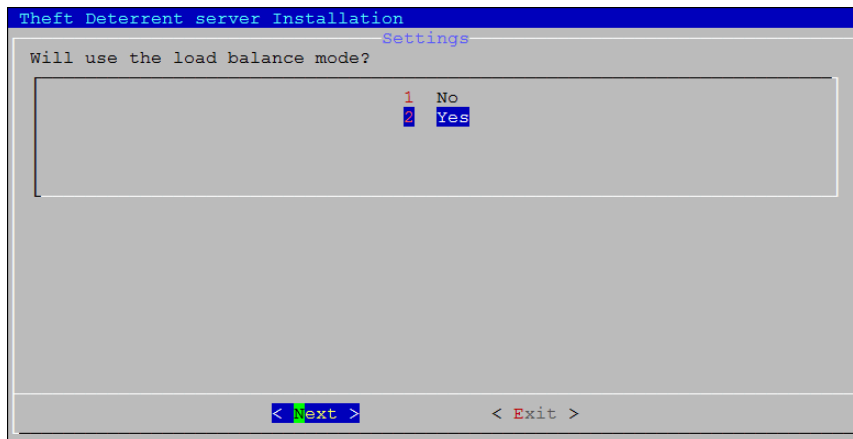
1. Run the installation package to open the install wizard:

```
su -
chmod +x Theft_Deterrent_server_v4.x.3010X.[version]
```

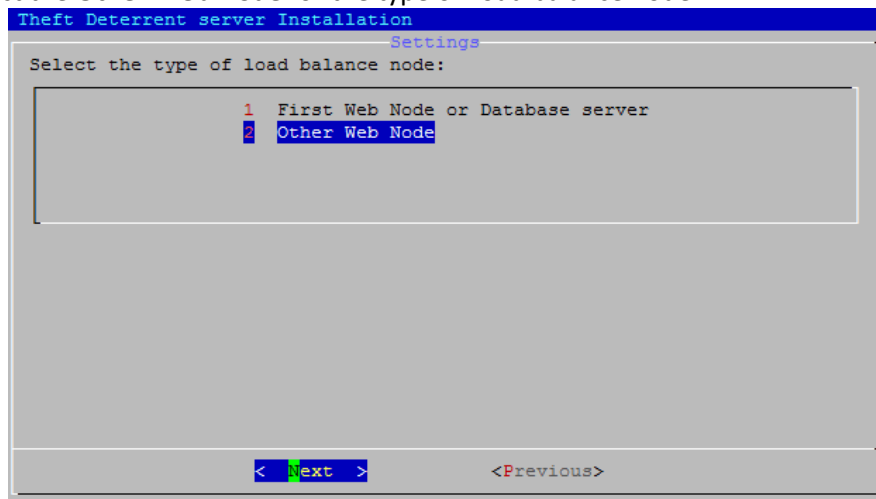


```
./Theft_Deterrent_server_v4.x.3010X.[version] install
```

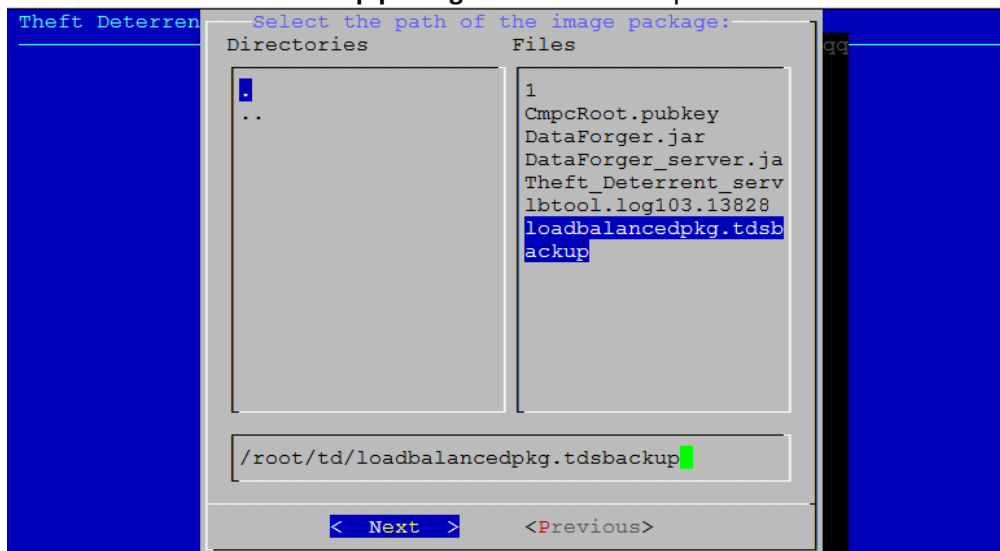
2. Select the Load Balance Mode as **Yes**



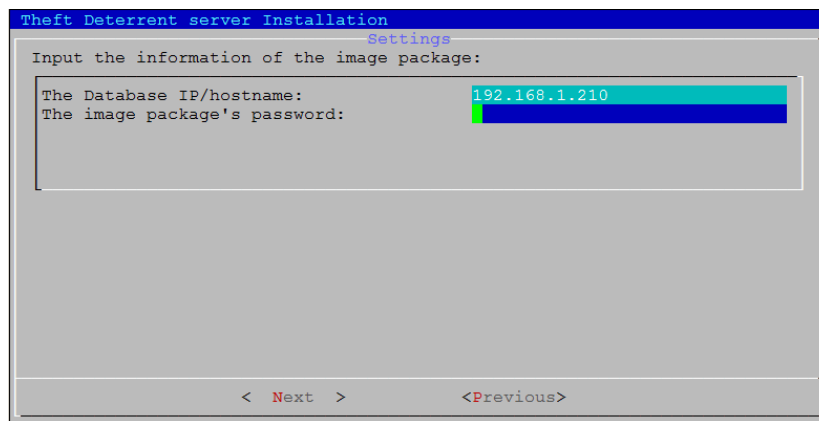
3. Select the **Other Web Node** for the type of Load balance node.



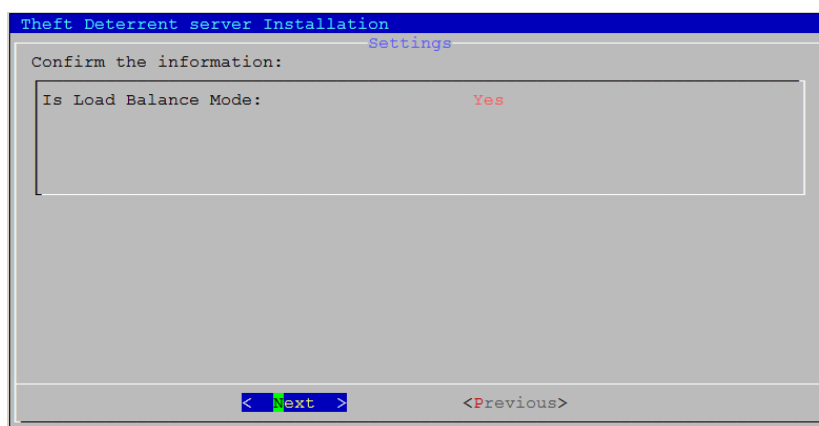
4. Select the **First Node's backup package** file location for path selection



5. Input the database server's IP address/hostname for the PGGate entrance address, and the backup image package's password if it has (leave it empty if no password)



6. After summary, you can confirm your selection and Next and complete the other Webservice Node's install in several minutes.



4.2.3 Configure TD Webserver Role

After install successfully, all these TDWebserver should can connect with the database components. For each of the TDWebserver, you need configure its role to one of the role before the TDweb load balance feature can work:

- 1: General Load balance Node. Can have one or several general node. Login to this server will not have manageability feature.
- 2: Manage Node. Must have one Node set as Manage node.
- 3: Manage back-up node. Optional. Can have one or several manage back-up node.

Select the Manage/Manage backup and General node in your infrastructure, go to one of the TDWebserver node with TD Database connection, run the command:

```
td lbtool -list
td lbtool -modify -mac [Web1_Mac] -role 2
td lbtool -modify -mac [Web2_Mac]-role 3
td lbtool -modify -mac [Web3_Mac]-role 1
```

For example:

```

root@kyang12x-debian2:/opt/TheftDeterrentserver# td lbtool -list
TheftDeterrent Server Loadbalance Configuration Tool 4.7

Database server 192.168.1.210 connected.

No.  Mac Address      IP Address      Server Name      Server Role
1    00-0c-29-ef-3b-49  192.168.1.128  192.168.1.128   General Loadbalance Node
2    00-0c-29-e9-cb-28  192.168.1.198  192.168.1.198   General Loadbalance Node

INFO: Loadbalance is enabled

root@kyang12x-debian2:/opt/TheftDeterrentserver# td lbtool -modify -mac 00-0c-29-ef-3b-49
-role 2
TheftDeterrent Server Loadbalance Configuration Tool 4.7

Database server 192.168.1.210 connected.

modify server [mac:00-0c-29-ef-3b-49] successful

No.  Mac Address      IP Address      Server Name      Server Role
1    00-0c-29-ef-3b-49  192.168.1.128  192.168.1.128   Manage Node
2    00-0c-29-e9-cb-28  192.168.1.198  192.168.1.198   General Loadbalance Node

INFO: Loadbalance is enabled

root@kyang12x-debian2:/opt/TheftDeterrentserver# td lbtool -modify -mac 00-0c-29-e9-cb-28
-role 3
TheftDeterrent Server Loadbalance Configuration Tool 4.7

Database server 192.168.1.210 connected.

modify server [mac:00-0c-29-e9-cb-28] successful

No.  Mac Address      IP Address      Server Name      Server Role
1    00-0c-29-ef-3b-49  192.168.1.128  192.168.1.128   Manage Node
2    00-0c-29-e9-cb-28  192.168.1.198  192.168.1.198   Manage Backup Node

INFO: Loadbalance is enabled

root@kyang12x-debian2:/opt/TheftDeterrentserver# █

```

4.2.4 Configure Database Cache server

If you need add the database cache server to improve the performance, run the command to configure it in the TDWebserver Manage Node.

1. Go to the TDWebserver Manage Node machine.
2. Run the command to configure cache server:

```
td redis add -address Cache_Server_IPAddress
```

Cache_Server_IPAddress: mean the IP address for the cache server if has.

3. Run the command to check the cache server status:

```
td redis status
```

```

root@kyang12x-debian2:~/td# td redis add -address 192.168.1.122
Theft Deterrent Redis Cache Server Configuration Tool 4.7

Current Cache Server Setting
No.  Server Address  Server Port
1    192.168.1.122   16379

WARNING:The setting will take effect after restart all TheftDeterrent web server
root@kyang12x-debian2:~/td# td redis status
Theft Deterrent Redis Cache Server Configuration Tool 4.7

Current Cache Server Setting
No.  Server Address  Server Port  Server Status
1    192.168.1.122   16379       Running

root@kyang12x-debian2:~/td# █

```

- The TD Webservice need be restarted for all of the web servers. In all Webserver machines, run the command:

```
td server restart
```

```
root@kyang12x-debian2:~/td# td server restart
Stopping the Theft Deterrent web server ...Clear up web server ...
done.
Stopping the Theft Deterrent broadcast service ... done.
Starting the Theft Deterrent broadcast service ... done.
Starting the Theft Deterrent web server ... done.
root@kyang12x-debian2:~/td#
```

4.2.5 Install and Configure Nginx server

- Run the installation package to run the install the Nginx server with TD Webserver's backup package file

```
su -
chmod +x Theft_Deterrent_nginx_v4.x.x.[version]
./Theft_Deterrent_nginx_v4.7.X.X install Webserver_backup_filename
```

```
root@kyang12x-debian3:~/td# ./Theft_Deterrent_nginx_v4.7.30103.13828 install loadbalancedpkg.tdsbackup
Selecting previously unselected package theftdeterrentnginx.
(Reading database ... 32788 files and directories currently installed.)
Preparing to unpack ../theftdeterrentnginx.deb ...
Unpacking theftdeterrentnginx (4.7.30103.13828) ...
Setting up theftdeterrentnginx (4.7.30103.13828) ...
Configure... done.
Starting the Theft Deterrent nginx server ... done.
root@kyang12x-debian3:~/td#
```

- Add TD Webserver node to Nginx server. Run command in Nginx server:

```
su -
tdngxctrl add all [WebIP1,WebIP2,WebIP3]
tdngxctrl refresh
```

WebIP1,WebIP2,WebIP3: mean the IP address for all the TD Webserver, separate the IP address with comma

```
root@kyang12x-debian3:~/td# tdngxctrl add all 192.168.1.128,192.168.1.198
ADDED [ all ] 192.168.1.128,192.168.1.198
root@kyang12x-debian3:~/td# tdngxctrl refresh
OK
root@kyang12x-debian3:~/td#
```

Note: if you do some customization for the TD Webserver HTTP/HTTPS port (not use the default 80:443 port), you need add one server through the 2 commands:

```
su -
tdngxctrl add service IP:HTTP_port
tdngxctrl add web IP:HTTPS_port
```

For example, the TD Webserver with IP 192.168.11.7 have customized port 8080/8443, then the 2 command will be like:

```
tdngxctrl add service 192.168.11.7:8080
tdngxctrl add web 192.168.11.7:8443
```

- For each of Nginx server, run the same steps for install and add TD Webserver node's step.

4.2.6 Append/Remove TD Webserver

You can add some TD Webserver node to improve the performance or remove some node in the future. The procedure will like:

1. Add/Remove the Webserver from Nginx server

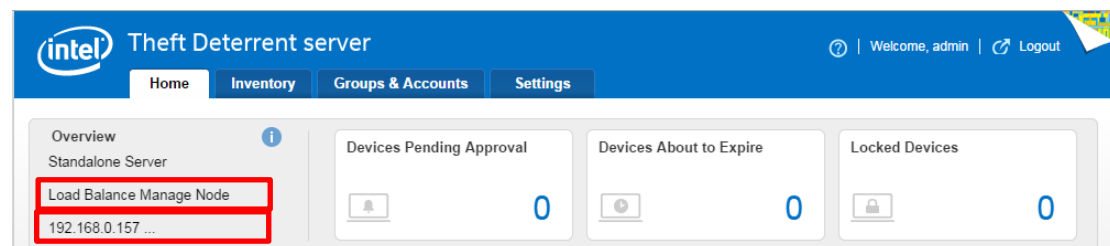
```
tdngxctrl add all WebIP  
tdngxctrl remove all WebIP
```

2. Configure the Webserver node's role. If one manage node is removed, you must configure another Webserver node as manage node. It is suggested modify the manage backup node as manage node.

4.3 Server Webpage Configuration

After all infrastructure setup, you can access the TDserver webpage through the Domain/Public IP of the Nginx server or the TD Webserver

1. Open browser and input address [http://\[domain_name\]/TheftDeterrent](http://[domain_name]/TheftDeterrent)
 - a. When first login or go to Settings->Advanced, set the server address according to the domain name/Nginx IP address. These address will be set to TDclient automatically if the TDclient support remote configure server address feature.
 - b. The Home Page will show the type of TD Webserver node current connected with and the TDserver's address(es)



- c. Under Settings, the Load Balance tab will be display to show the TD Webserver and Database server Node list and each of their status.

The screenshot shows the Intel Theft Deterrent server web interface. The top navigation bar includes links for Home, Inventory, Groups & Accounts, and Settings. The Settings menu is expanded, and the Load Balance option is highlighted with a red box. Below the navigation bar, the page title is "Load Balance Settings". A warning icon and text state: "Only use these settings or tools if you are an advanced user. Contact your product field representative for support when needed." The page displays the "Webserver Node List" with the following information: "The node you are visiting is 192.168.1.128" and "The following are the Webserver nodes." A table lists two nodes:

IP Address	MAC Address	Last Update Time	Version	Role
192.168.1.128	00-0c-29-ef-3b-49	2015-12-24 11:18:09	4.7.30103.13828	Load Balance Manage Node
192.168.1.198	00-0c-29-e9-cb-28	2015-12-24 11:18:08	4.7.30103.13828	Load Balance Manage-backup Node

Below the table, the "Database Server Node List" is shown with the information: "Current primary database node is 192.168.1.125" and "The following are the Database nodes." A table lists two nodes:

IP Address	Postgre Status	SSH Status	WAL Sequence Number
192.168.1.125	Normal	Normal	00000001000000000000000003
192.168.1.124	Normal	Normal	00000001000000000000000003

The footer of the page includes copyright information: "© Intel Corporation | Version 4.7.30103.13828" and links for Language, Terms of Use, *Trademarks, Privacy, and Cookies.

And you can also use the TD client to connect with the server with Domain Name/Public IP to verify the TD function, like first provision, lock and unlock.

5. Monitor Server Setup and Monitor

5.1 Install Monitor server

Refer to the Monitor server deployment guide on how to install and configure the monitor server to monitor TD load balance infrastructure.

5.2 Regular Monitor

The admin of the TD infrastructure need keep eyes to monitor system, understanding the CPU/Memory/Network usage of each component and adjust the server, network etc

5.2.1 Adjust Database server

According the monitor result, if the CPU usage of database server is high, admin need add the logical CPUs of database server.

If the process status of 'postgres' mostly is 'D', it is means the database server is busy on waiting the hard disk operation. Admin need improve the hard disk performance, such as move to another physical server with more powerful hard disk raid.

5.2.2 Adjust TD web server

According the monitor result, if the CPU usage of TD web server is high while the free memory is enough, admin need add the logical CPUs for the TD Webserver, or add a new TD Webserver.

If the CPU usage of TD web server is not high while the kept TCP connection is high, admin need improve the TD Webserver's hard disk performance, or add a new TD web server.

If add a new TD Webserver, please follow the steps:

1. Adjust the database server setting, increase the supported max connection.
2. Clone or install a new TD web server, follow the Webserver install and append steps in Section 4.2.
3. Modify the firewall rule.
4. Add the new server to monitor system.

5.2.3 Adjust TD Nginx server

According the monitor result, if the CPU usage of Nginx server is high, admin need add the logical CPUs of Nginx, or add a new Nginx server.

If you want increase the logical CPUs of Nginx server, follow the steps:

1. Modify /opt/TheftDeterrentnginx/conf/nginx.conf, set the 'worker_processes' to the quantity of logical CPUs of the Nginx server.

If you want to add a new Nginx server, follow the steps:

1. Change the DNS server setting, add the public IP of new Nginx server to the server domain name.

2. Modify the TD Setting for Server Address, add the public IP in the server address. Refer to 4.2.5.
3. Add the new server to monitor system.

Note: the workload of Nginx servers are not balanced, the new Nginx server maybe has less workload compared with other Nginx server.