YouTestMe

Business Continuity Planning

This document describes YouTestMe logistic plan used to restore interrupted business services

Table of Contents

1 Introduction

Consider a scenario where we lost the entire physical server with all virtual machines and all data on it (e.g., server burned down, stolen, or hijacked)
This document should provide answers to the following questions:

1. What do we need to do regularly to efficiently reactivate service to a client and enable them to continue their business?
2. How we will do it (step by step procedure)
3. Who will do it, and how long will it take?
4. How we test the process, and how often?

Data safety is ensured by maintaining standby servers with periodic or real-time data replication.

We should set realistic goals, for example:

- Recovery can be made within 6 hours of the incident
- We may lose a maximum of one hour of data (data created in the last hour between the previous backup and failure time)
- If an incident occurs and the server becomes unavailable, it will take us up to 15 minutes to redirect users to the standby site so they can continue business

The priority for us is to minimize downtime and service interruption to the client.

In the case of the incident, we have two options depending on how fast we can do each of them:

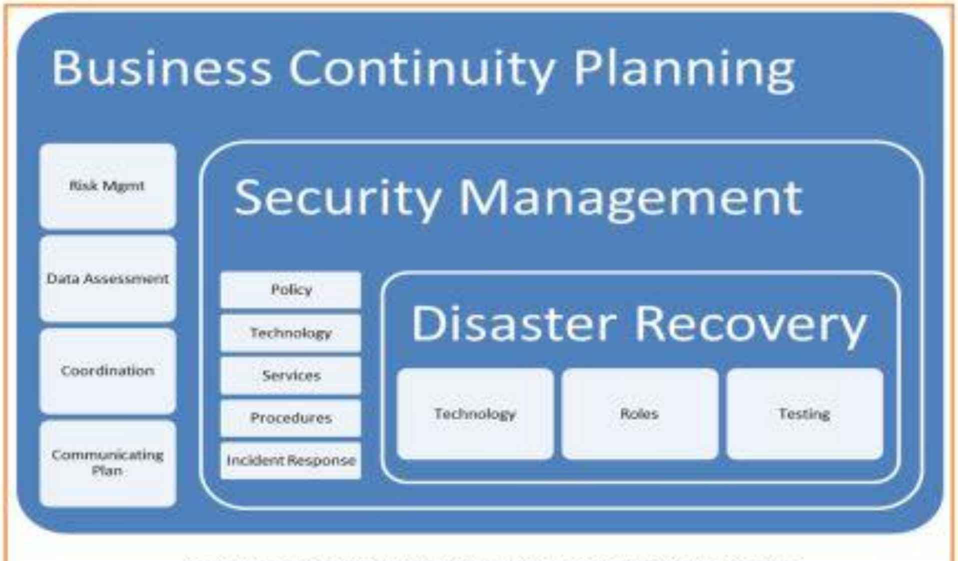
- To recover a server that encountered an incident
- To switch to the standby server

This document will address BCP (Business Continuation) and DR (Disaster Recovery).

2 Terminology and Definitions

DR strategy is the cornerstone to ensuring infrastructure and applications continue to operate when a major outage hit.

While BCP (Business Continuation Plan) focuses on the whole business, the DR (Disaster Recovery) plan focuses more on its technical side. DRP is a documented process or set of procedures to execute an organization's disaster recovery processes and recover and protect a business IT infrastructure in the event of a disaster. It's best to think of a BCP as an umbrella policy, with DR as part of it.



Business Continuity Planning as it relates to IT

3 Disaster Recovery Procedure

The procedure depends on data backup frequency and how it is implemented, but there are two main approaches:

- Activate Warm Standby Site
- Activate Hot Standby Site

The first restore strategy is adequate for periodic-type data backup (daily backup, for example) where there is a tolerance of data loss between two database snapshots.

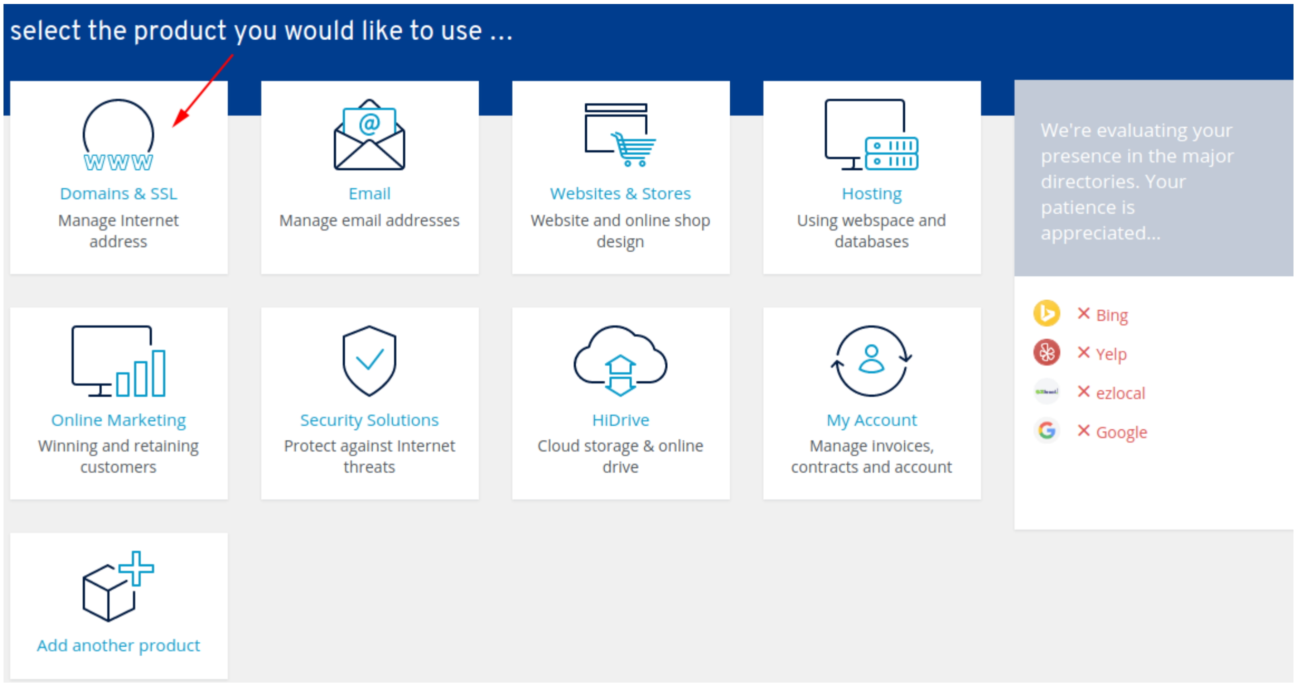
In case there is a need for continuous recording of data, PITR will ensure that interrupted operations continue from the moment of primary database failure.

3.1 Activate Warm Standby Site

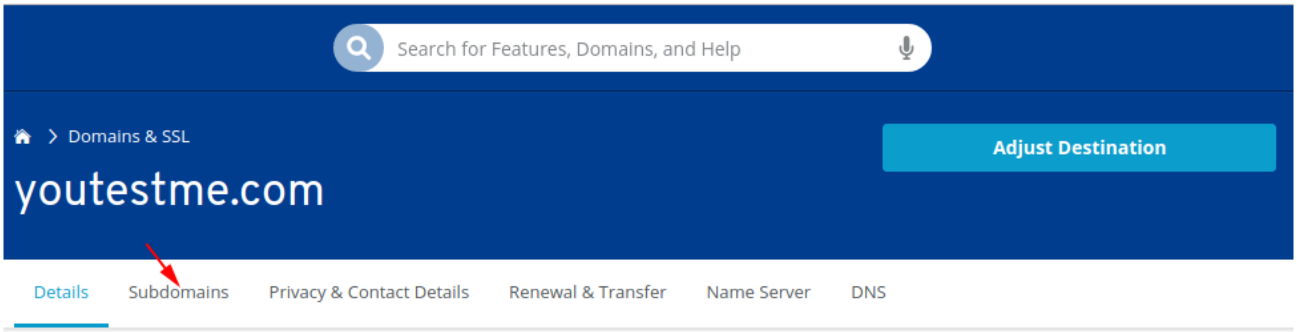
Warm standby is a redundancy method in which the secondary (i.e., backup) system runs in the primary system's background. Data is mirrored to the secondary server at regular intervals, which means that there are times when both servers do not contain the same data.

When a disaster happens, it is necessary to redirect the application link to the Warm Standby site located on the separate physical server as soon as possible. The following actions should be taken:

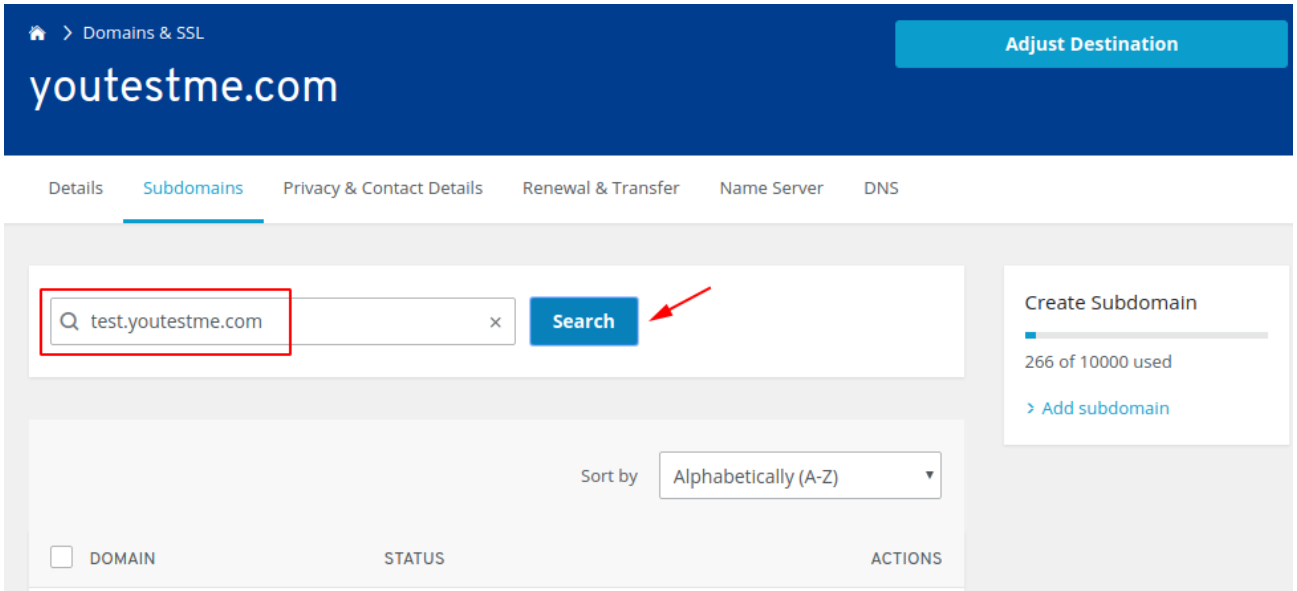
1. Log in to Domain Provider Web Control Panel (www.ionos.com)
2. Navigate to the "Domains and SSL" page:


select the product you would like to use ...
Domains & SSL
Manage Internet address
Email
Manage email addresses
Websites & Stores
Website and online shop design
Hosting
Using webspace and databases
We're evaluating your presence in the major directories. Your patience is appreciated...
✕ Bing
✕ Yelp
✕ ezlocal
✕ Google
Online Marketing
Winning and retaining customers
Security Solutions
Protect against Internet threats
HiDrive
Cloud storage & online drive
My Account
Manage invoices, contracts and account
Add another product

3. Click on "Subdomains":



4. Search for specific subdomain:



youtestme.com

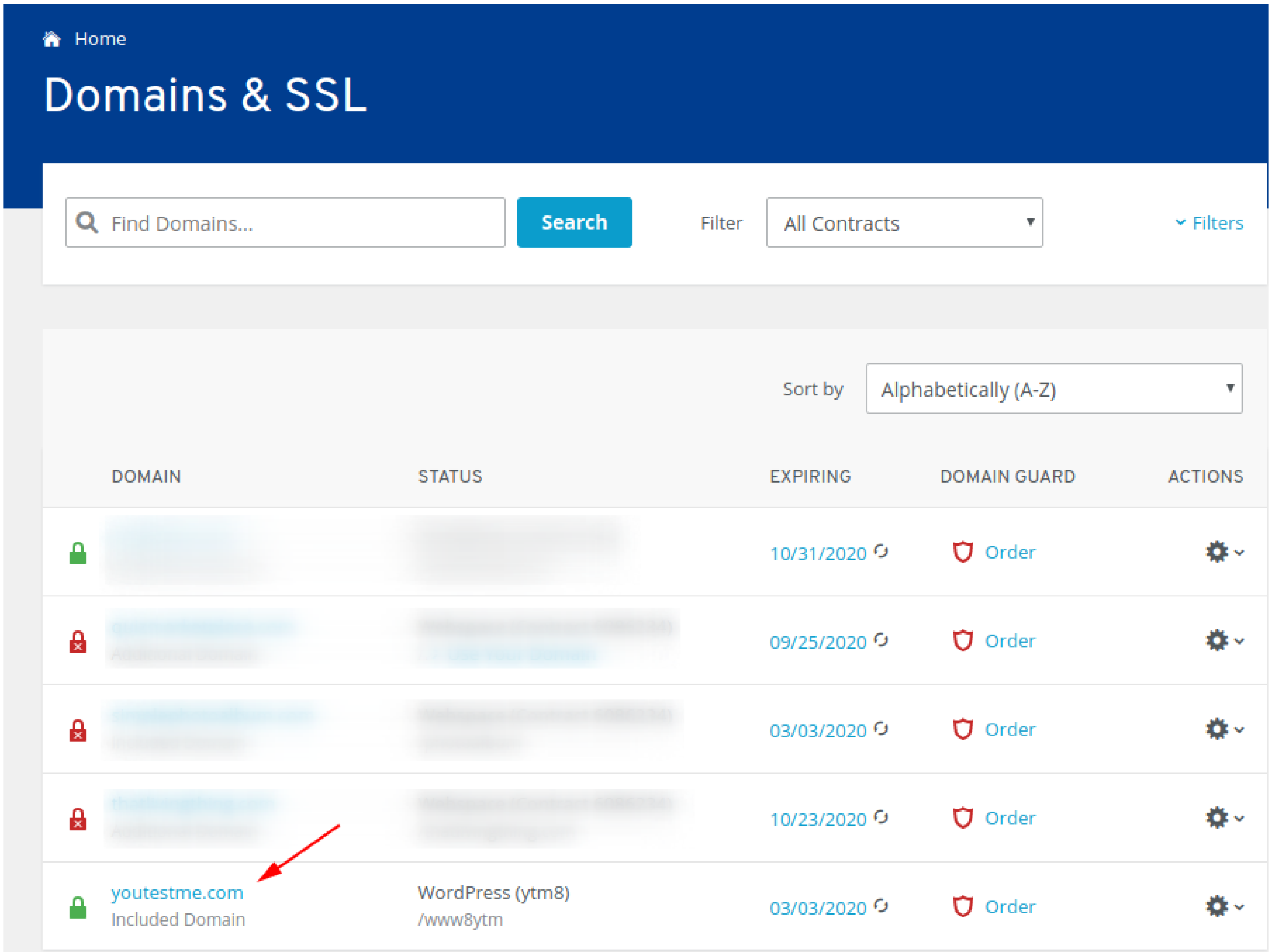
test.youtestme.com

Create Subdomain

266 of 10000 used

Sort by: Alphabetically (A-Z)

□ DOMAIN	STATUS	ACTIONS



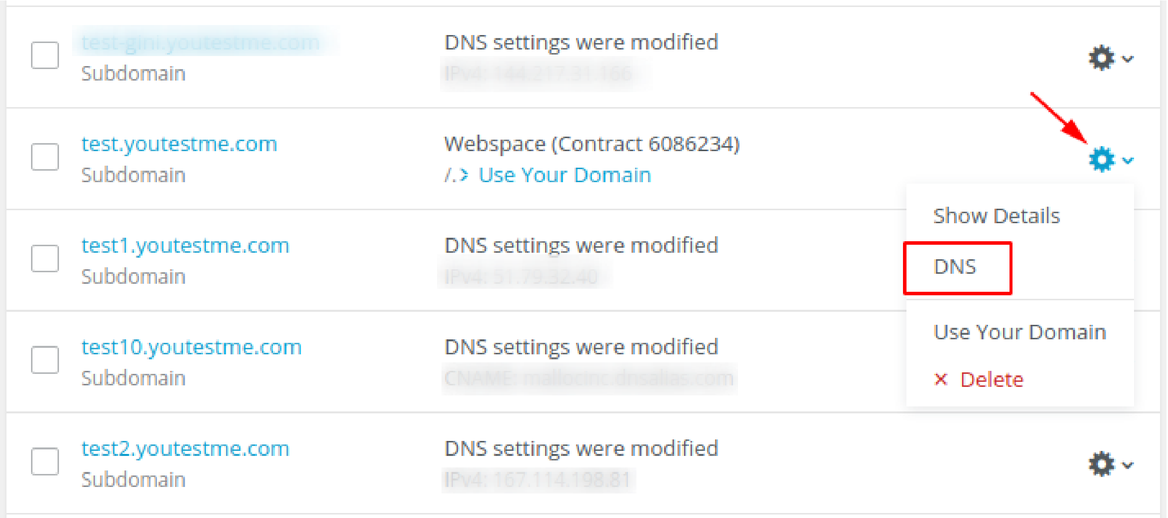
Domains & SSL

Filter: All Contracts

Sort by: Alphabetically (A-Z)

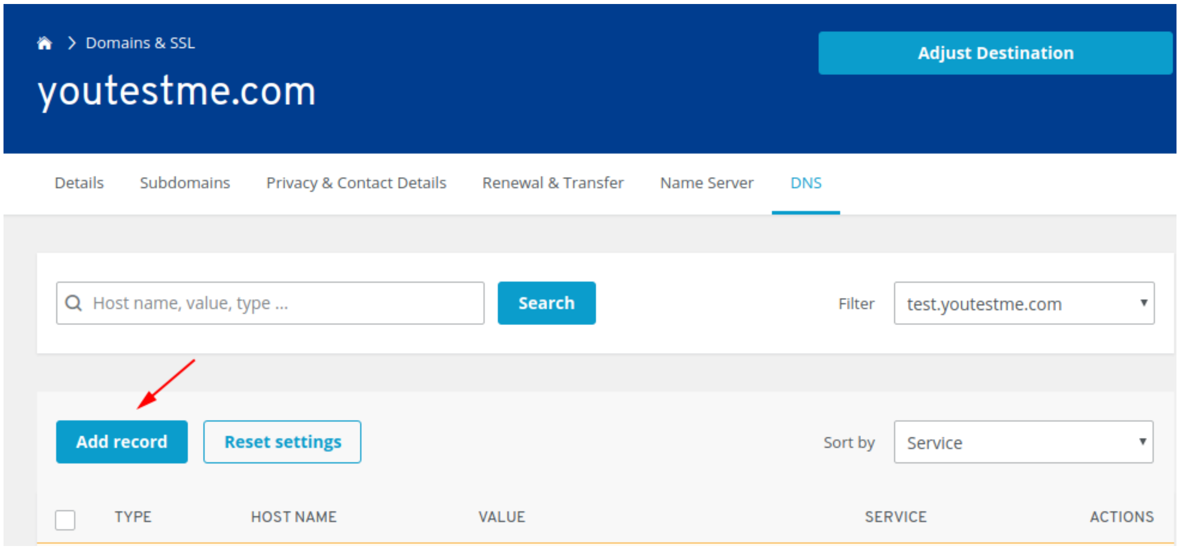
DOMAIN	STATUS	EXPIRING	DOMAIN GUARD	ACTIONS
[redacted]	[redacted]	10/31/2020	Order	⚙
[redacted]	[redacted]	09/25/2020	Order	⚙
[redacted]	[redacted]	03/03/2020	Order	⚙
[redacted]	[redacted]	10/23/2020	Order	⚙
youtestme.com Included Domain	WordPress (ytm8) /www8ytm	03/03/2020	Order	⚙

5. Select "DNS" to modify DNS settings for the specified subdomain:



□	[redacted] Subdomain	DNS settings were modified [redacted]	⚙ ⌄
□	test.youtestme.com Subdomain	Webspace (Contract 6086234) /.› Use Your Domain	⚙ ⌄
□	test1.youtestme.com Subdomain	DNS settings were modified [redacted]	
□	test10.youtestme.com Subdomain	DNS settings were modified [redacted]	
□	test2.youtestme.com Subdomain	DNS settings were modified [redacted]	⚙ ⌄

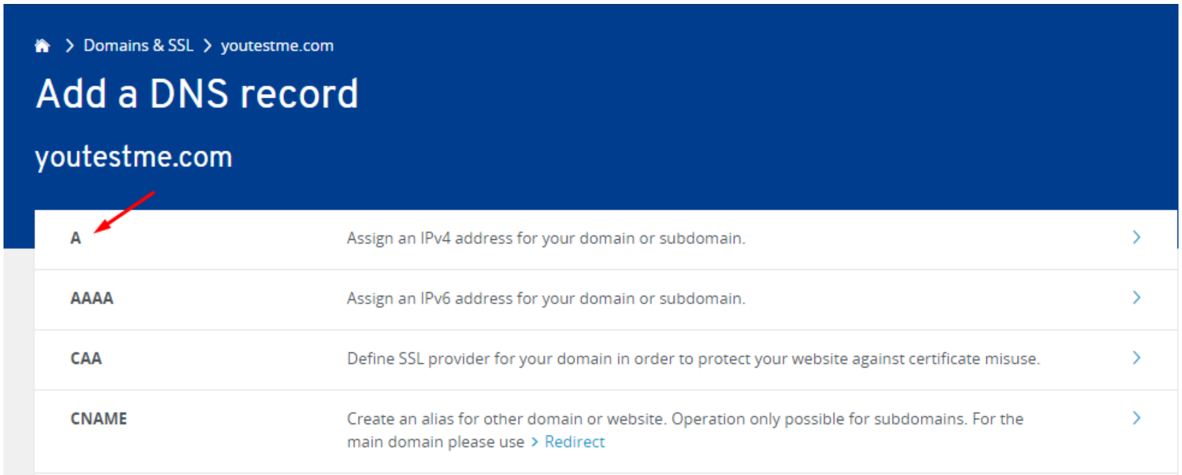
6. Click on the "Add record" button to create a new A record for the specified subdomain:



Filter: test.youtestme.com

Sort by: Service

□	TYPE	HOST NAME	VALUE	SERVICE	ACTIONS

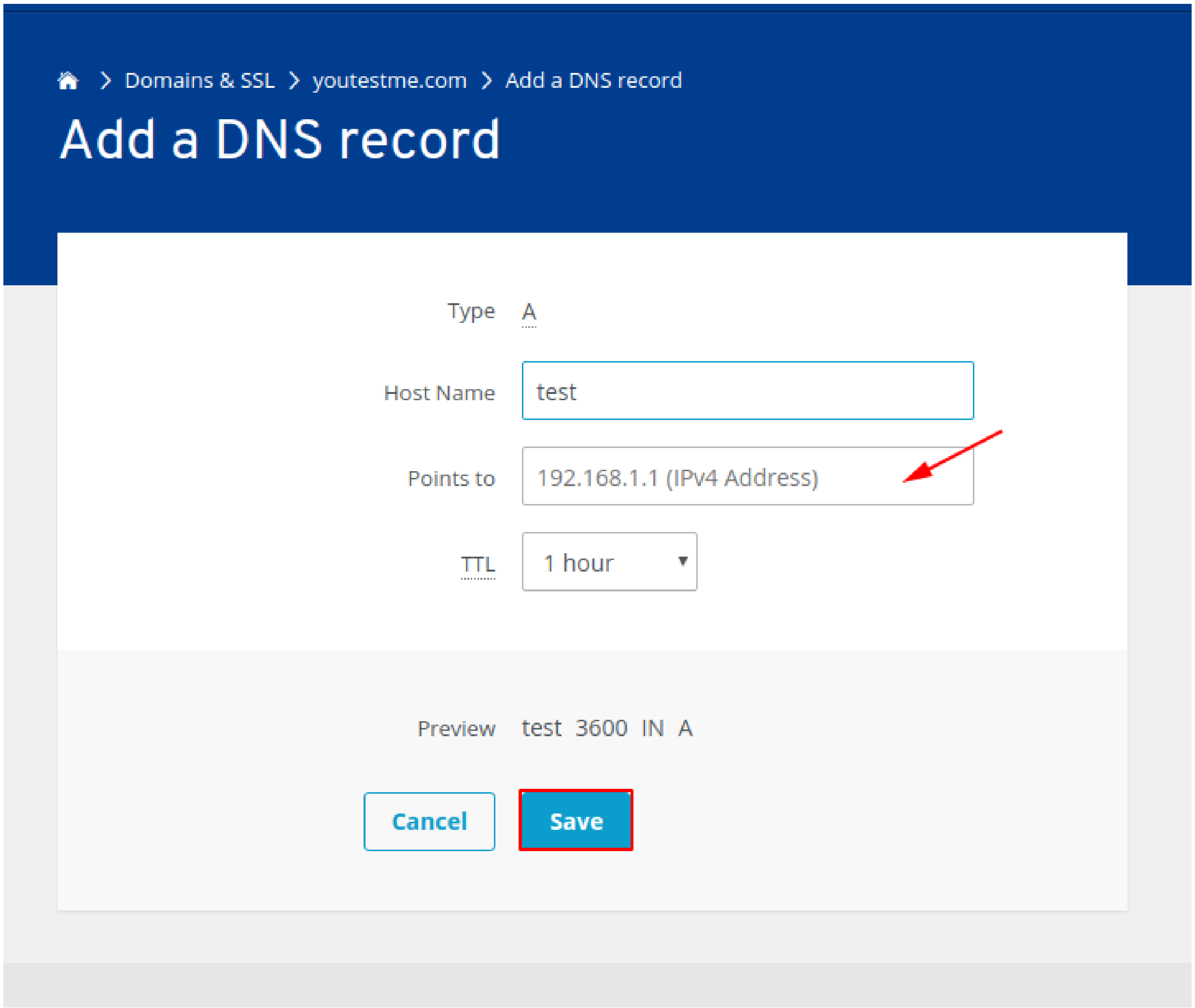


Add a DNS record

youtestme.com

A	Assign an IPv4 address for your domain or subdomain.	›
AAAA	Assign an IPv6 address for your domain or subdomain.	›
CAA	Define SSL provider for your domain in order to protect your website against certificate misuse.	›
CNAME	Create an alias for other domain or website. Operation only possible for subdomains. For the main domain please use › Redirect	›

7. Enter Standby Site IP address and apply the changes:



Domains & SSL > youtestme.com > Add a DNS record

Add a DNS record

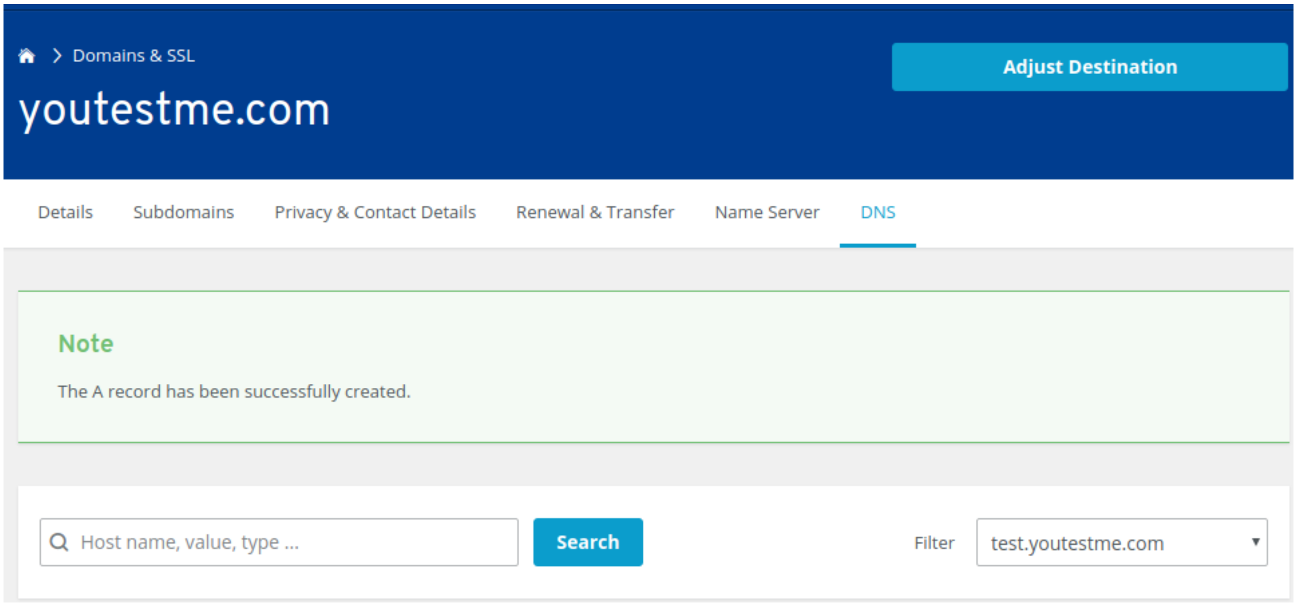
Type A

Host Name: test

Points to: 192.168.1.1 (IPv4 Address)

TTL: 1 hour

Preview test 3600 IN A



Domains & SSL

youtestme.com

Note

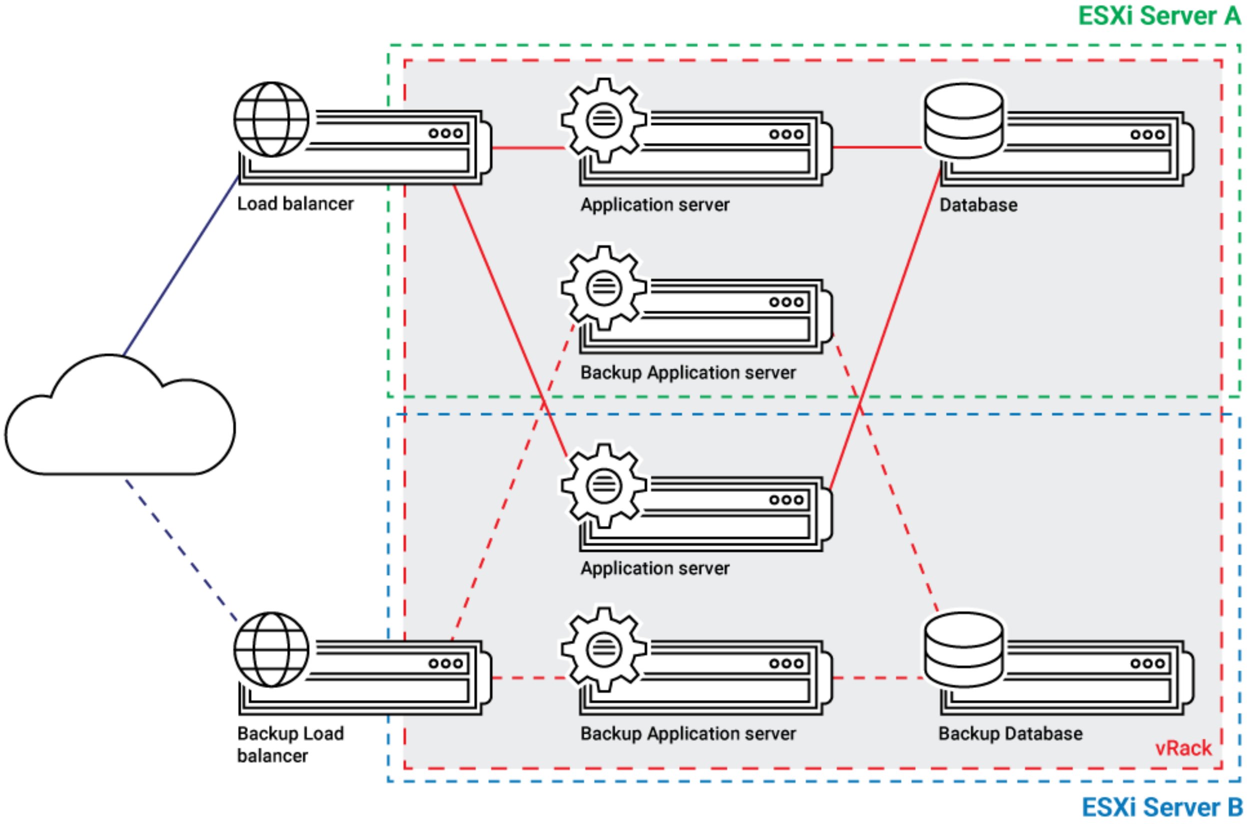
The A record has been successfully created.

Filter: test.youtestme.com

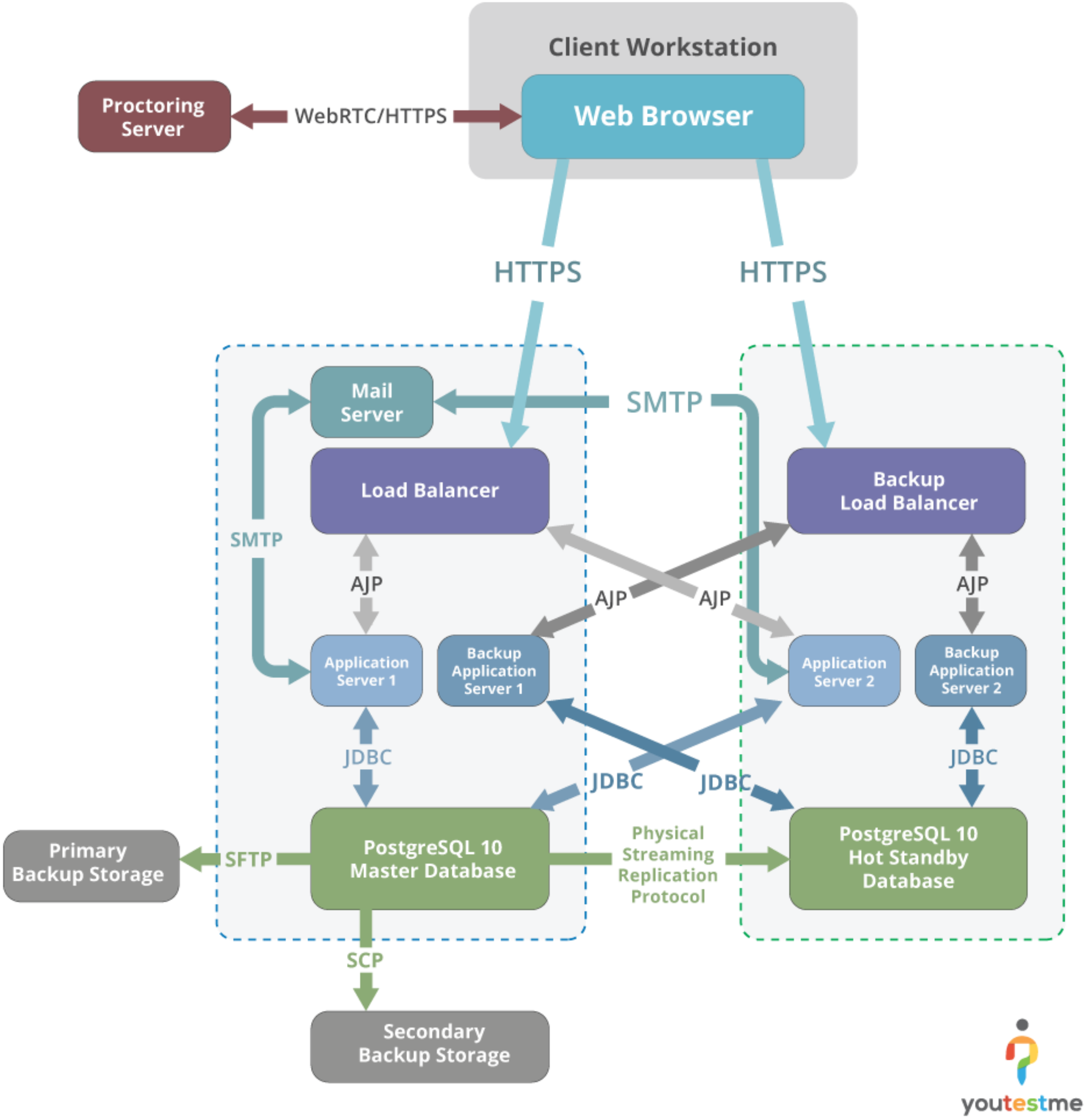
3.2 Activate Hot Standby Site

Hot standby is a redundant method in which one system runs simultaneously with an identical primary system. Upon failure of the primary system, the hot standby system immediately takes over, replacing the primary system. However, data is still mirrored in real-time. Thus, both systems have identical data.

3.2.1 Network Diagrams



3.2.2 Data Flow Diagram



3.2.3 Disaster Scenarios

Many possible issues can occur and interrupt a complex system's functionality, such as the YTM Application - Enterprise Edition.

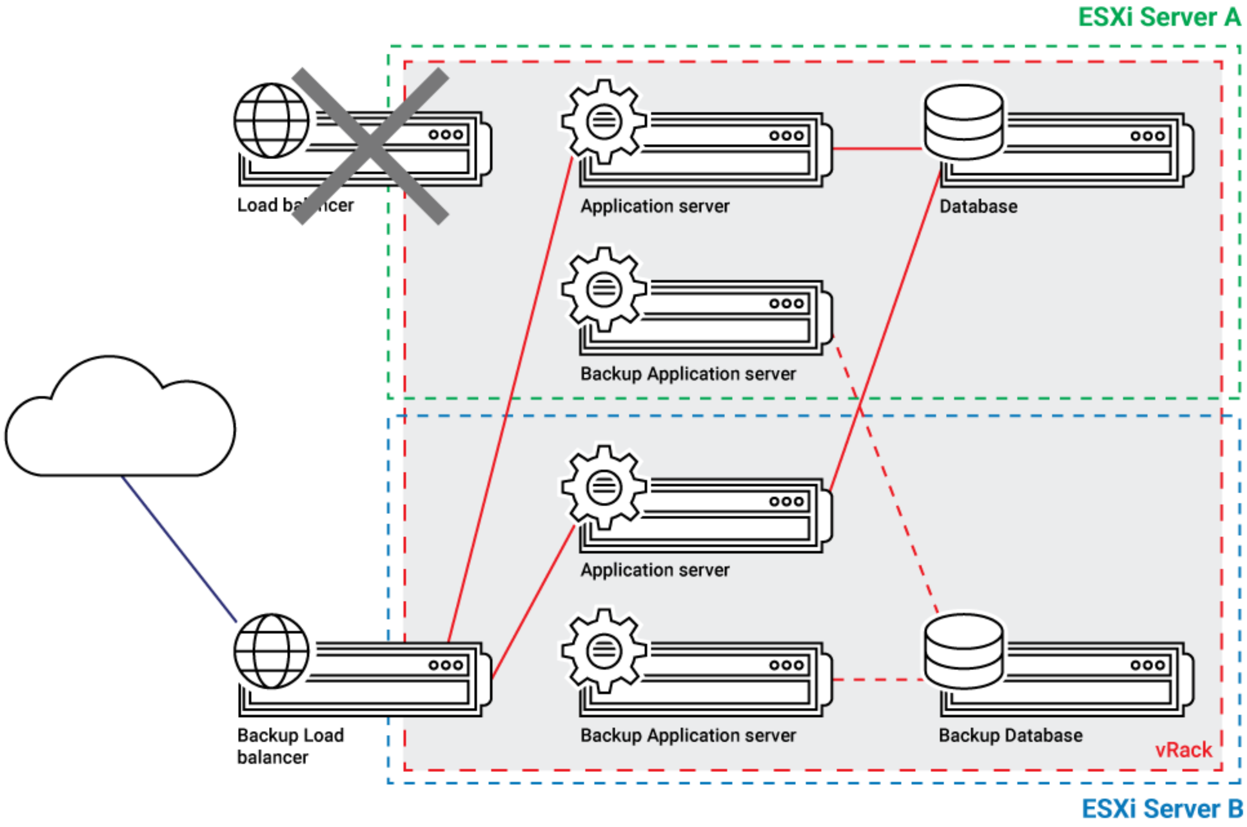
The table below lists the most critical scenarios that could cause an application to crash or dramatically reduce its performance.

#	Disaster Scenario	Criticality	Disaster Recovery Procedure
1.	Load Balancer Failure	High	Load Balancer Failure
2.	Application Server Failure	Medium	Application Server Failure
3.	Database Server Failure	High	Database Server Failure
4.	Primary Server Failure	Critical	Primary Server Failure

Every disaster scenario type will be explained in a separate chapter with an appropriate recovery procedure.

3.2.4 Load Balancer Failure

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across several servers. Load balancers are used to increase the capacity (concurrent users) and reliability of applications.

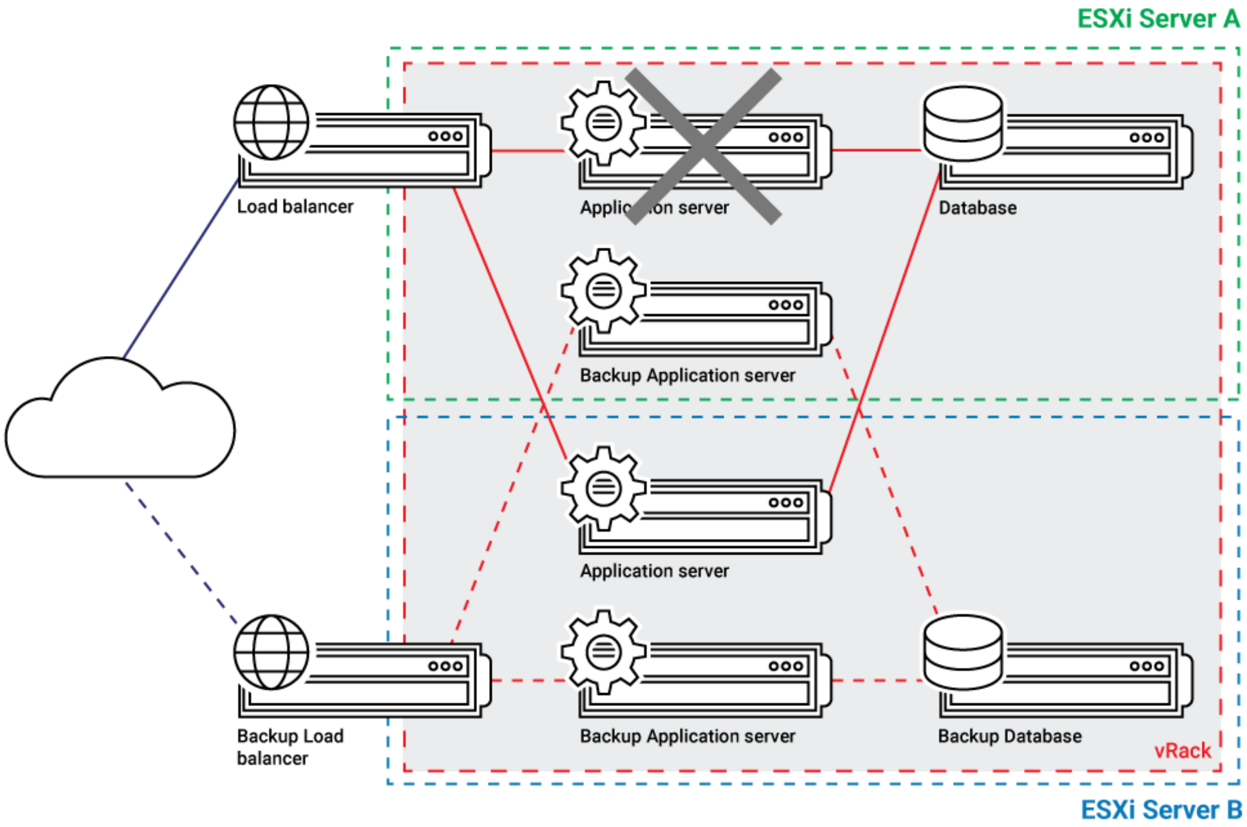


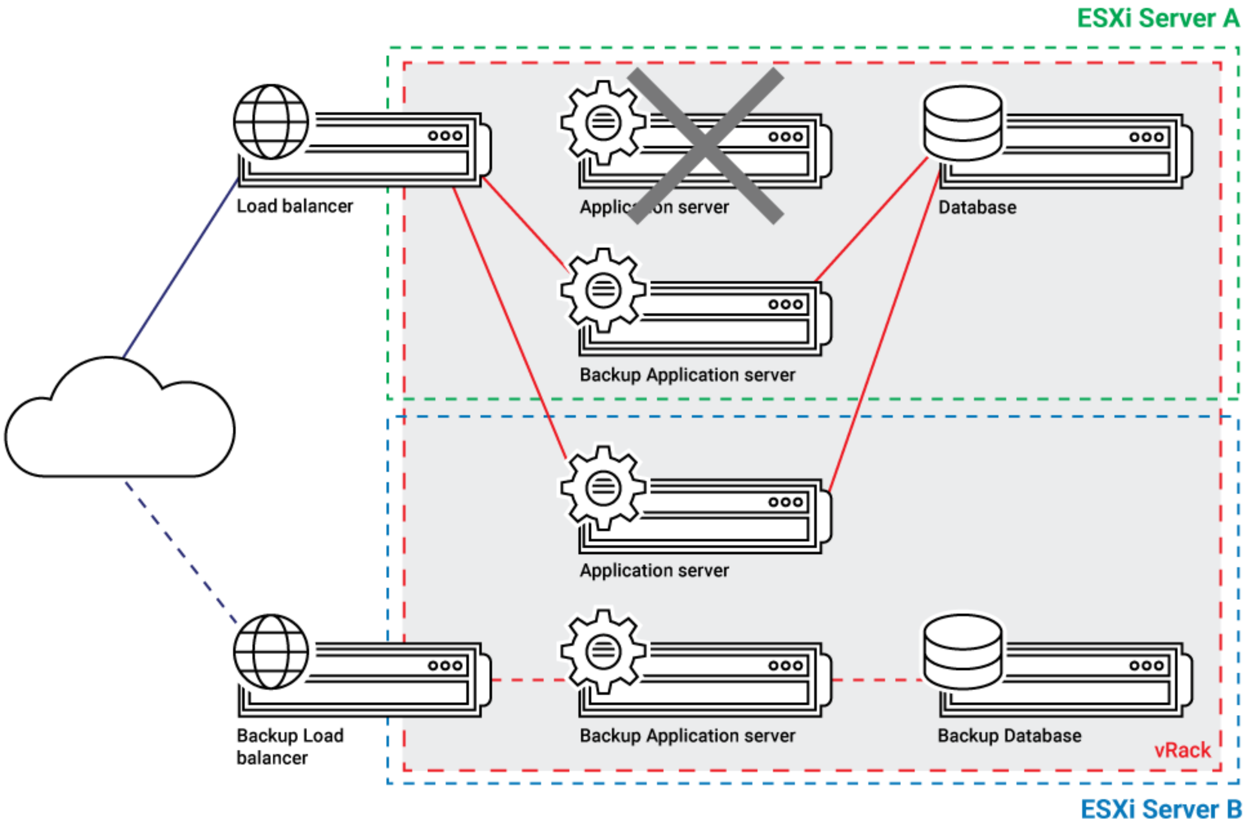
If the primary Load Balancer fails on server A, all traffic will be redirected to backup Load Balancer located on Standby physical server B.

The following actions need to be taken:

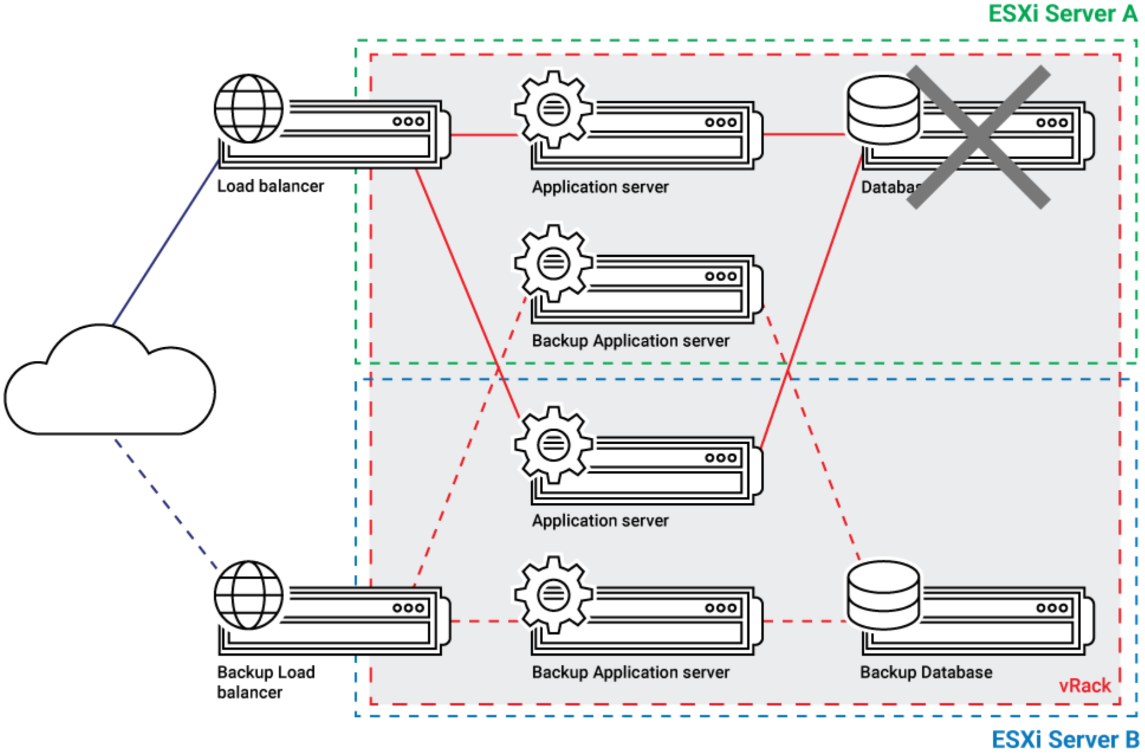
1. Modify DNS settings of the YTM subdomain to ensure that client URL points to IP address of Standby Load Balancer
2. Ensure that new active LB distribute application traffic to the same pair of application server that was active in the failover time

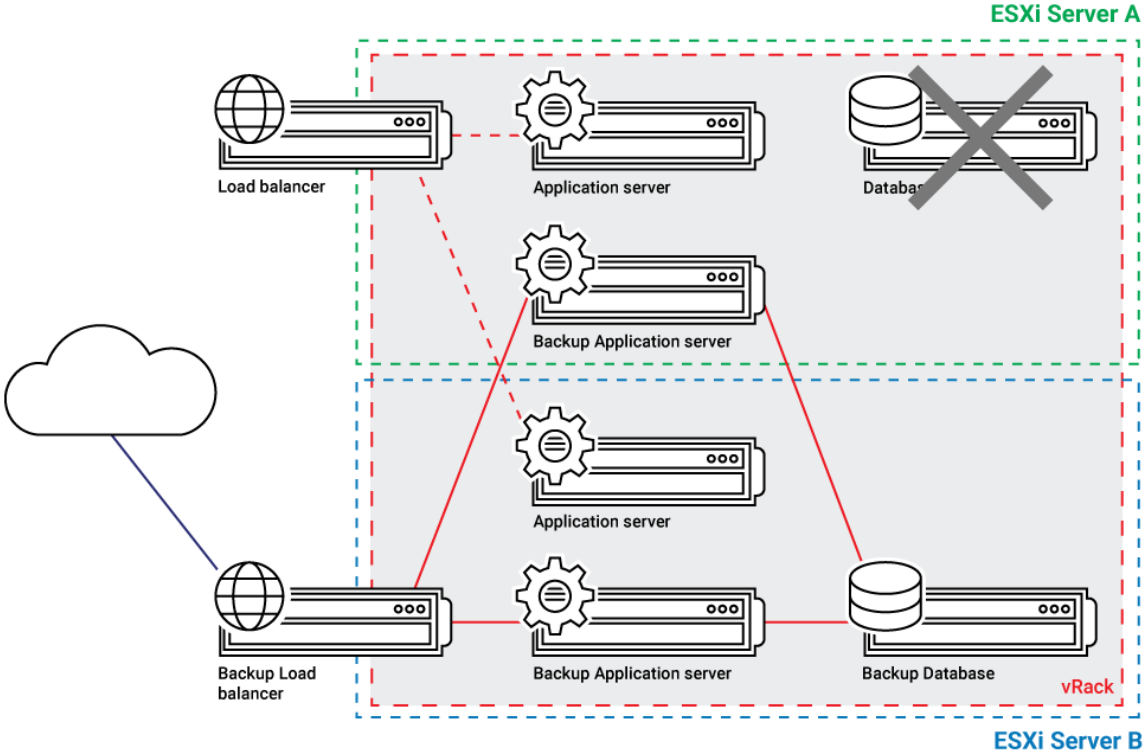
3.2.5 Application Server Failure



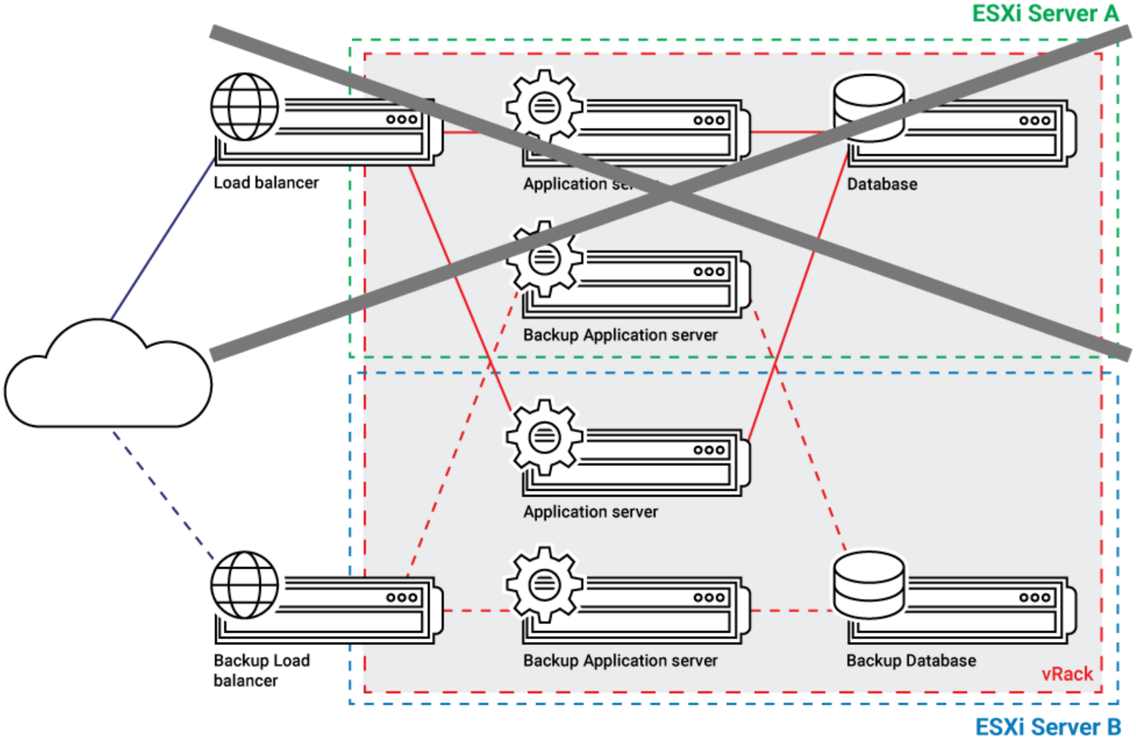

ESXi Server A
Load balancer
Application server
Database
Backup Application server
Application server
Backup Load balancer
Backup Application server
Backup Database
vRack
ESXi Server B

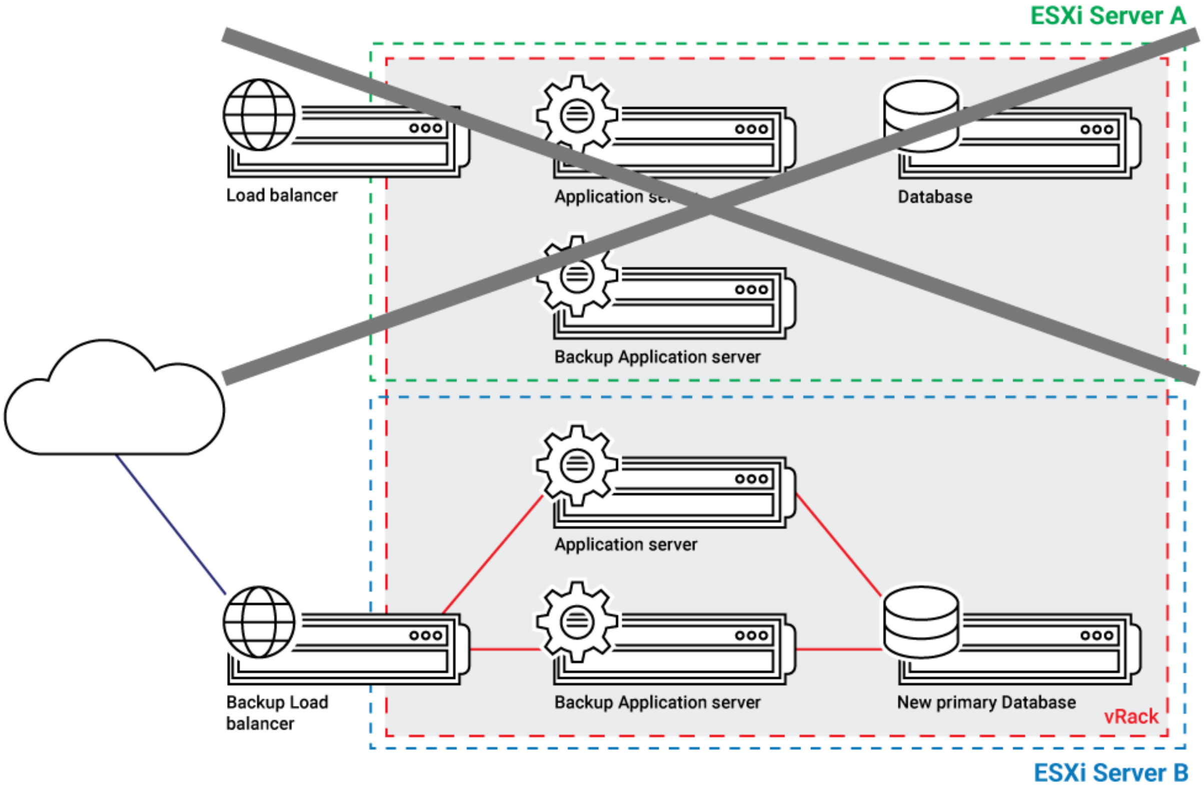
3.2.6 Database Server Failure





3.2.7 Primary Server Failure





4 Backup Strategy

4.1 Regular VM snapshots

A regular weekly snapshot has to be taken for all VM in use.

4.2 Regular Export to a File

In addition to snapshots, an export of every VM in use should be done as per server categorization. Mission-critical servers should be exported regularly. The continuation of the business requirements determines the frequency of the export.

In other words, in a total disaster and all data on disks are lost, recovery should be possible in a reasonable amount of time to continue without significant loss of data or functionality after the restoration is completed.

Since the Virtual machine has to be shut down to be exported, this activity should be planned, and the team should be notified. The export operations should happen during less active hours (usually on the weekends and late in the evenings).

1. Export of the VMs should be done on disks other than disks where VM is running
2. All export files have to have a date of export in their file names
3. If several exports are done on the same day, then time should be added to the file name
4. All crucial exports have to be verified by importing an export file to another physical server
5. The standard location for the exported files should be multiple separate backup servers

4.3 Data Backup

In addition to backup of the virtual machines, a selected set of data should be regularly backed up:

1. SVN repositories (using SVN ***svnadmin dump*** command)
2. Database exports (using PostgreSQL ***pg_dump*** command)
3. Important configuration files (e.g., router configuration file, web server configuration files, etc.)
4. Software
5. Archives

4.4 Automatization

Virtual Box has an extensive API that allows automatization of the snapshots and exports.

VMware OVF Tool is a command-line utility that allows you to import and export OVF packages to and from many VMware products.

Any frequent task should be automated if possible.
The file backup process should also be automated.

4.5 Remove Old Backup Files

To save disk space, create space for new backups, delete old backup files, and be careful not to delete files before export is taken.

1. Export VM -> ***example.ovf***
2. Delete ***example.ovf.old***
3. Remove old/deleted export files from Backup Files List Inventory

4.6 Database Backup

4.6.1 Backup Locations

Location Name	URL/IP	Description	Retention (default)
YouTestMe Backup Server		Main Backup Storage with restricted access	30 days
OVH FTP Server		Secure FTP server for backups provided with each dedicated server from OVH	30 days
Local Storage		Separate disk/partition on the production server for instant database restore	30 days
Standby database		Keeps the user data replicated in real-time	

4.6.2 Creating Daily Database Backups

SVN backup script location:

https://svn.youtestme.com/scm/svn/res/trunk/Scripts/Unix/util/postgres/customer_database_backup/database_backup_wrapper.sh

1. Script execution is scheduled via a crontab job
2. The following directory, “${HOME}/env” stores a configuration file “*db-backup.cfg*” that contains all relevant backup information: a storage location, backup frequency, retention period, etc.
3. Linux command that triggers database backup operation:

```
./database_backup_wrapper.sh  db-backup.cfg
```

5 Restore Strategy

5.1 Test Backed up Files

The export of all VMs should be tested at least once. For Mission-Critical Machines, the export file should be tested more frequently, at least every third export, until we reach a comfort level regarding the backup procedure.

Care should be taken when testing export files - when a machine is restored from backup and started, the IP address might conflict with the original one. For that reason, the MAC address should be changed before VM is started, and the IP address should be changed immediately after the machine is started.

5.2 Database Restore

SVN script location:
https://svn.youtestme.com/scm/svn/res/trunk/Scripts/Unix/util/postgres/ytm_pg_load_client_backup.sh
Requirements:

- Access to backup storage servers
- PostgreSQL database

Loading steps:

1. Open the configuration file and specify values for the following variables:
   - **BACKUP_SERVER** – IP address of YTM Backup Storage server (can be found on Passbolt)
   - **DB_NAME** – target database in which client's schema will be loaded. If the database doesn't exist, it will be created. If the database exists, it will create the schema. If the database and schema exist, the schema will be overwritten.
   - **HOST -** IP/URL of the database to import schema
   - **PORT** - target database port (default is 5432)
   - **CLIENT** – name of client instance (subdomain). List of clients can be presented by running:
     ```
     ./ytm_pg_load_client_backup.sh config_file.cfg --list
     ```
   - **DATE** - backup date in format YYYY-MM-DD
   - **PGPASSWORD** – password for PostgreSQL superuser
2. Run the script with config file as argument (user data are scrambled):
   ```
   ./ytm_pg_load_client_backup.sh config_file.cfg
   ```
3. Run the script with additional argument to disable data scrambling:
   ```
   ./ytm_pg_load_client_backup.sh config_file.cfg –no-scramble
   ```

5.3 Bugzilla - Restore Data from Backup

1. Copy tar.gz. files from the backup location to Bugzilla VM
2. Extract data from a file:
   ```
   tar xzvf bugzilla-backup-*.tar.gz
   ```
3. Create a user and database named “***bugs***” if they don’t exist. If they exist, drop the old database and create a new one. Database password can be found on Passbolt, but also in the file: ***/var/lib/bugzilla5/localconfig***
4. Import database:
   ```
   mysql -u bugs -p -d bugs < path/to/exported/*.sql
   ```
5. Restart Apache Web server:
   ```
   systemctl restart httpd.service
   ```

5.4 Passbolt Recovery Procedure

The password management service should be available to the team despite any disaster that can hit the hosting infrastructure.

When the primary server fails, it is necessary to activate the Cold Standby Server.

The primary database is backed up every day, and the backup files are stored in multiple secure locations.

5.4.1 Activate Cold Standby Site

The password required for SSH connection to Standby Server was sent by email to SA team members.

1. Change DNS settings for the subdomain **passbolt.youtestme.com** to point to the Proxy server's IP address in front of the Standby Server.
2. Inform the YouTestMe team that the Passbolt recovery procedure is in progress

Restore script is running every day after the database is backed up. The procedure for manually starting the restore script is following:

1. SSH to the Standby Machine
2. Switch to ***root*** user
3. Execute the following bash script:
   /root/scripts/restore_db_from_backup.sh
4. Clear the cache in your favorite browser and try to access the fresh activated Passbolt server using the same URL: ***passbolt.youtestme.com***

DNS propagation delay can vary, but its average duration is about 30 minutes.

The main Passbolt server should be activated as soon as possible. If the main server can’t be reactivated, the Standby server becomes the main server.

5.4.2 Checking Standby Site

The standby site should be checked every three months.

Date	Tester	Status	Comment

5.5 SVN Data Recovery

Physical Server Geolocation	**Toronto, Canada**
Backup server storing dump files	Name: **ytm-SVN-backup** (access via a proxy server)
Backup script SVN location	https://svn.youtestme.com/scm/svn/res/trunk/Scripts/Unix/util/SVN-scripts/dump_all_repos.sh
Description	Running every day at 23:00 UTC, saving the last 15 repositories' backups
Dump Files System Path	/ytm-storage/svn-backup/

5.5.1 Loading Files from Backup

1. Login to standby server (SCM-manager installed) as root using SSH or VMware client software
2. Copy dump files from Backup Server using some FTP client.
3. Create repository on SCM server if it doesn't exist or delete old repository and recreate it:
   ```
   svnadmin create /var/lib/scm/repositories/svn/$REPO
   ```
4. Load dump file in new repo:
   ```
   svnadmin load /var/lib/scm/repositories/svn/$REPO/ --force-uuid <
   "$REPO"*.dump
   ```
5. Repeat the previous step for all dump files
6. Change ownership for all repositories:
   ```
   chown -R scm:scm /var/lib/scm/repositories/svn/*
   ```