

# Installazione vte su Linux Ubuntu 24.04 LTS

- [Installazione](#)
- [Configurazione](#)
- [Hardening](#)

# Installazione

Aprire il programma *Putty* e collegarsi all'host remoto dove si dovrà installare vtenext tramite connessione SSH.

Si consiglia di aggiornare i pacchetti linux

```
sudo apt update && sudo apt upgrade -y
```

Riavviare il server in caso di aggiornamenti del kernel così da rendere attivo l'ultimo kernel.

Dopo aver aggiornato il sistema è necessario installare i pacchetti, se non presenti, che permetteranno il funzionamento di vtenext.

## Installare Apache

```
sudo apt install apache2
```

Una volta installato, attivare i moduli rewrite ed headers

```
a2enmod rewrite headers
```

Modificare il virtualhost che sarà utilizzato per vtenext in modo da consentire i rewrite necessari per il funzionamento delle RESTAPI aggiungendo la seguente parte

```
<Directory /var/www/html/VTE_FOLDER>  
Options -Indexes +FollowSymLinks +MultiViews  
AllowOverride All  
Require all granted  
</Directory>
```

## Installare PHP

Vedi [scheda requisiti](#) per maggiori dettagli sui moduli richiesti

```
sudo apt install php php-cli php-bcmath php-gd php-imap php-ldap php-mysql php-curl php-  
imagick php-mbstring php-xml php-apcu php-zip libapache2-mod-php
```

Modificare il file php.ini in modo da configurare i parametri come richiesto da vtenext

```
sudo nano /etc/php/8.3/apache2/php.ini
```

```
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT & ~E_NOTICE  
display_errors = Off  
memory_limit = 256M  
log_errors = On  
file_uploads = On  
output_buffering = On
```

**Salvare il file ed applicare la stessa modifica al file `/etc/php/8.3/cli/php.ini`**

Riavviare il servizio apache per rendere le configurazioni attive

```
sudo systemctl restart apache2
```

## Installare MySQL

```
sudo apt install mysql-server mysql-client
```

Per il corretto funzionamento del tool [Importazione Dati](#) di vtenext, è necessario che il servizio MySQL lavori con `sql_mode` non strict e che il comando "local infile" sia concesso.

Per farlo è possibile creare un file di configurazione in `/etc/mysql/conf.d` chiamato ad esempio `vtenext.cnf` con il seguente contenuto

```
[mysqld]  
sql_mode = ''  
local-infile  
  
[mysql]  
local-infile
```

Riavviare poi il servizio MySQL

```
sudo systemctl restart mysql
```

Creare un utente dedicato ed il nuovo database che sarà utilizzato poi nel wizard di installazione che segue nella sezione "Deploy VTENEXT"

Accedere con un utente mysql privilegiato e creare l'utenza chiamata ad esempio "vtenext"

```
CREATE USER 'vtenext'@'localhost' IDENTIFIED BY 'PasswordComplessa';
```

Creare il database ed assegnare i GRANT all'utente appena creato

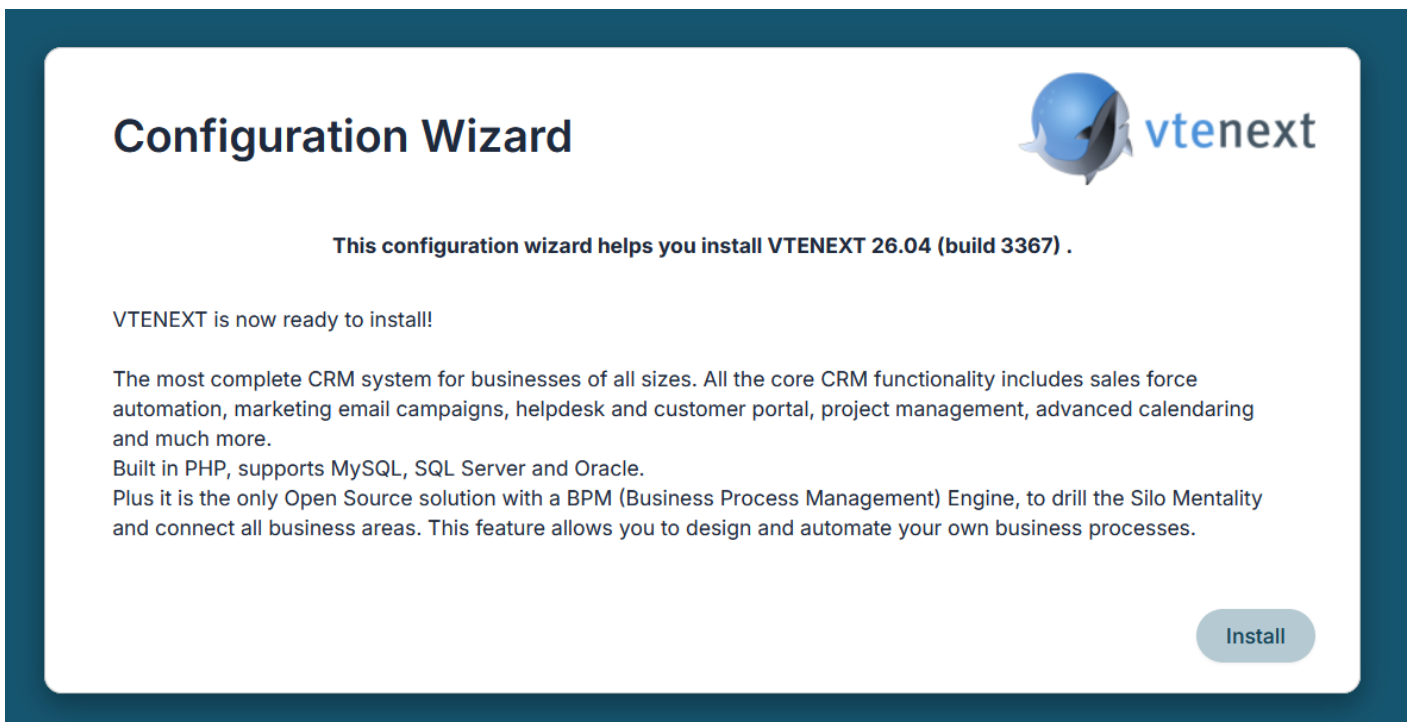
```
CREATE DATABASE vtenext CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;  
GRANT ALL PRIVILEGES ON vtenext.* TO 'vtenext'@'localhost';  
FLUSH PRIVILEGES;
```

## Deploy VTENEXT

Decomprimere il pacchetto vtenext nella cartella `/var/www/html/` ed assegnare proprietario e gruppo alla cartella e ai file contenuti ricorsivamente con il comando

```
chown -R www-data:www-data /var/www/html/CARTELLA/
```

Aprire il browser digitate nella barra degli indirizzi l'url per giungere alla cartella appena generata nel server e si avvierà la procedura di configurazione di vtenext.



The screenshot shows the 'Configuration Wizard' for VTENEXT. It features a blue header with the title 'Configuration Wizard' and the VTENEXT logo (a blue sphere with a white arrow) and the text 'vtenext'. Below the header, a message states: 'This configuration wizard helps you install VTENEXT 26.04 (build 3367) .'. The main content area contains the text: 'VTENEXT is now ready to install!', followed by a description: 'The most complete CRM system for businesses of all sizes. All the core CRM functionality includes sales force automation, marketing email campaigns, helpdesk and customer portal, project management, advanced calendaring and much more. Built in PHP, supports MySQL, SQL Server and Oracle. Plus it is the only Open Source solution with a BPM (Business Process Management) Engine, to drill the Silo Mentality and connect all business areas. This feature allows you to design and automate your own business processes.' At the bottom right, there is a blue 'Install' button.

Premere il pulsante **Install** e accettare le condizioni di licenza per proseguire.

# License Agreement



## VTENEXT Business License

The VTENEXT software ("the Software") is copyright © 2017 VTENEXT SRL of VERONA, Italy ("VTENEXT"). Use of the Software is permitted subject to the below terms and conditions. A company or other legal entity wishing to deploy the Software ("Customer") must accept these terms. Without acceptance, Customer may not use the Software except as permitted under the GNU Affero General Public License version 3 ("AGPL").

### Article 1. Grant of license

VTENEXT hereby grants Customer a limited, non-exclusive license to install, deploy and use the Software for its business operations.

The license is limited to Customer. Customer may not distribute copies to third parties, and may not make available functionality of the Software to third parties, for example through a Software-as-a-Service business models or by offering the services of the Software to third parties. Independent contractors working for the sole benefit of Customer, e.g. consultants and temporary employees hired through a staffing agency, are not considered third parties.

The license includes the right to make modifications to the Software and to have independent contractors

Back

I do not agree

I agree

Se tutti i pacchetti sono stati installati e le impostazioni del file `php.ini` sono state settate correttamente si visualizzerà la seguente schermata.

Per modificare i parametri di **RECOMMENDED PHP SETTINGS** digitare `sudo nano/etc/php/8.3/apache2/php.ini` e cercare i valori da modificare, riavviare Apache e premere il pulsante **Check Again**.

# Pre Installation Check



PHP Version >= 8.3	8.3.6
IMAP Support	Yes
Zlib Support	Yes
GD graphics library	Yes
Database Extension	Yes
cURL library	Yes
SimpleXML extension	Yes
Multibyte String extension	Yes
Imagick extension	Yes

Check Again

### Recommended PHP Settings:

Your PHP directives have the Recommended values

Back

Next

Premere il pulsante **Next**. Configurare i parametri del database e premere il pulsante **Next**.

# System Configuration



## Database Information

Database Type \* MySQL

Host Name \*

localhost

Server listen Port

3306

User Name \*

vtenext

Password

••••••••••

Database Name \*

vtenext

Create Database (Will drop if the database exists)

Populate database with demo data

Back

Next

## CRM Configuration

URL \*

http://mycrmurl

Currency Name \*

Euro(€)

Confermare le configurazioni e avviare l'installazione.

# Configurazione

## Configurazione CRON

Verificare che il file *RunCron.sh* nella cartella cron abbia i permessi di esecuzione attraverso il comando `sudo chmod a+x RunCron.sh`. Digitare il comando `crontab -e -u www-data` e inserire la seguente riga nel crontab dell'utente `www-data`:

```
***** /PATH_VTENEXT/cron/RunCron.sh >> /PATH_VTENEXT/logs/cron.log 2>&1
```

**NB: Sostituire "PATH\_VTENEXT" con il percorso assoluto di vtenext su disco del server**

## Backup e Restore

Per effettuare il Backup utilizzare strumenti a riga di comando che si possono reperire facilmente effettuando una ricerca sul web.

Restore:

1) Decomprimere il backup dei file

```
tar xzf /backups/FILE.tgz PATH_VTENEXT
```

2) ricreare il DB (CHARSET **utf8mb4** collation **utf8mb4\_general\_ci**) e lanciare il comando di restore del dump:

```
zcat FILE.sql.gz | mysql DATABASE
```

Se spostate/duplicate l'ambiente verificare i parametri nel nuovo *config.inc.php*:

- `$PORTAL_URL`
- `$dbconfig['db_name']` e relative credenziali di accesso al servizio database
- `$site_URL`
- `$root_directory`

**NB: In questo caso sarà necessario riattivare la licenza di vte.**

# Hardening

Per eseguire un hardening efficace di vtenext su stack **LAMP (Linux, Apache, MySQL, PHP)** Ubuntu 24.04 si consiglia di seguire i seguenti passi suddivisi per i vari componenti dello stack.

## Linux

Si consiglia di installare fail2ban in modo da bloccare tentativi di scansioni da parte di tool automatici / scanner di vulnerabilità.

Per farlo:

```
sudo apt install fail2ban
```

Verificate che il servizio sia attivo:

```
systemctl status fail2ban
```

Creare un file personalizzato che registri la definizione di un nuovo filtro in modo da bloccare l'ip sorgente della scansione.

Il filtro rileva gli status HTTP 404 e li riporta al motore di fail2ban per la valutazione

```
sudo nano /etc/fail2ban/filter.d/apache-404.conf
```

contenuto:

```
[Definition]

failregex = ^<HOST> .* "(GET|POST|HEAD|PUT).*" 404
ignoreregex =.*(robots.txt|favicon.ico|jpg|png|gif)
```

Attivare il filtro creato creando in file

```
sudo nano /etc/fail2ban/jail.local
```

con il seguente contenuto:

```
[DEFAULT]

ignoreip = 127.0.0.1/8 ::1
```

```
[apache-404]

enabled = true
port = http,https
filter = apache-404
action = iptables-allports[protocol=all, blocktype=DROP]

logpath = /var/log/apache2/access.log

bantime = 3600
findtime = 120
maxretry = 100
```

Nella configurazione sopra, viene letto il file "access.log" e se il filtro "apache-404" rileva un numero di tentativi uguale o superiore a "maxretry" nell'arco di "findtime" secondi, l'ip sorgente da cui arrivano le richieste web sarà bannato per "bantime" secondi.

Per bannato si intende l'applicazione della "action" ovvero il drop delle connessioni.

Riavviare il servizio fail2ban

```
systemctl reload fail2ban
```

Richiamando il comando

```
sudo fail2ban-client status
```

saranno mostrate le configurazioni attive per cui fail2ban opera.

E' inoltre disponibile il comando fail2ban-client che permette di visualizzare lo stato dei blocchi IP attivi per un determinato "filtro".

Considerando il filtro "apache-404" per visualizzare lo stato:

```
sudo fail2ban-client status apache-404
```

Rimuovere un ban:

```
fail2ban-client set apache-404 unbanip 1.2.3.4
```

Bannare manualmente:

```
fail2ban-client set apache-404 banip 1.2.3.4
```

# Apache

E' utile nascondere le informazioni relative alla versione di apache in modo da evitare attacchi mirati.

Modificare:

```
sudo nano /etc/apache2/conf-enabled/security.conf
```

Impostare:

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off
```

Riavviare:

```
sudo systemctl restart apache2
```

# MySQL

MySQL fornisce un comando dedicato a questo scopo che è possibile richiamare.

Questo comando avvia un wizard da terminale dove verifica lo stato attuale e propone delle modifiche che si possono accettare o meno.

```
mysql_secure_installation
```

Esempio di output

```
root@ubuntu24:~# mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y
```

There are three levels of password validation policy:

LOW Length >= 8

MEDIUM Length >= 8, numeric, mixed case, and special characters

STRONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1

Skipping password set for root as authentication with auth\_socket is used by default.

If you would like to use password authentication instead, this can be done with the "ALTER\_USER" command.

See <https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management> for more information.

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? (Press y|Y for Yes, any other key for No) : y  
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? (Press y|Y for Yes, any other key for No) : y  
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? (Press y|Y for Yes, any other key for No) : y  
- 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? (Press y|Y for Yes, any other key for No) : y

Success.

All done!

**NB. Si consiglia sempre di creare un utente MySQL dedicato per il singolo database di vtenext.**

Nel caso il server condividesse più installazioni di vtenext (come ad esempio l'ambiente di produzione e quello di test) è sempre consigliato creare utenze diverse in modo da evitare propagazioni indesiderate su altri database/ambienti di lavoro.