

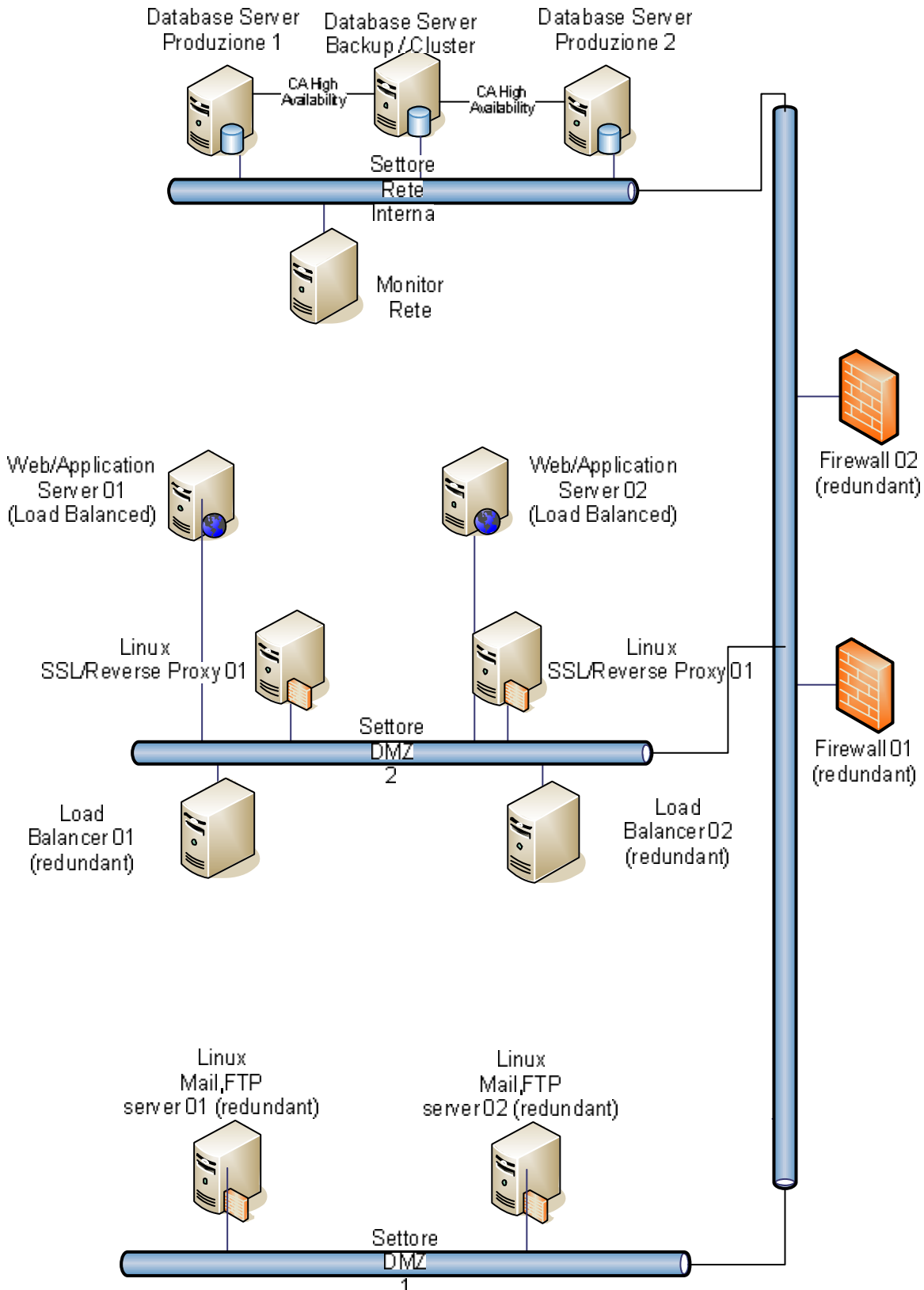
Architettura WebFarm

RD Sistemi per erogazione servizi in modalità ASP

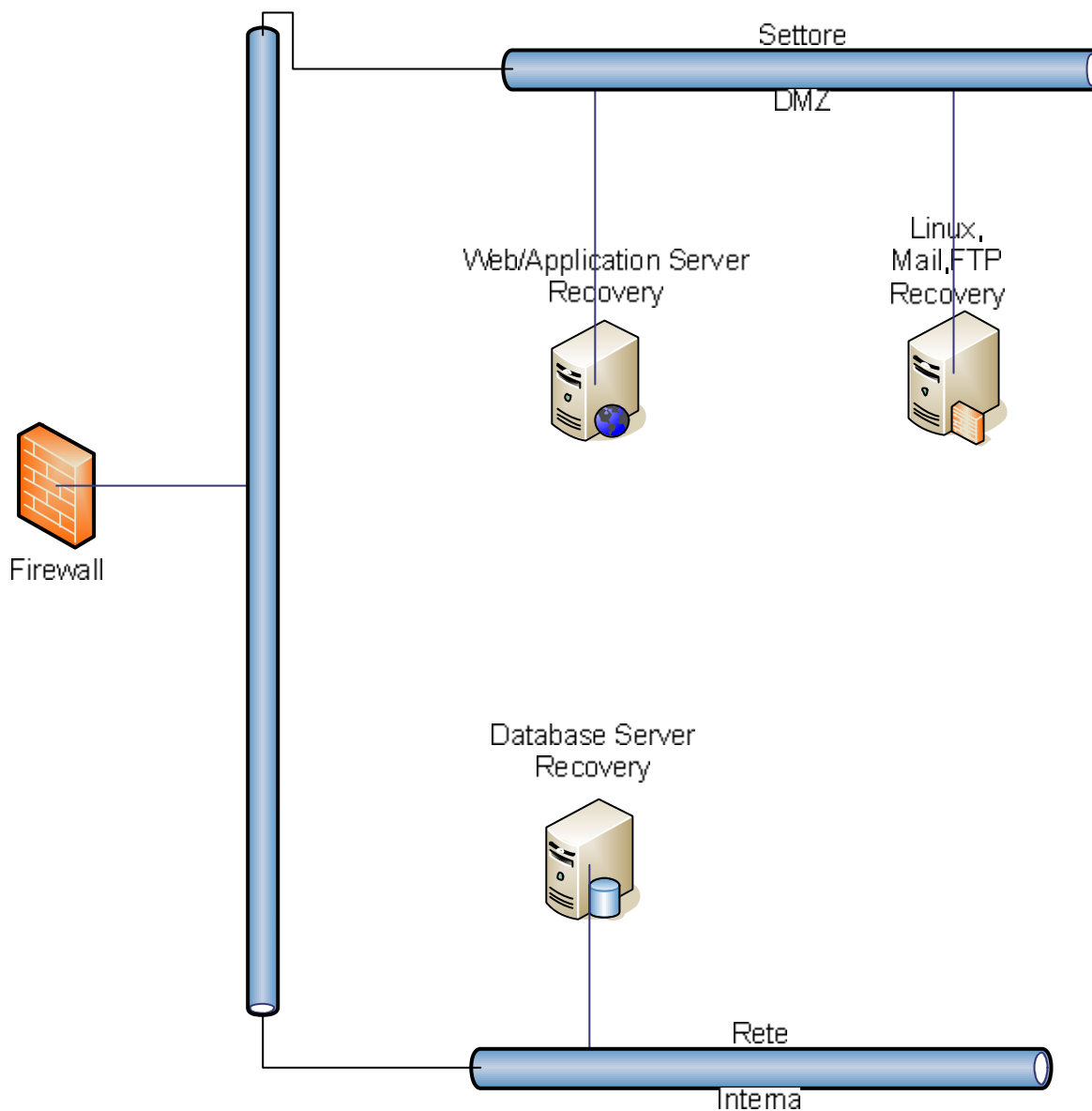
Indice

1. DIAGRAMMA ARCHITETTURA DI RETE WEBFARM PRINCIPALE	2
2. DIAGRAMMA ARCHITETTURA DI RETE WEBFARM SECONDARIA	3
3. CONFIGURAZIONE DEI SISTEMI NELLA WEBFARM PRINCIPALE	4
4. CONFIGURAZIONE HARDWARE DELLE MACCHINE IN WEBFARM PRINCIPALE	5
5. CONFIGURAZIONE HARDWARE DELLE MACCHINE IN WEBFARM SECONDARIA	6
6. FUNZIONAMENTO DEI SISTEMI DI BACKUP	7
7. BACKUP AGGIUNTIVO DATABASES	8
8. GARANZIA DEI DATI	9
WEB SERVER:	9
DB SERVER:	9

1. DIAGRAMMA ARCHITETTURA DI RETE WEBFARM PRINCIPALE



2. DIAGRAMMA ARCHITETTURA DI RETE WEBFARM SECONDARIA



3. CONFIGURAZIONE DEI SISTEMI NELLA WEBFARM PRINCIPALE

Tutti i sistemi presenti nella WebFarm principale sono duplicati in maniera di avere la massima garanzia di funzionamento nel caso un componente della rete dovesse avere problemi.

In particolare sono presenti:

- 2 Firewall CISCO in Fail-Over. Nel caso in cui il firewall principale dovessero avere qualunque tipo di problema, il firewall secondario subentra in maniera immediata e totalmente automatica.
- 2 Switch di rete CISCO in Fail-Over, per il collegamento dei Firewall con le DMZ e la rete interna. Anche in questo caso, se uno dei due switch di rete dovesse avere un problema, l'altro subentra in maniera immediata e totalmente automatica.

La rete è suddivisa in due reti DMZ (DMZ1 e DMZ2) separate a livello di VLAN e una rete interna. Nella rete interna, sono presenti altri 2 Switch di rete CISCO in Fail-Over, per garantire la continuità della rete interna a prescindere dalle apparecchiature esposte verso il mondo esterno.

- Configurazione DMZ1:
 - 2 Server LINUX per la gestione di MAIL e FTP.
I due Server sono in configurazione High Availability. Il file system delle due macchine è sempre allineato e nel caso di caduta di una delle due macchine, l'altra la sostituisce immediatamente ed in maniera totalmente automatica.
- Configurazione DMZ2:
 - 2 Server LINUX con la funzione di bilanciatori di carico verso i server WEB.
Il traffico non viene indirizzato direttamente ai server WEB, ma è inoltrato a dei REVERSE PROXY.
 - 2 Server LINUX con la funzione di REVERSE PROXY e crittografia SSL .
I REVERSE PROXY sono in configurazione 1 a 1 con i WEB Server.
La funzione di queste macchine è quella di filtrare le richieste inviate al WEB Server, eliminando quelle che non soddisfano i criteri di sicurezza impostati (URLSCAN).
Funzionano inoltre da proxy server verso i client per i contenuti statici (immagini, sfondi ecc). Le richieste per questi contenuti vengono soddisfatte quindi dai REVERSE PROXY senza appesantire il WEB Server.
Per ultimo, questi Server effettuano la crittografia SSL a 128bit per rendere la navigazione nelle applicazioni pi sicura.
 - 2 WEB Server che si occupano di rispondere alle richieste degli utenti.

In questa configurazione, è possibile aumentare la capacità di elaborazione del sistema, aggiungendo più coppie WEB Server/REVERSE PROXY. I bilanciatori provvederanno a far giungere richieste ai nuovi server.

- Configurazione Rete Interna:
 - 2 Database Server (SQL SERVER) su cui sono appoggiati i Database di tutte le applicazioni attive nella WebFarm.
I databases sono suddivisi tra i due server in modo da bilanciare il carico di lavoro di entrambi.
Ognuna delle due macchine è sorvegliata da una terza macchina la quale controlla

lo stato di funzionamento dei sistemi ed è in grado di intervenire automaticamente, sostituendosi a quella eventualmente in avaria.

- 1 Backup Database Server, su cui sono appoggiati tutti i Database delle applicazioni attive.

Questa macchina controlla costantemente lo stato delle due macchine principali e in caso di malfunzionamento di una delle due, la sostituisce sostituendola in tutte le funzioni.

- 1 Server per il Monitoraggio delle prestazioni della rete.

Questa macchina effettua continuamente dei test su tutti i server e le apparecchiature di rete presenti in configurazione.

Non appena identifica un problema, invia una segnalazione all'help desk tramite posta elettronica e tramite SMS per maggiore sicurezza.

In caso di failure del Monitor, i server FTP invieranno una segnalazione all'help desk segnalando l'anomalia

Tutti dati presenti nei Database e i servizi web attivi, vengono inoltre replicati in una WebFarm secondaria. Tale struttura è quindi sempre allineata alla struttura principale e pronta ad intervenire in caso di disaster recovery. L'attivazione della struttura secondaria non è immediata, ma richiede l'intervento umano per attivare i servizi e aprire al traffico in ingresso.

La struttura secondaria è studiata per entrare in funzione solo in caso di eventi di eccezionale gravità (distruzione fisica della WebFarm principale).

4. CONFIGURAZIONE HARDWARE DELLE MACCHINE IN WEBFARM PRINCIPALE

Le macchine presenti in WebFarm hanno le seguenti caratteristiche:

- Ognuno dei due Server LINUX per MAIL e FTP è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete
- Ognuno dei due bilanciatori di carico è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete
- Ognuno dei due REVERSE PROXY è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

- Ognuno dei due WEB Server è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - **4 GB** di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

- Ognuno dei due DB Server Principali Server è composto da:
 - 4 hard disk SCSI da 72GB 15000rpm in RAID 5 dei quali 3 attivi ed uno come HOT SPARE.
In caso di malfunzionamento di uno dei dischi, il disco in HOT SPARE subentra automaticamente in sostituzione di quello guasto.
 - Scheda madre biprocessore con 2 Processore XEON 3,6 GHz
 - **6 GB** di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

- Il BACKUP DB Server è composto da:
 - 6 hard disk SCSI da 300GB 10000rpm in RAID 5
 - Scheda madre biprocessore con 2 Processore XEON 3,6 GHz
 - **6 GB** di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

- Il Monitor è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

5. CONFIGURAZIONE HARDWARE DELLE MACCHINE IN WEBFARM SECONDARIA

Le macchine presenti nella WebFarm secondaria hanno le seguenti caratteristiche:

- Il server MAIL/FTP/REVERSE PROXY è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

- Il WEB Server è composto da:
 - Due hard disk SCSI da 72GB 15000rpm in RAID 1 (Mirror)
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz

- 2 GB di memoria RAM
- doppio alimentatore
- doppia scheda di rete

- Il Database Server è composto da:
 - Due hard disk SCSI da 300GB 10000rpm
 - Scheda madre biprocessore con 1 Processore XEON 3,6 GHz
 - 2 GB di memoria RAM
 - doppio alimentatore
 - doppia scheda di rete

6. FUNZIONAMENTO DEI SISTEMI DI BACKUP

Nella configurazione studiata, tutte le apparecchiature di rete (Firewall, Switch, Router) sono ridondanti.

In caso di malfunzionamento di una qualunque delle apparecchiature, un'altra identica e sempre allineata interviene automaticamente in sostituzione.

Un sistema di monitoraggio continuo, verifica lo stato dell'infrastruttura. Nell'eventualità di un problema di qualsiasi natura, il Monitor è in grado di inviare la segnalazione ad un Help Desk competente.

Per assicurare la notifica delle anomalie, al sistema di Monitor è associato un modem GPRS che permette anche in assenza di connessione alla rete di inviare le notifica sotto forma di SMS.

Il Monitor, a sua volta, è tenuto sotto controllo da due macchine che quando il Monitor dovesse per qualunque ragione smettere di interrogare i sistemi di rete, invieranno all'Help Desk la segnalazione di malfunzionamento del Monitor.

Tutte le macchine presenti nelle reti DMZ (Mail e FTP Server, Load Balancer, Reverse Proxy e Web server) hanno dischi in configurazione RAID 1 (Mirror).

In caso di problema su un disco, l'altro è sempre allineato e pronto per il funzionamento. Ovviamente il problema sul disco sarà intercettato dal Monitor che lo segnalerà all'Help Desk.

Tutte le macchine inoltre sono configurate per lavorare a coppie. In caso di avaria di una macchina, l'altra interverrà immediatamente a sostituirla.

I DB Server sono equipaggiati con 4 Dischi SCSI, dei quali 3 in configurazione RAID5 ed il Quarto in HOT SPARE, quindi pronto ad intervenire nel caso uno dei 3 principali subisca un danno. Quindi, ogni macchina può sopportare la rottura di 2 dischi senza perdere i dati.

Dietro ai due DB Server, è presente un BACKUP DB Server, che è sempre allineato con entrambi. Nel caso in cui uno dei due server dovesse entrare in avaria, il BACKUP DB Server subentra non permettendo l'interruzione del servizio.

Non appena il server principale viene ripristinato, il server di Backup ripassa il controllo al principale e si mette di nuovo in attesa.

Tutta la rete della WebFarm è collegata ad una WebFarm secondaria, di minore complessità, studiata per funzionare come Disaster Recovery della principale.

Nel caso di distruzione fisica della WebFarm Principale (a causa di incendio, terremoto o altro), una copia di tutte le applicazioni e dei database è presente nella Webfarm secondaria.

L'attivazione della WebFarm secondaria deve avvenire mediante l'intervento di un operatore che valuti l'effettiva impossibilità di lavorare con la WebFarm principale.

In tal caso, il traffico diretto verso la WebFarm principale viene rediretto verso la secondaria che permetterà la continuazione dell'attività.

7. BACKUP AGGIUNTIVO DATABASES

Oltre alle funzioni di backup e recovery dei sistemi, sia la WebFarm principale che la WebFarm secondaria dispongono di un ulteriore supporto di archiviazione dei dati.

Una funzione di backup notturno, trasferisce una copia di backup di ogni Database su un disco fisso esterno da un Terabyte di capacità.

Su questo disco esterno viene mantenuto anche una copia storica dei backup di ogni ambiente per un periodo di tempo di 1 mese.

Oltre ai dati, vengono memorizzati ogni notte anche gli script contenenti la struttura di tabelle, viste e procedure.

8. GARANZIA DEI DATI

Con quanto esposto in precedenza, diamo un esempio di danni possibili alle macchine e quali conseguenze possono derivarne:

WEB SERVER:

- Rottura di un Hard Disk
 - Interviene il secondo disco. Nessun downtime
- Rottura di entrambi gli Hard disk di una macchina Web Server
 - Il load balancer sposta tutto il carico di lavoro sulle macchine rimanenti (Nessun downtime; possibile perdita di performance; caduta delle sessioni utente connesse alla macchina in fault)
- Rottura di una scheda di rete di una macchina Web Server
 - L'attività continua sulla seconda scheda di rete (Nessun downtime)
- Rottura di entrambe le schede di rete di una macchina Web Server
 - Il load balancer sposta tutto il carico di lavoro sulle macchine rimanenti (Nessun downtime; possibile perdita di performance; caduta delle sessioni utente connesse alla macchina in fault)
- Rottura di un alimentatore
 - Interviene il secondo alimentatore
- Rottura di entrambi gli alimentatori
 - Il load balancer sposta tutto il carico di lavoro sulle macchine rimanenti (Nessun downtime; possibile perdita di performance; caduta delle sessioni utente connesse alla macchina in fault)

DB SERVER:

Per i DB Server valgono tutte le caratteristiche di sicurezza viste per le macchine WEB dal punto di vista di schede di rete e alimentatori.

Analizziamo invece la sicurezza dei dati:

- Rottura di un Hard Disk
 - Interviene il quarto disco (Hot Spare) (Nessun Downtime e nessun degrado prestazionale)
- Rottura di 2 Hard Disk
 - Essendo in configurazione RAID5, i due dischi rimanenti continuano a lavorare. (Nessun Downtime, possibile degrado prestazionale)
- Rottura di 3 Hard Disk
 - Tutto il carico elaborativo viene spostato sul Server DB di Backup (sempre allineato e pronto). Il server di Backup è dotato di 6 HD in configurazione RAID5. E' quindi ampiamente in grado di sostenere il carico del server in errore. (Downtime di circa 3 minuti; Nessun degrado prestazionale)

In sostanza, perché i server non siano in grado di rispondere si devono rompere:

- Almeno 3 Hard Disk sul DB Server Principale
- Almeno 3 Hard Disk sul DB Server Secondario

Anche in questa eventualità, esiste una copia dei dati sul disco fisso esterno aggiornato alla notte precedente.

Nel caso di calamità naturale, incendio grave o comunque in caso di distruzione della WebFarm (ipotizzando quindi che non siano recuperabili ne' i dischi dei Server ne' i dischi esterni di Backup), esiste una copia dei DB nella WebFarm Secondaria (geograficamente distante dalla principale).

In questa ipotesi servirà del tempo per fare in modo che tutto il traffico sia rediretto alla WebFarm secondaria, ma sia gli applicativi che i DB sono allineati.