SISTEMI CENTRALI (2)
Anno Accademico 2023-24

Docente: Fabrizio Messina

SISTEMI CENTRALI – LEZIONE 2

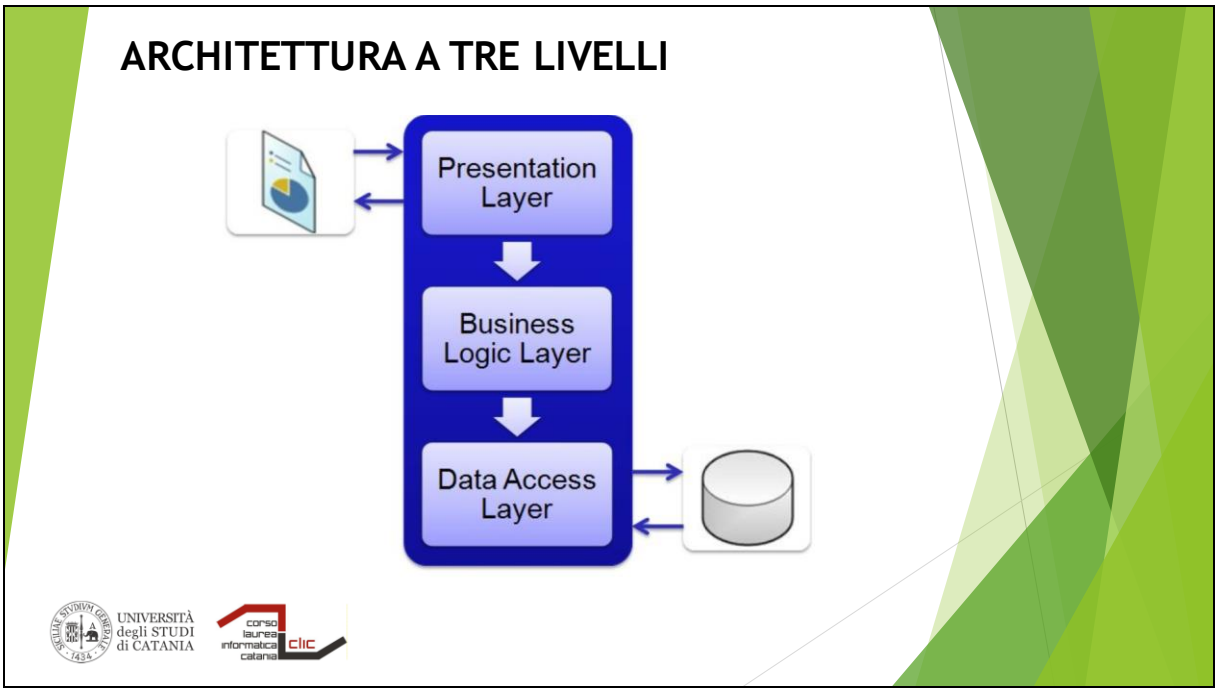
PRIMA PARTE
- Architettura a tre livelli

SECONDA PARTE
- Continuità Operativa e Scalabilità
- Alta affidabilità (High Availability)
- Clusters
- Bilanciatori di carico e load balancing
  - Politiche di bilanciamento
- Scalabilità orizzontale e verticale
- Ridondanza dei dischi (RAID)
- Altri punti di vulnerabilità (single point of failure)
- Backup e recovery
- Disaster Recovery

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic catania

PRIMA PARTE



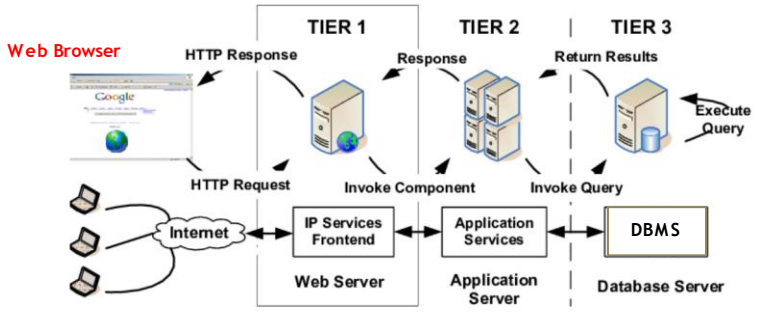
- **Livello di presentazione (presentation layer).** Il livello di presentazione interagisce con il client e la parte applicativa; prepara e mostra le informazioni relative alle richieste utente. Comunica con altri livelli inoltrando le richieste browser/client e ricevendo le risposte.

- **Livello applicazione** (**business logic layer).** Esegue le funzionalità di business. A questo livello girano i programmi applicativi, che ricevono le richieste utente, elaborano i dati letti e scritti sul database o sui file. Prepara ed inoltra le query al server i database.

- **Livello dati (Data access layer)** A questo livello opera il database server, che memorizza e recupera. Il Database Management Server (DBMS) consente di disegnare la struttura dei dati e la relazione tra di essi e gestisce gli accessi. Nasconde la logica dei dati alle da applicazioni di business.

Opzionale: https://it.wikipedia.org/wiki/Architettura_multi-tier

ARCHITETTURA A TRE LIVELLI



Vedi Note

Il **web browser** rappresenta il livello di interfaccia utente (UI) dell'applicazione. Gestisce la creazione dell'UI e supporta client-side scripting (ad es. JavaScript). Nel corso del tempo sono stati adottati meccanismi per estendere le funzionalità, quali Java Applets, Plug-ins per Netscape, o ActiveX Controls per Internet Explorer (ormai obsolete e ritirate da Microsoft).
Comunica tramite connessione non sicura (HTTP) oppure sicura perchè encrypted (HTTPS, con SSL).
I browser supportano vari tipi di applicazioni, tra cui email.

Il web server è un applicativo software che gira su di un server fisico in ascolto su porte dedicate, per comunicare con i client che richiedono i suoi contenuti ed i suoi servizi.
Un web server dialoga con una gran varietà di client utilizzando dei *protocolli* riconosciuti da tutti. Quello principale per la navigazione web è l'**HTTP** (**Hyper Text Transfer Protocol**).
Il browser traduce l'indirizzo URL in una **richiesta http** e la consegna al web server indicato. Riceve poi da questo una risposta http e visualizzato (*rendering*) sotto forma di testo e immagini a video.

Il web server riceve tipicamente uno o piu' file f**iles HTML** che viene interpretato opportunamente.
HTML è il linguaggio per costruire i siti web. E' un **markup language,** cioè contiene parti che

sono usate per descrivere il contenuto più il contenuto stesso. La versione più recente è **HTML5** del Gennaio 2008, rivisto nel 2014. **World Wide Web Consortium** (**W3C**) l'organizzazione internazionale principale degli standard per il World Wide Web.

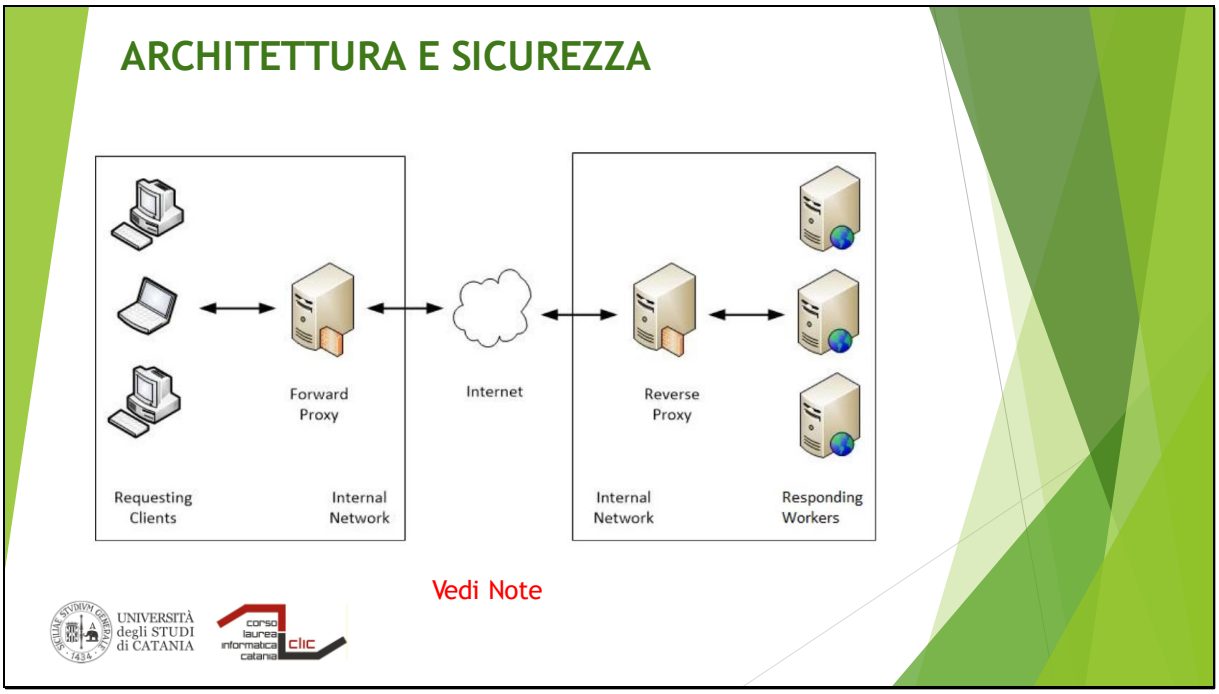
Le pagine web possono essere sia *statiche* che *dinamiche*.

La **pagine statiche** sono scritte solamente con codice HTML e al loro interno contengono già tutti i dati che verranno poi mostrati all'utente finale.
Le **pagine dinamiche**, invece, oltre ad HTML usano altri linguaggi (PHP, ASP, ecc..) attraverso i quali sono definite delle istruzioni che generano il contenuto della pagina richiesta. In questo caso è il web server a processare queste istruzioni (presenti sotto forma di script), mostrando all'utente finale i contenuti generati dinamicamente con l'aspetto predefinito dal programmatore.

Il **Web Browser** è interpreta le pagine HTML e visualizza la pagina in formato ipertesto.
Il Web Browser (anche 'browser') rappresenta il sistema software di interfacciamento dell'utente con la rete che rende la navigazione dell'utente user-friendly
I browser vengono utilizzati su personal computer, i palmari e gli smartphone. Quelli più noti e diffusi sono Microsoft Edge, Mozilla Firefox, Google Chrome, Safari e Opera. Ancora in uso anche se ormai obsoleto è Microsoft Internet Explorer che però sopravvive in azienda dove siano ancora in uso applicazioni che facciano uso degli ActiveX.

Application server. Ospita ed espone la logica e i processi aziendali. Il server funge fondamentalmente da intermediario tra il server del database e il server web. Ciò consente alle informazioni estratte di essere incorporate in una pagina HTML particolare e personalizzata; questo non è un processo riutilizzabile. Un secondo cliente dovrà richiedere nuovamente le informazioni e ricevere un'altra pagina HTML incorporata con le informazioni richieste. Questo tipo di server è molto flessibile grazie alla sua capacità di gestire le proprie risorse, inclusa la sicurezza, l'elaborazione delle transazioni, la messaggistica e il pool di risorse.

Database server. E' il server su cui è ospitato il servizio di DBMS, e per estensione il **server** su cui il programma opera, che si occupa di fornire i servizi di utilizzo della base di dati ad altri programmi e ad altri computer secondo la modalità client/server.



Forward Proxy
Il proxy server è situato tra i browser e rete Internet. Il browser si rivolge al Proxy invece che alla rete; sarà poi il proxy a svolgere tale operazione.

Questa opzione garantisce tra l'altro la possibilità di effettuare un **caching dei contenuti**. Se tutti i browser della rete interna visitano www.google.com, i contenuti che possono essere tenuti nella **cache del proxy** non dovranno essere richiesti al sito di destinazione co i due vantaggi:

1. **Performance:** meno dati sono scaricati dalla rete.
2. **Costi**: nel caso la fatturazione avvenga per soglie di traffico

Inoltre il **proxy può effettuare filtri alla possibilità data agli utenti** di uscire dalla rete aziendale e a quali siti accedere

Il Proxy implementa politiche di **caching passivo o attivo**
Con il caching passivo una pagina acceduta viene memorizzata in cache con politiche predeterminate.
Con il caching attivo, nei periodi di basso carico il proxy interroga i server di Internet per rinfrescare la sua cache.

Solo a titolo informativo, i proxy scambiano informazioni tra di loro usando protocolli di comunicazione, per decidere quali pagine devono essere memorizzate.
I protocolli sono **Internat Cache Protocol (ICP)** descritto nella RFC 2168 e 2187 ed il **Cache Array Routing Protocol (CARP):** quest'ultimo utilizza un array di cache distribuite tra più server

Reverse Proxy
Può essere installato alle spalle di un firewall o essere esso stesso un firewall a livello applicazione; svolge tre funzioni diverse:

- **Sicurezza**: Maschera i veri indirizzi di rete al mondo esterno. In questo modo non può essere attaccato un server con il suo indirizzo
- **Bilanciamento di carico**: può indirizzare diversi tipi di richieste ad application server specifici (ad es. Pagine statiche ad un server, dinamiche ad un altro)
- **Caching**: come nel caso del forward proxy

SECONDA PARTE

Continuità Operativa e Scalabilità

UN SISTEMA APPLICATIVO DEVE GARANTIRE:

- **Continuità Operativa** – Guasti hardware, malfunzionamenti del software, errori umani **non devono interrompere la disponibilità del sistema** per una **durata che diventi critica** per le necessità operative
- **Scalabilità** – Il sistema deve essere sufficiente a supportare il carico di lavoro e deve essere possibile adeguarlo alle aumentate esigenze di carico
  - Scale up
  - Scale down

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

La continuità operativà deve garantisce che:

- **Il sistema rimanga disponibile anche a fronte di eventi distruttivi**: guasto, errore umano, attacco deliberato
- **Il tempo di indisponibilità durante l'evento sia minimo** e stimabile a priori
- Sia garantita **la salvaguardia dei dati aziendali**

- La **scalabilità** consiste nella possibilità di adeguare la capacità elaborativa ad un livello di carico crescente
- In Inglese si definisce Scalability. Scale up è l'aumento della capacità. Scale down è l'inverso

High Availability (HA)

Come **Alta Affidabilità**, d'ora in poi indicata come **High Availability** (HA) si intende:

- Il servizio applicativo ed i suoi dati sono disponibili all'utente finale con un tempo di fermo imprevisto (**minimal unplanned downtime**) **che sia minimo.**
- La caratteristica di HA di un'applicazione è di solito definita come **percentuale di disponibilità in un intervallo di tempo.**
- Un'applicazione HA deve avere di solito **almeno il 90% di disponibilità (misurato nei 30 giorni).**
- Al crescere del tempo di disponibilità i costi aumentano in modo esponenziale

Vedi Note

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic catania

Confrontare con - **Scalable Service – Load Balancing**

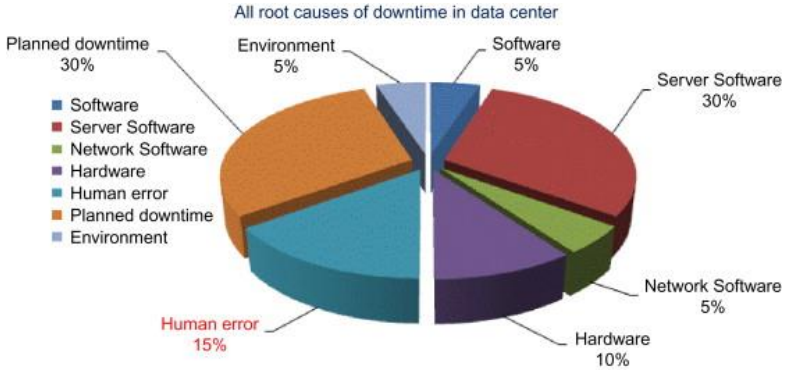
L'obiettivo è di raggiungere un livello del 99.999% di availability (uptime).
Traducendo questo valore di uptime in un periodo di 30 giorni si ottiene:

- 95% equivale a 684 ore di uptime e 36 ore di downtime in un periodo di 30 giorni
- 99% equivale a 712.8 ore di uptime e 7.2 ore di downtime in un periodo di 30 giorni
- 99.9% equivale a 719.28 ore di uptime e 1.72 ore di downtime in un periodo di 30 giorni
- 99.99% equivale a 719.928 ore di uptime e 0.072 ore di downtime in un periodo di 30 giorni
- 99.999% availability vuol dire 719.9928 ore uptime e 0.0072 o 25.92 secondi downtime in un periodo di 30 giorni

Livelli di disponiblità superiori al 99% sono di solito richiesti pee la applicazioni «***mission critical***» ovvero applicazioni che soddisfano necessità cruciali per la vita aziendale

High Availability (HA)

Lo schema mostra una distribuzione delle cause di downtime **(70% unplanned/imprevisto!!) :**



Vedi Note

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Si osserva che il 70% del downtime è unplanned. Le cause sono varie:

- Software defects - 40%
- Hardware defects - 10%
- Errore umano - 15%
- Cause esterne all'ambiente applicativo - 5%
- Network - <1%
- Client application (PC or laptop error) – <1%

Una soluzione di HA deve essere in grado di fronteggiare problemi causati da uno o più dei casi precedenti e mitigarne gli effetti in caso si verifichino

HA - Topologie e tecnologia

L'HA si deve occupare di due aspetti:

- **Disponibilità dei processi** (es. DBMS), che devono essere:
  1. **Attivi** (il processo deve essere attivo)
  2. **Accessibili** (disponibilita'/raggiungibilita' del server)
- **Disponibilità dei dati:**
  1. **Dati applicativi!**
  2. **File di sistema** (file riservati all'applicazione)

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Non solo deve essere disponibilie il server fisico ma anche il «processo».

Ad esempio, se il DBMS gira come uno dei vari processi attivi su di un server fisico, il sistema HA deve garantire la disponibilità del servizio DB.

Quindi se il processo DB cade, il DBMS diventerà indisponibile anche se il server fisico è attivo ed accessibile in rete.

Un applicativo utilizza file riservati di sistema per funzionare, oltre ad accedere ai dati applicativi. Se questi file di sistemi diventano inaccessibile,il sistema sarà bloccato indipendentemente dalla disponibilità di tutto il resto

HA - Continuità dei processi

Le tecnologie in uso per la continuità dei processi sono:

- Target/goal: **Failover Services**
  - ✓ --> Failover **clusters**
- Target/goal: **Scalable Services**
  - ✓ --> **Load balancing**

HA - Continuità dei dati

Le tecnologie in uso per la disponibilità dei dati sono:

Il goal e' la "Data resilience" (ovvero continuità dei dati).

- Resilient disk storage
- Data replication

Vedi Note

Poichè la Data integrity è vitale, esamineremo nel seguito le forme di Resilient Disk Storage e data replication (ad esempio dischi RAID)

HA - Failover services

- **Esiste una sola istanza del processo attiva ad un certo istante**
- Failover service girano su di un cluster
- Riavviati automaticamente su un nodo attivo
- Servizio switched o "failed-over" ad un altro nodo:
  - ✓ Automatico
  - ✓ Trasparente all'utente
  - ✓ Non richiede riconfigurazione client

Vedi Note

Failover services girano su di un cluster e possono essere riavviati (restarted automatically) sulla macchina attiva se la macchina iniziale è indisponibile

Possono essere utilizzati solo se esiste un'istanza singola del processo attiva ad un certo istante, cioè lo stesso Servizio non gira simultaneamente su più machine. Un esempio è sempre il DBMS. Un solo DBMS serve la/le applicazioni. Quindi se cade deve essere riavviato.

In caso di failure, il Servizio migra (switched or "failed-over") su un server differente

Il Failover deve essere **automatico**, non è richiesto intervento operatore.

Il Failover **deve essere trasparente** per gli utenti e non va richiesta la riconfigurazione del client.

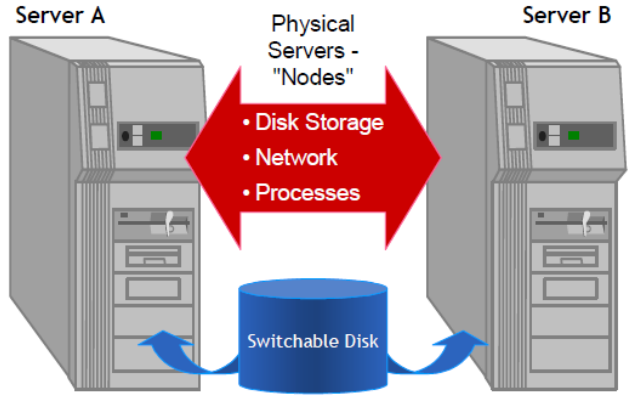
Failover vs Switchover

- Nel failover lo ``switch`` avviene automaticamente
  - Downtime ridotto al minimo
- Switchover -- > switch manuale
  - Breve periodo di downtime

Vedi Note

Cluster per HA [4]

Un cluster a due nodi:



Vedi Note

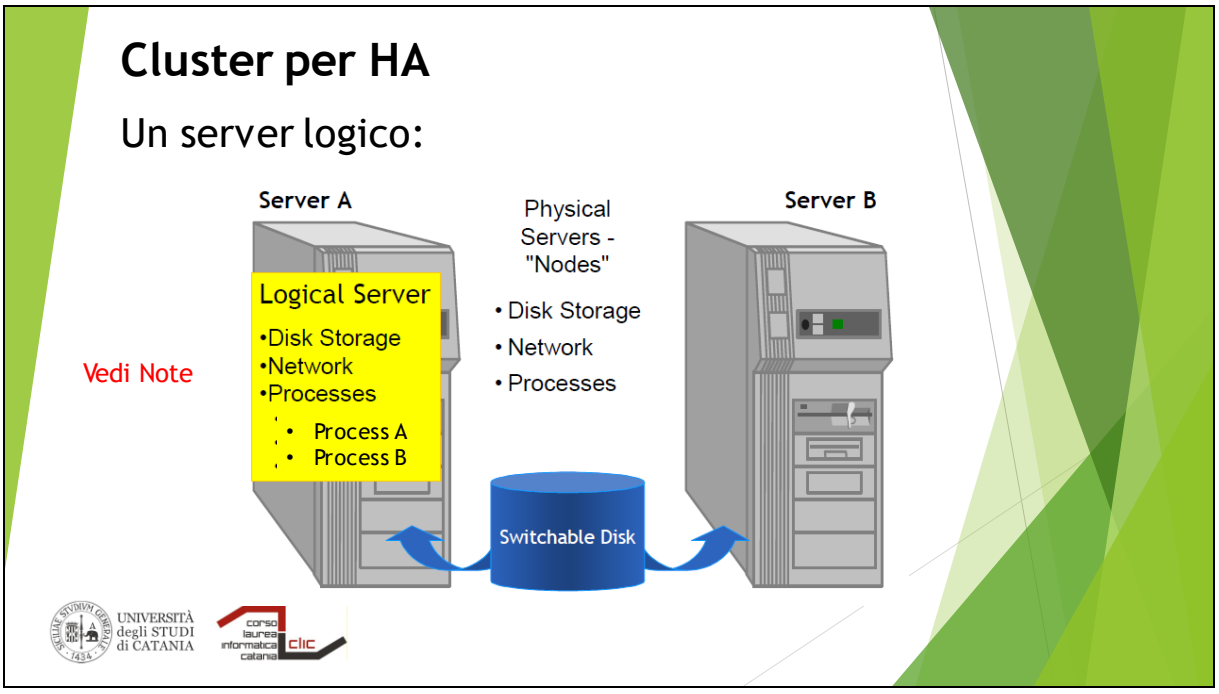
Componenti di un cluster.

Il **cluster** si compone di duo o più server fisici, definiti **nodi.**

Inoltre esiste un **software di gestione (cluster framework)** delle risorse **del cluster**.

Nella figura si vede che ogni nodo dispone di risorse quali il sistema operativo, disco e connettività di rete.

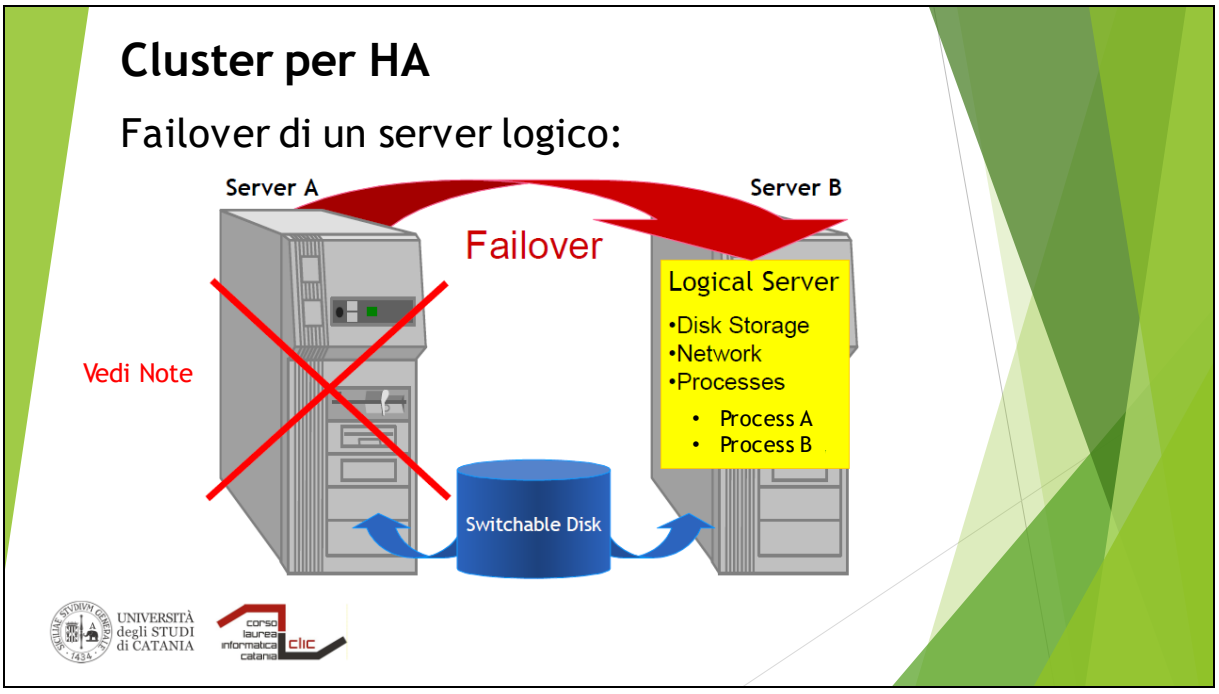
In un ambiente in cluster a queste risorse si aggiungono i **server logici**



Un **server logico** è un **raggruppamento di risorse che appare come un server fisico separato**. Tipicamente include spazio disco, un nome ed indirizzo di rete e dei processi attivi.

La differenza chiave è che **i server logici non sono legati ad un server fisico ma possono girare su di un qualsiasi nodo del cluster**.

Vediamo come si comporta il server logico che ospita i processi A e B in figura

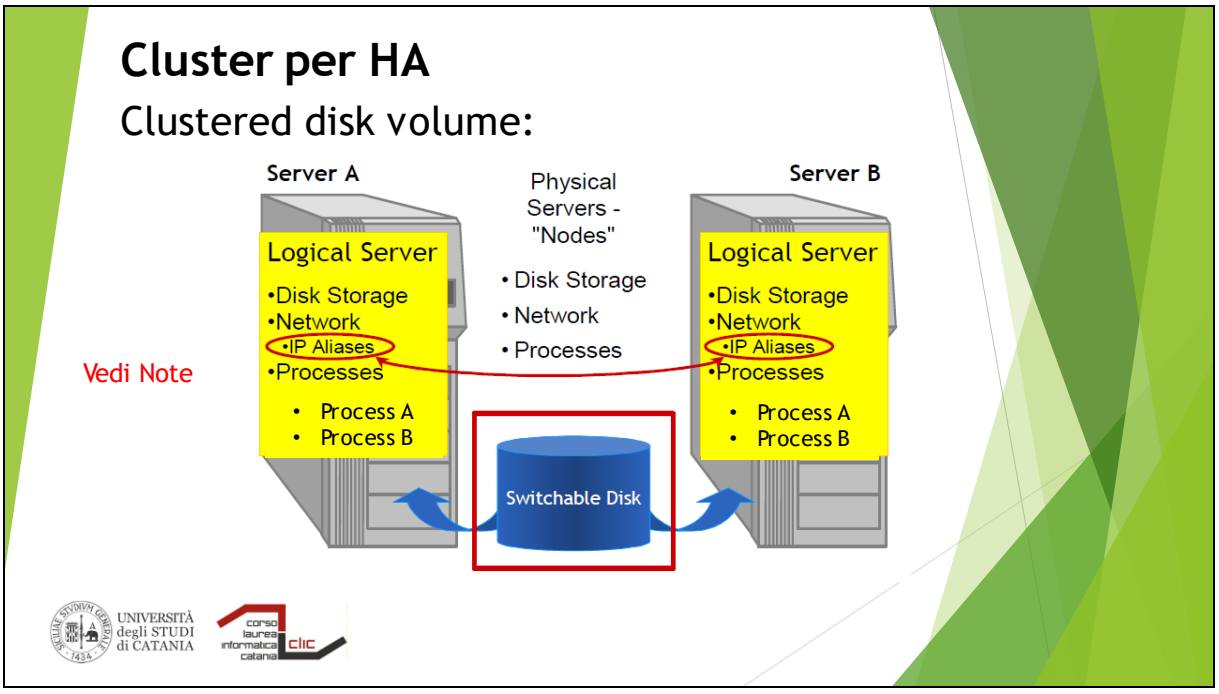


Se avviene un malfunzionamento hardware o software sul Server/Nodo A, il cluster framework rileverà la condizione anomala. Il server logico sarà spostato sull'altro nodo fisico, cioè il Server/Nodo B.

L 'utilizzo di indirizzi IP multipli su una connessione di rete è chiamato genericamente **IP Alias.**

Il concetto fondamentale e' che si fa uso di meccanismi che permettano di associare al server di failover l'indirizzo IP che era in uso sul server, ovvero di configurare entrambi server con gli stessi indirizzi IP.

Quindi Lo stesso indirizzo IP e hostname che era usato per il server logico quando girava sul nodo A è anche configurato sul nodo B. L' IP alias consente di spostare un server logico ad un server fisico differente. Nell'esempio i processi A e B continueranno a girare sul server B

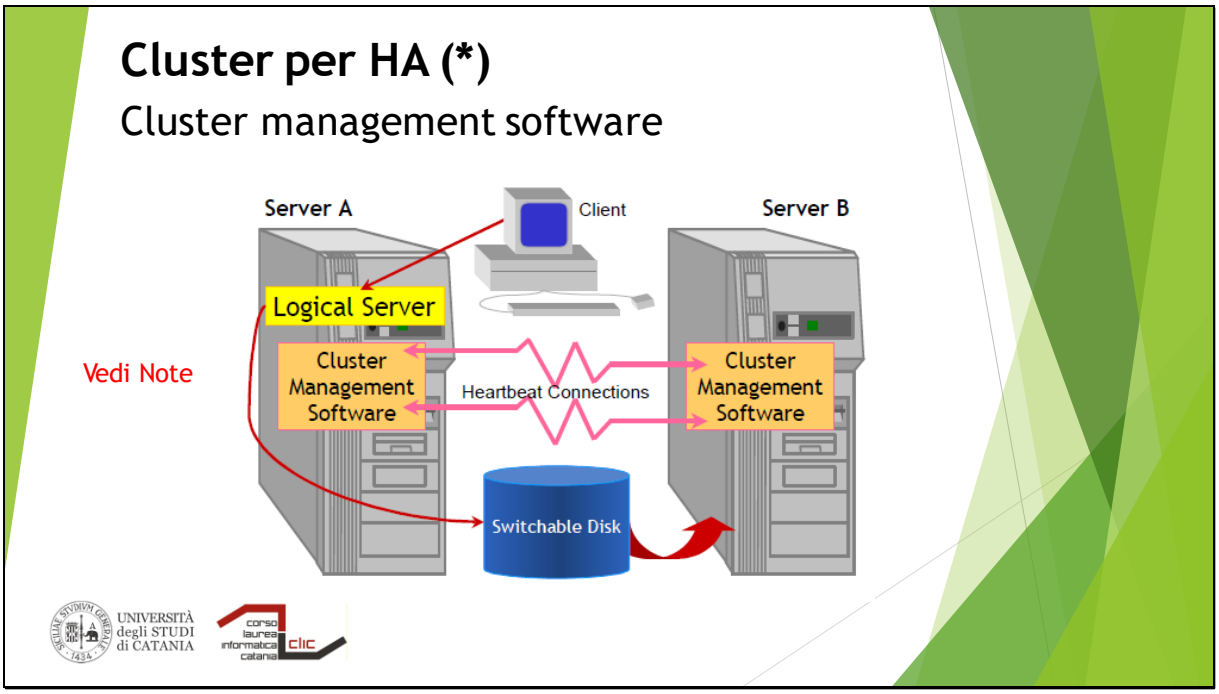


Un **requisito fondamentale** di un cluster per la gestione del failover è l'esistenza di **un volume di dischi condiviso ed accessibile da tutti i server del cluster.**

Di solito solo un server alla volta accede al volume condiviso.

Se il server cade, **il volume viene spostato sotto un altro server attivo.**

Quando questo accade **l'indirizzo ed il nome di rete della risorsa in cluster sono attivati sul server di failover.**



In un cluster per il failover ci sarà il **cluster management software installato su ogni nodo.**

Ad esempio (il cluster managent software integrato nel DB di IBM):
https://www.ibm.com/docs/en/db2/11.5?topic=model-cluster-management-software

Per i cluster management software disponibili, vedi anche bibliografia alla fine delle slide.

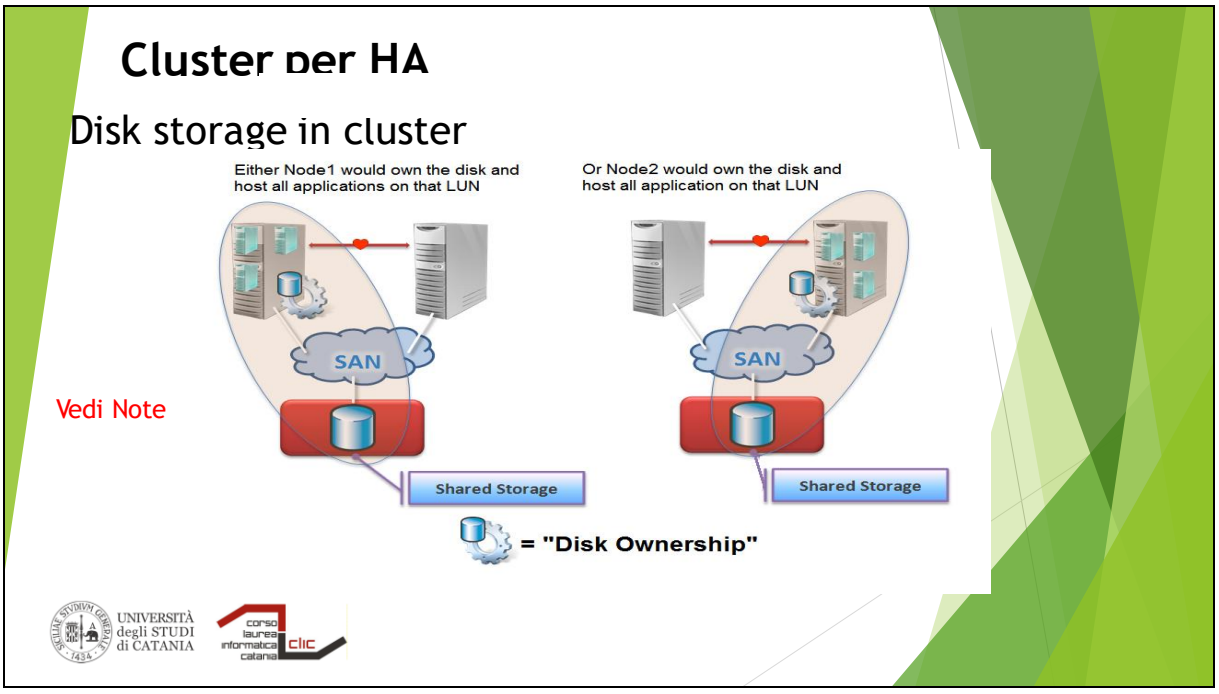
Il cluster management software effettua il monitoraggio degli altri nodi del cluster e delle risorse in cluster sul suo nodo. Può mettere online o offline le risorse in cluster se necessario.

Si veda anche opzionalmente la documentazione Microsoft [4].

Il cluster management software verifica lo stato di un altro nodo del cluster tramite lo **heartbeat connection** (connessione per il battito del cuore). Questa tecnica richiede che un componente invii periodicamente un messaggio (heartbeat) per indicare che sta funzionando normalmente. Se il componente di ascolto non riceve il messaggio di heartbeat entro il periodo di tempo predefinito, determina che si è verificato un errore di sistema e intraprende l'azione appropriata.

L'azione appropriata e' rappresentata dall'avvio delle procedure di migrazione delle applicazioni residenti nel server che non risponde ai messaggi di heartbeat, verso un altro server (esempio il server B).

Un altro meccanismo di controllo della disponibilità di un componente è la **Risposta ping / eco.** In questo metodo di rilevamento dei guasti, un componente, che funge da monitor di sistema, invia un ping al componente, cioè una richiesta di eco **ICMP** (Internet Control Message Protocol) e attende una risposta di eco ICMP. Se la destinazione non risponde al ping in un intervallo di tempo predefinito (avviene il timeout), il componente che funge da monitor di sistema segnala che l'altro componente ha avuto esito negativo.

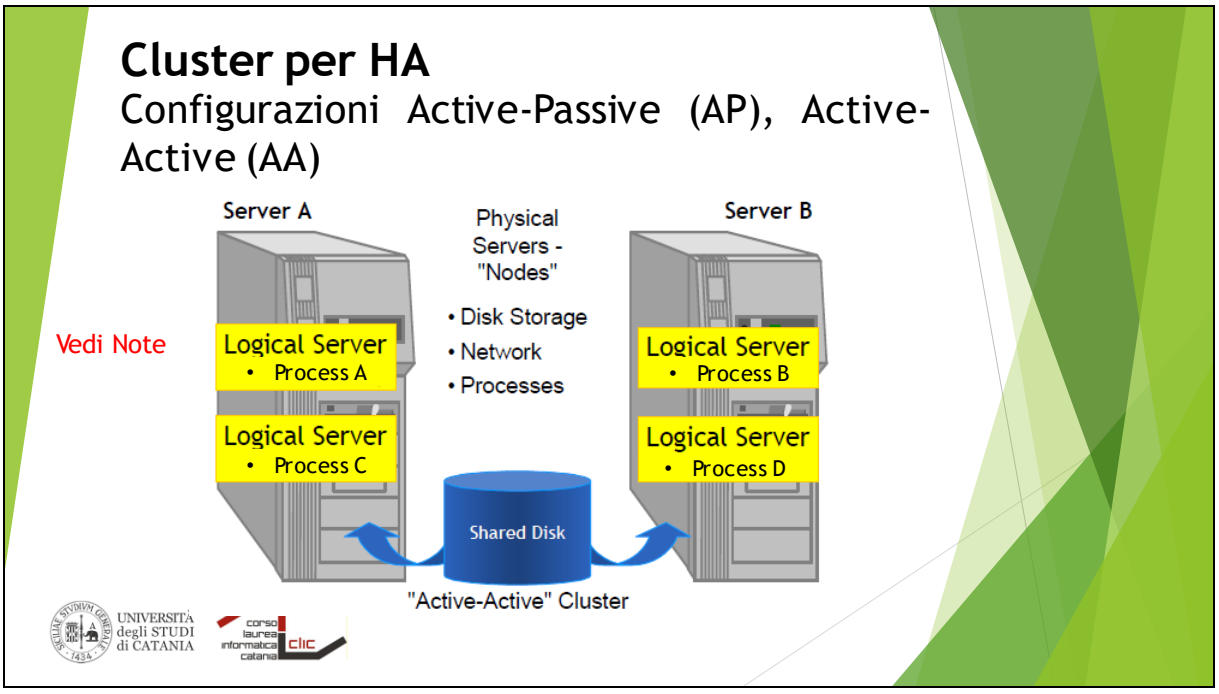


Un componente fondamentale del cluster di failover è lo **spazio disco (disk storage) che può essere acceduto da tutti i nodi del cluster.**
(Tutto lo storage deve essere allocato su **resilient disk**, che sarà esaminato nel seguito.)
L'accesso al **disk storage in cluster può essere girato (switched) a nodi diversi**.
Questo potrebbe essere fatto con switch fisici ma invece è effettuato via software utilizzando il protocollo di accesso ai dischi. In ogni modo il sottosistema disco deve supportare il software di cluster management prescelto,
per poter attivare la funzionalità di switch.
Nella maggior parte dei casi solo un server alla volta può accedere ad un volume di dischi , diventane proprietario (vedi esempio Microsoft nello schema). Si veda [1] opzionalmente.

SAN = Storage Area Network. Tecnologie che permettono di collegare uno o piu dischi mediante fibra ottica o collegamenti simili, usando il comune protocollo SCSI.

Comunque esistono anche soluzioni dove l'accesso allo stesso storage è consentito a più nodi simultaneamente. Il sistema di gestione del cluster deve garantire l'integrità del dato.

LUN = Logical Unit Number.



Le tecnologie di cluster supportano di solito più di un server logico su di un singolo nodo fisico.
Nello schema si vede una configurazione **Active-Active (A-A)** dove, ad **un dato istante, ci sono delle applicazioni in esecuzione su entrambi i nodi**.

In alternativa si parla di configurazione **Active-Passive (A-P) ,** dove un nodo non ha nessun server logico attivo ma è in stand-by pronto ad ospitare un server logico in cso di fail-over (si veda la slide precedente «Failover di un server logico»)

Esistono poi topologie di **cluster con più di due nodi.**

In questo caso è possibile suddividere i server logici attivi su più nodi con possibilità di switch tra diversi nodi del cluster.

Cluster per HA

Active-Passive vs. Active-Active

- **Active-Passive Clusters**
  1. (-) **Maggiori Costi** – Parte dello hardware è inattivo
  2. (+) **Nessun rischio Performance** – Performance invariata dopo failover
  3. (i) Solitamente in uso per sistemi **performance-critical**
     - Database

- **Active-Active Clusters**
  1. (+) **Minori Costi**– Tutto lo hardware viene utilizzato
  2. (-) **Rischio Performance** – Performance potrebbe diminuire dopo failover
  3. (I) Solitamente in uso per sistemi **non performance-critical**

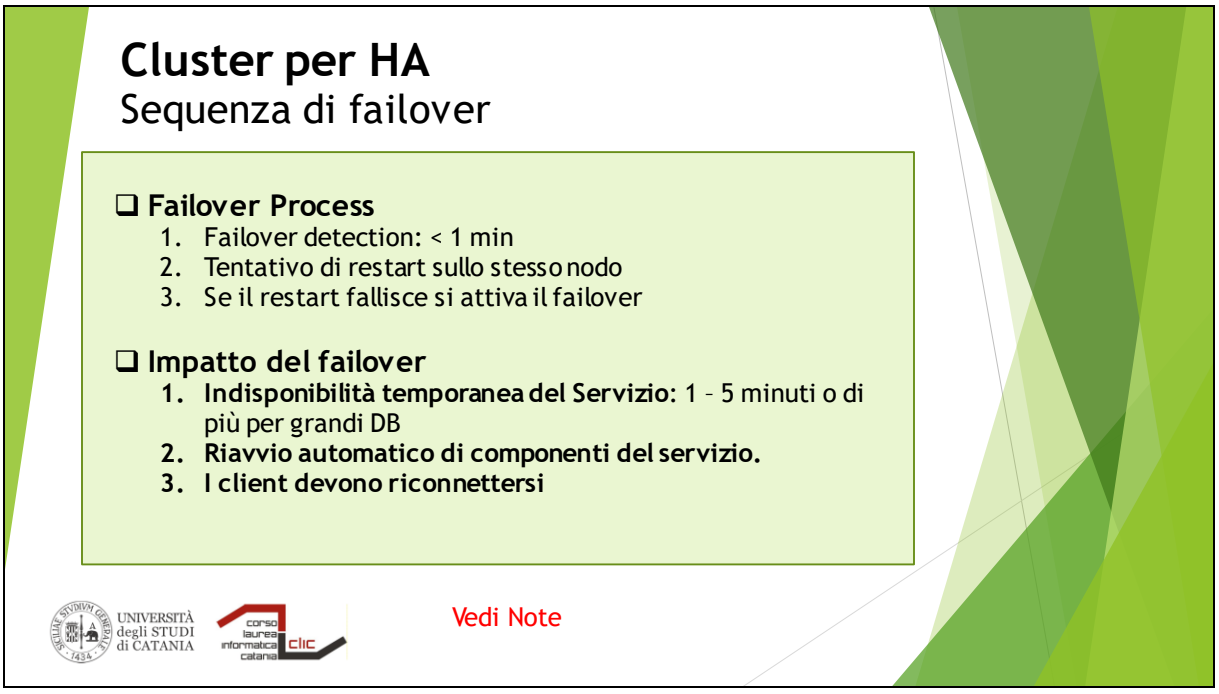
UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Active-Passive vs. Active-Active.

- Soluzione **Active-Active, adozione in casi reali:**
  A. allocare su uno dei nodi **un'applicazione che può essere fermata in caso di failover,** in modo da lasciare all'applicazione principale tutta la potenza di calcolo.
  B. Applicazioni che possono passare in stato di **funzionamento a performance ridotte**: il concetto di **graceful degradation** (anche load balancing).

- Dunque, i criteri di decisione della topologia del cluster dipendono dalle seguenti considerazioni:
  - **Necessità** di livello di **performance** dell'applicazione
  - **Accettabilità** di un **degrado** della performance durante transitori critici.
  - Analisi costi benefici o del **Return Of Investment.**



La sequenza di failover parte con il tentativo del **cluster management software** di riavviare il servizio sullo stesso nodo(se attivo).

Se il nodo non è attivo oppure se il restart fallisce, scatta il vero failover, riavviando il server logico su un altro nodo disponibile.

L'operazione può richiedere qualche minuto ed il client deve ricollegarsi al ritorno alla normalità.
Ogni applicazione ha le proprie specifiche necessità di avvio (e quindi di riavvio dopo il failover).
Il system administrator deve aver definito la procedura di failover tenendo presente le necessità specifiche dell'applicazione in oggetto

Cluster per HA
Prodotti software per il cluster: esempi

- ❑ Oracle Solaris Sun Cluster
- ❑ HP Service Guard
- ❑ **Microsoft Cluster Server (MSCS), Red Hat Cluster Suite,**
- ❑ IBM PowerHA System Mirror
- ❑ Veritas Cluster Server (rebranded as Veritas Infoscale Availability)
- ❑ IBM Tivoli System Automation for Multiplatforms (SA MP)
- ❑ Il cluster managent software integrato nel DB(2) di IBM:
  - https://www.ibm.com/docs/en/db2/11.5?topic=model-cluster-management-software

Si veda 2, 3 e 4 (opzionale) come ulteriori descrizioni di software di cluster per i prodotti Oracle, Microsoft ed HP

Misurare la High Availability

1. **Expected period of operations**
   - ❑Ovvero per quanto tempo il sistema e' operativo in un anno.
2. **% Availability**
   - ❑target rispetto alla prima misura.
3. **Mean time between Failures** (MTBF)
   - ❑stima "predittiva"

Misurare la High Availability

Expected period of operations.

Durata totale in ore di lavoro del sistema, ovvero le ore in cui il Sistema e' disponibile per le normali operazioni di business.

Essa rappresenta **la base di calcolo della disponibilita'**, per ottenere il valore in ore del Downtime atteso.

Expected period of operations - Rappresenta la base di calcolo della disponibilità, per avere il valore in ore del downtime ammesso

Misurare la High Availability

- **% Availability**

  E' solitamente indicata come la percentuale di ore – settimanali, mensili o annuali – nel quale il Sistema **deve essere disponibile per le attività di business**

Vedi Note

% Availability = (Total elapsed time – Sum of inoperative time) / Total elapsed time

Misurare la High Availability

24x365 (Ex. Per. Operations) System
Sistema che lavora 24 ore per 365 giorni l'anno

Availabilty	Minimum Expected Time	Maximum Allowable downtime	Remaining time
99.00%	8672	88	0
99.50%	8716	44	0
99.95%	8756	4	0
100.00%	8760	0	0

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Expected period of operations – La tabella mostra un **sistema attivo 24x365**, cioè tutto l'anno o **H24:** ad esempio i call centre delle compagnie telefoniche. La durata totale di un anno è **8760** ore.

Si osserve il valore decrescente del periodo ammesso per il downtime. Questa è la finestra di tempo nella quale possono essere effettuate le manutenzioni

Misurare la High Availability

12x5x52 System (si osservi la voce remaining time)
->12 ore x 5 gg/settimana x 52 settimane

Availabilty	Minimum Expected Time	Maximum Allowable downtime	Remaining time
99.00%	3089	31	5640
99.50%	3104	16	5640
99.95%	3118	2	5640
100.00%	3120	0	5640

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Expected period of operations – La tabella mostra un **sistema attivo 12x5x52**, cioè tutto l'anno, 5 giorni/settimana per 12 ore.
Si osserve il valore decrescente del periodo ammesso per il downtime. Tuttavia la finestra di tempo nella quale possono essere effettuate le manutenzioni rimane costante, perchè il sistema non è H24

ean time between Failures (MTBF) [15,16]
omma dei tempi di attività di tutti i componenti - inclusi quelli che non sono soggetti a guasti - **diviso per il o di guasti.**

Total operating time / Total number of failures = 1 / FR (Failure Rate)
mente si riferisce ad una unità (disco, stampante, memoria, scheda di rete). E' un indicatore utile ma che **non onto del tempo di ripristino.**

ratica è una **stima dei downtime attesi** sulla base delle rilevazioni precedenti, contando costanti i tassi unzionamenti. **E' un indicatore "predittivo".**

ci sono **più unità dello stesso tipo , il valore unitario del MTBF è diviso per il numero di unità**, diventando molto più basso.

O:
o ha MTBF di 500.000
ventole e alimentatore (di ogni disco) MTBF=200,000 ore (< 500.000)
MTBF da considerare e' 200.000 (immaginando 1 ventola + 1 alim. X disco)
presenza di 200 dischi, il MTBF aggregato scende a 1000 ore (!!).

Scalable Service – Load Balancing

- Processi applicativi che possono essere istanziati **più volte sullo stesso application server** o su più application servers
- In caso di malfunzionamento, qualunque processo Y!=X può eseguire le stesse operazioni di X.
- Utilizzata quando :
  - ✓ Esiste un **grande numero di connessioni allo stesso Processo**
  - ✓ Il Processo è **eseguito su due o più server**
  - ✓ Ogni connessione **è assegnata al server secondo una politica di gestione**
  - ✓ In caso di fallimento di un processo X, le altre connessioni saranno indirizzate agli altri processi (--> failover)

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

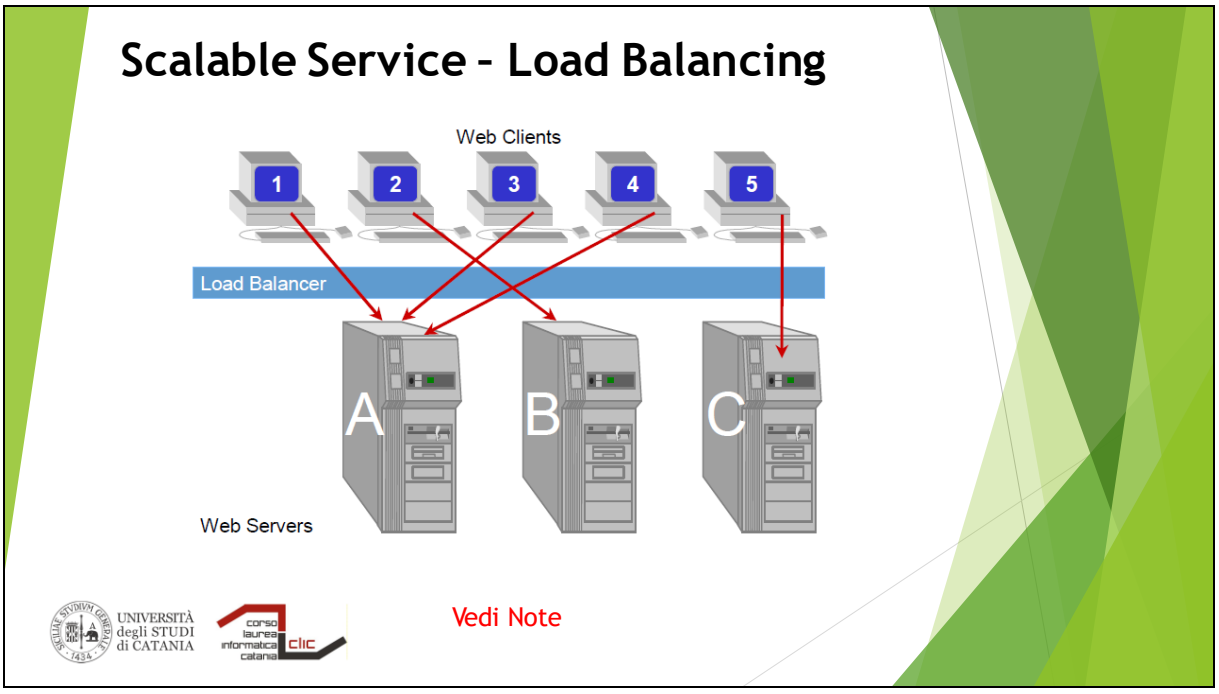
Si affrontano adesso i sistemi scalabili o anche load balanced (**LB**), cioè con un bilanciamento di carico.
E' indicato quando uno servizio può essere erogato da più istanze uguali simultaneamente. Le singole istanze sono ospitate su più server (anche più di un'istanza per server se il programma è costruito in quel modo).

Quando si usa il load balancing, le richieste sono indirizzate al server secondo una politica di indirizzamento; ad esempio:

- Server meno carico
- Round robin

Se uno o più server diventano indisponibili, le nuove connessioni saranno indirizzati ai server superstiti. I web server sono esempi di servizi che possono essere installati in load balancing
Per ogni tipo di servizio che si vuole installare in LB occorrerà stabilire:

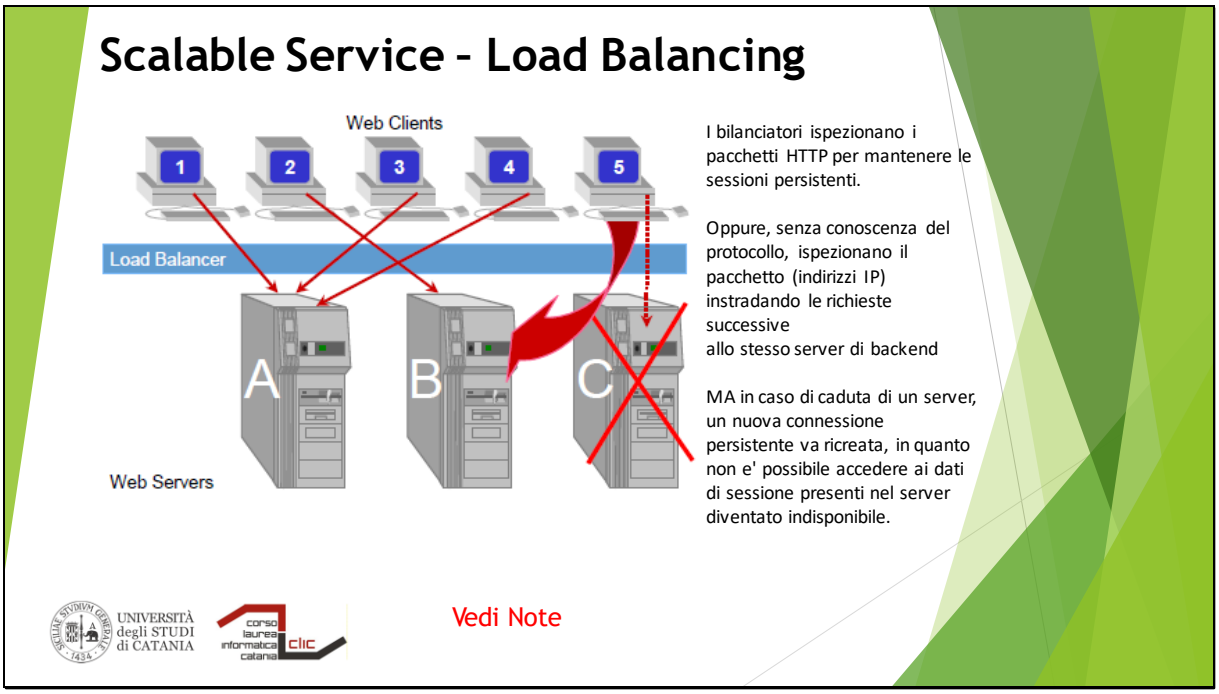
1. Benefici
2. Limitazioni
3. Prerequisiti



Nell'esempio i cinque web clients sono distribuiti:

- 3 sul server A
- 1 sul server B
- 1 sul server C

Questo avviene all'avvio della sessione client. Se il server C diventa indisponibile, le nuove connessioni non saranno più dirette a C, che sarà rimosso dal pool dei server disponibili. Le connessioni andranno ai server disponibili

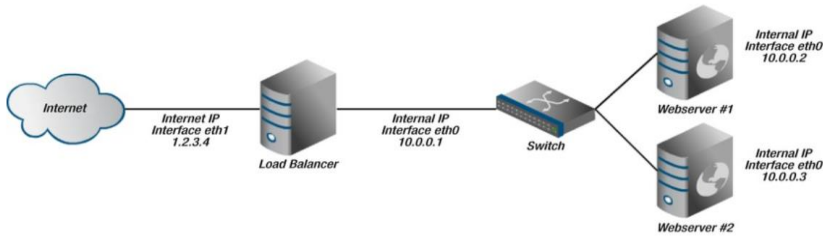


Il client 5 si riconnetterà al server B, quello attualmente con meno sessioni, in caso di una politica «load sensitive», cioè basata sul carico.

Persistenza della sessione.
In alcuni scenari in cui è presente un bilanciatore di carico, è importante che un utente venga indirizzato allo stesso server di back-end ad ogni interazione successiva.
Questa è una soluzione ad un problema che presenta il bilanciamento del carico. Per migliorare le prestazioni, un server di back-end può archiviare i dati in locale, ad esempio se il set di dati è troppo grande per poter essere utilizzato in rete in modo immediato oppure se ci sono dati in cache sul web server. In questo caso, il client avrà bisogno che le richieste successive vengano indirizzate allo stesso server di backend.
Il reindirizzamento di un client allo stesso server di back-end in connessioni successive viene definito **persistenza della sessione** o, in alternativa, semplice persistenza. Usiamo il termine persistenza della sessione perché è più comune.
Viene definita anche come “sticky session”, ovvero “sessione appiccicosa”.
In caso di traffico HTTP, i bilanciatori del carico sono spesso in grado di ispezionare i pacchetti per i **cookie di sessione**, che possono essere utilizzati per instradare il client allo stesso server per la stessa sessione di accesso.
Se il bilanciatore non ha conoscenza del protocollo, il bilanciatore può tornare a stabilire la persistenza della sessione al livello di trasporto (TCP) ispezionando l'IP di origine dei

pacchetti e instradando lo stesso client allo stesso server. Questo è noto come persistenza della sessione IP di origine ("source-IP session persistence").
In ogni caso, se il server di backend su cui è stata creata la connessione diventa indisponibilie, il bilanciatore indirizzerà a un endpoint alternativo e apre una nuova sessione persistente.

Scalable Service – Load Balancing



Il LB ha **due interfacce di rete:**

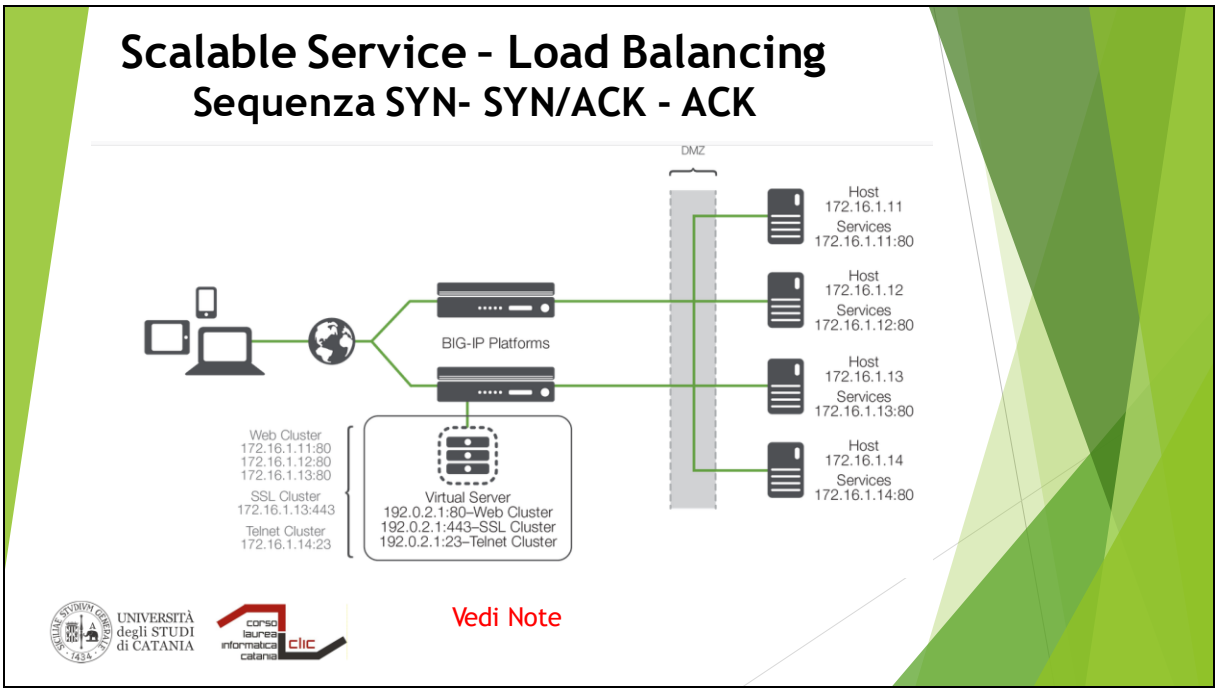
- **Una connessione alla rete pubblica** – diciamo **et0** - da cui provengono le richieste, con un idirizzo nell'esempio di 1.2.3.4
- **Una su di una rete virtuale** su cui sono attestati i server applicativi da bilanciare: 10.0.0.1
- I server applicativi avranno indirizzi 10.0.0.2 e 10.0.0.3, NO IP pubblici

Servizio di LB:

- mantiene la tabella dei server fisici
- gestisce la **politica di carico.**
- Ogni richiesta proveniente dalla rete pubblica sara' distribuita ai server nella tabella di indirizzamento, indipendentemente dal numero di server disponibili.
- Il servizio LB può **definire in principio anche più servizi da bilanciare**, con l'elenco dei server su cui girano

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

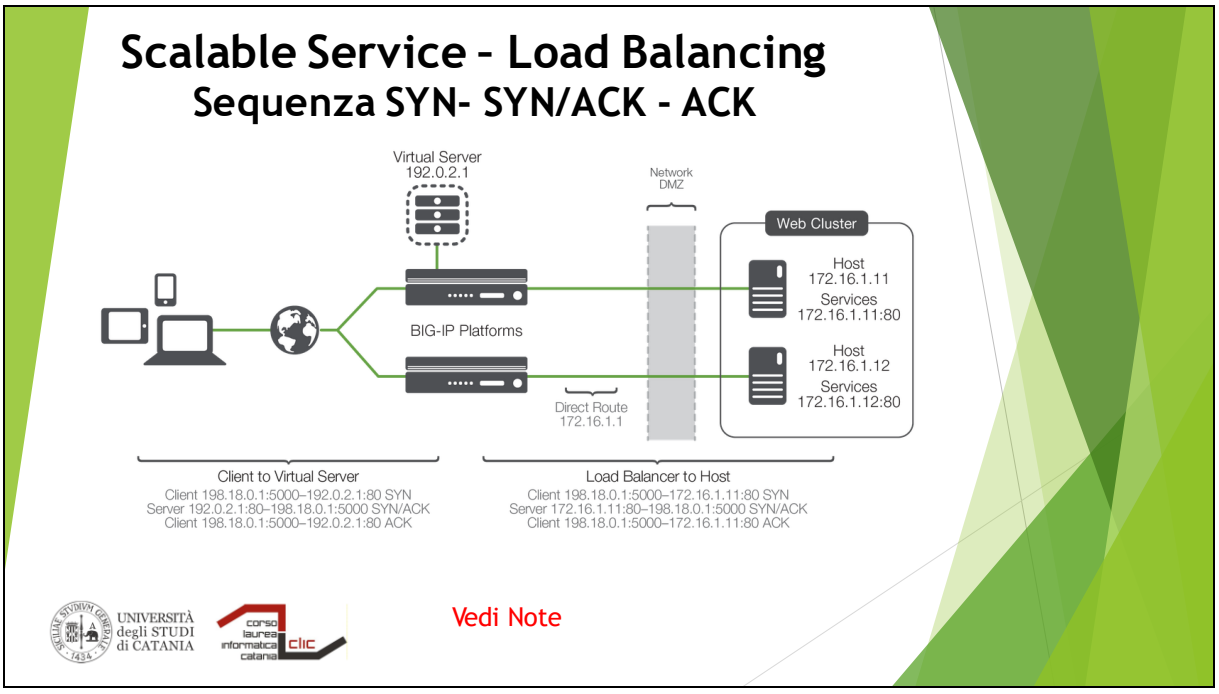


NB: BIG-IP e' un noto fornitore di load balancer

NB: La figura mostra un CLUSTER DI load balancer. Altrimenti avremmo un single point of failures..

Il client 198.18.0.1 invia una richiesta di connessione SYN su HTTP dalla porta 5000 alla porta 80 del server virtuale 192.0.2.1 (**il load balancer LB**), per raggiungere il web server
Il client 198.18.0.1 vede solo il server logico 192.0.2.1:80
Nelle sue tabelle di indirizzamento, il LB ha tre web server che ascoltano sulla porta 80: 172.16.1.11, 172.16.1.12, 172.16.1.13.
NOTA. Lo stesso LB può anche indirizzare il servizi Telnet sul 172.16.1.14:23 ed SSL su 172.16.1.14:443
Decide di indirizzare la richiesta al servizio server 172.16.1.11:80

https://www.f5.com/services/resources/white-papers/load-balancing-101-nuts-and-bolts



(**continua**)

Il client 198.18.0.1 vede solo il server logico 192.0.2.1
Il web server 172.16.1.11 risponde con una conferma SYN/ACK al client 198.18.0.1:5000. la richiesta viene intercettata dal LB 192.0.2.1:80 che la trasforma in una sua conferma SYN/ACK al client 198.18.0.1
A questo punto il client 198.18.0.1 invia una conferma di connessione ACK al LB 192.0.2.1:80 che ripete la sequenza con il server fisico 172.16.1.11:80

https://www.f5.com/services/resources/white-papers/load-balancing-101-nuts-and-bolts
https://it.wikipedia.org/wiki/Transmission_Control_Protocol

Scalable Service - Load Balancing

- **Politiche di bilanciamento**

1. **Round-Robin**
   - a rotazione, senza ponderare lo stato dei server o la natura del carico
2. **Weighted Round-Robin**
   - Peso (weight) aumenta con la capacita di carico del server
3. **Least-Connections Based Schedules**
   - Priorita' ai server con il minor numero di connessioni attive
4. **Weighted Least-Connections**
   - No. Connections / weight
5. **Locality-Based Least-Connection**
   - Inviare le richieste provenienti da IP identici alle stesse macchine (ma IP mascherati da NAT?), assumendo che I server mantengono dati in cache (efficienza)

UNIVERSITÀ degli STUDI di CATANIA — corso laurea informatica catania CLIC

Vedi Note

Principali politiche di bilanciamento

1. **Round-Robin Based Schedule (RR)** – I server sono elencati in una tabella ed il **carico distribuito a rotazione**. Semplice gestione, **non viene considerate lo stato di carico del server** che potrebbe ricevere sempre le richieste più pesante o lunghe. Si applica al meglio se è noto che le richieste hanno lo stesso peso in termini computazionali
2. **Weighted Round-Robin** – Ai server del Servizio sono assegnati **pesi più alti** (Weight Value) se hanno **maggiore capacità di calcolo**. Il carico viene assegnato in RR ma con una percentuale maggiore ai server con peso maggiore. Si applica al meglio se è noto che le richieste hanno lo stesso peso in termini computazionali. Ad una Migliore distribuzione a fronte di capacità differenti di calcolo, corrisponde però la necessità di gestire manualmente le tabelle dei pesi
3. **Least-Connections Based Schedules** – Il carico viene distribuito prima ai **server con meno connessioni attive**. Comporta maggiore overhead (tempo di calcolo amministrativo) per la definizione della macchina a cui assegnare il carico
4. **Weighted Least-Connections** – La connessione viene assegnata alla macchina con il numero minimo di connessioni ed il **peso più alto, quindi con il minimo rapporto "Number of Connections" / "Weight Value."**
5. **Locality-Based Least-Connection** – Questa politica tende ad indirizzare allo stesso server le richieste che provengono dallo stesso indirizzo IP, in questo modo

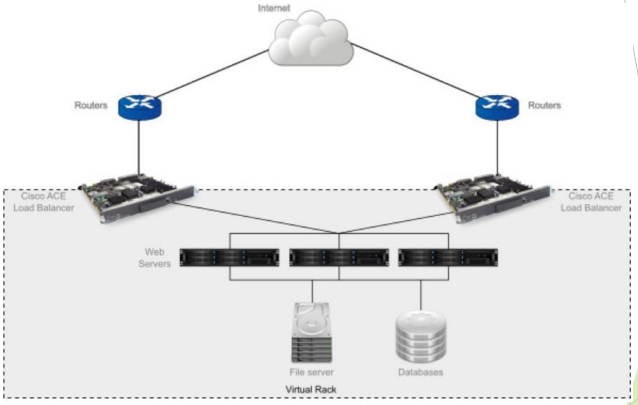
favorendo al massimo l'uso di eventuali dati mantenuti in una cache del server. Il problema che se le richieste giungono da una rete private che utilizza NAT (Network Address Translator) per la traduzione degli indirizzi, al server potrebbero arrivare molte richieste dallo stesso indirizzo, ma in realtà originate dalla rete privata attestata dietro l'indirizzo NAT – Si veda [5] per qualche info addizionale sul NAT in Cisco.

Scalable Service - Load Balancing

- I load balancer possono essere
  1. Software
  2. Dispositivi hardware

Es: Apache http / Ngix

High availability anche per I bilanciatori



Vedi Note

Tipi di load balancer

- **Dispositivi hardware. Esempi sono i LB Cisco ed F5 BigIP**
  - https://www.f5.com/services/resources/glossary/load-balancer
  - https://www.cisco.com/c/en/us/td/docs/ios/slb/configuration/guide/slb_cg_book/slb_cg_info.html

- **Applicativi software tipi web servers**
  - **Apache HTTP**, o più comunemente Apache, è il nome di un server web libero sviluppato dalla Apache Software Foundation. È la piattaforma server Web modulare più diffusa, in grado di operare su una grande varietà di sistemi operativi. https://httpd.apache.org/
  - **Nginx** è un web server/reverse proxy leggero ad alte prestazioni; https://www.nginx.com/

Continuità Operativa - Graceful degradation

- A seguito di uno o piu' guasti, le risorse rimanenti possono essere destinate **solo alle applicazioni critiche**
- **Applicazioni non critiche** possono essere **temporaneamente fermate**

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

La Graceful degradation è un approccio di recupero degli errori in cui solo alcune funzionalità sono rese non disponibili al fine di evitare che l'intero sistema diventi inutilizzabile.

Se i guasti impediscono che l'intero sistema software sia operativo, alcune funzioni possono essere eliminate a favore di altre.

Ad esempio, se a seguito di alcuni fault un sistema sta esaurendo le risorse, le funzioni più importanti possono essere mantenute attive mentre altre vengono chiuse.

Scalabilità orizzontale e verticale

- **Scalabilità verticale:** aumentare le risorse di calcolo (RAM e/o numero e/o frequenza di clock delle CPU) dei singoli server applicativi.
  - Questo può essere sia sui cluster che le architetture in LB.
  - Esempio di scalabilita' orizzontale su cluster: DBMS Oracle + opzione Real Application Cluster (RAC), in grado di sfruttare i nodi del cluster in parallelo
- **Scalabilità orizzontale:** consiste nell'aumentare il numero di server applicativi in LB per aumentare la capacità di calcolo

UNIVERSITÀ degli STUDI di CATANIA corso laurea informatica clic

Vedi Note

In Inglese: **vertical/horizontal scalability**

Per loro natura I cluster HA si prestano maggiormente alla scalabilità verticale.

Tuttavia alcune applicazioni specifiche, quali il DBMS Oracle quando si usa l'opzione Real Application Cluster (RAC), sono in grado di sfruttare entrambi I nodi del cluster in parallelo, salvo fare uno switch sul nodo superstite in caso di failover. In questo caso viene implementata una scalabilità orizzontale anche in presenza di un cluster.

Continuità dei dati

- **Resilient disk storage.** Tecnologie per alta affidabilità e disponibilità dei dati.
  - **Redundant Array of Inexpensive Devices (RAID).**
    - Controller appositi o soluzioni software per ridondanza dei dati su piu' dischi e informazioni per la correzione di errori (parita').
  - **Storage Area Network (SAN)**
    - Ideale per failover/cluster. Implica spesso uso di soluzioni RAID
  - **Data Mirroring**
    - Replica dei dati in localita remota (supporta il disaster recovery)

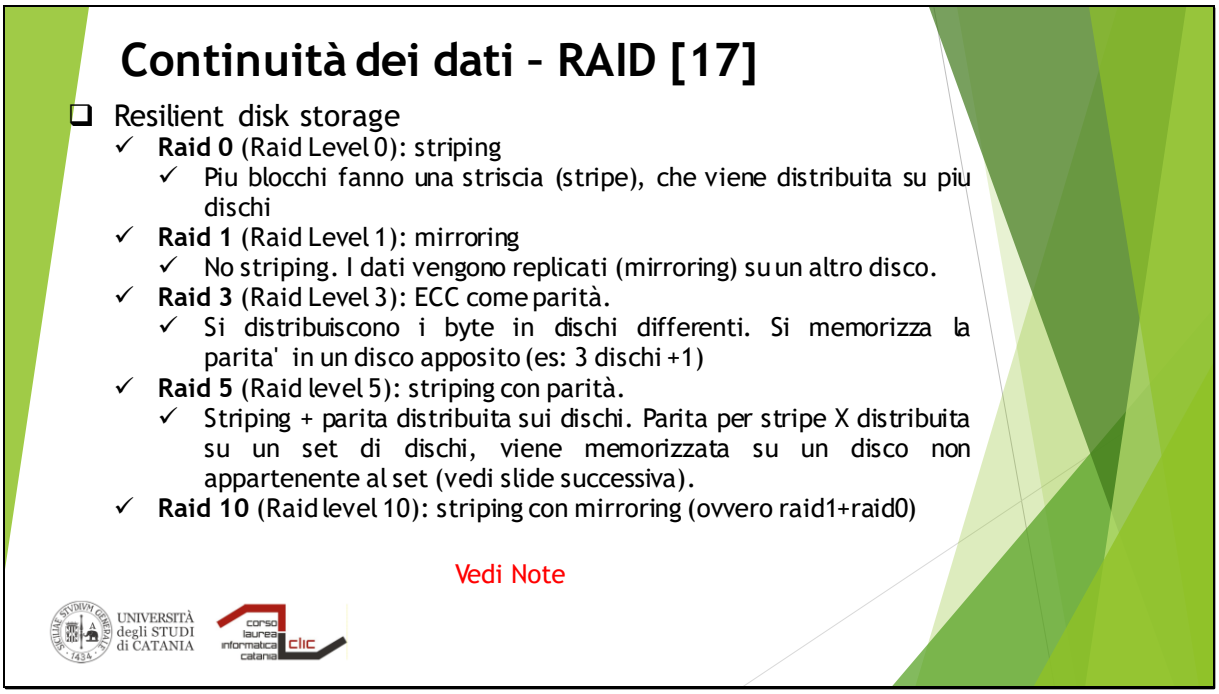
Un sistema disco resistente (**resilient disk storage**) garantisce la disponibilità dei file anche in presenza di un guasto hardware o danneggiamento del supporto. Il resilient disk storage è una condizione necessaria perchè un sistema applicativo nel suo complesso sia in high availability.
I file di cui si deve garantire la **disponibilità** sono sia i **file di sistema, i file di dati applicativi**.

Le tecnologie ed i prodotti che forniscono alta affidabilità e disponibilità dei dati sono:

- Redundant Array of Inexpensive Devices (RAID)
- Storage Area Network (SAN)
- Data Mirroring

Nel seguito saranno eaminate in dettaglio le configurazioni RAID. Esaminiamo brevemente SAN e Data Mirroring

- **Storage Area Network (SAN).** Consentono l'istallazione di risorse di memorizzazione (dischi) sulla rete e renderlo accessibile a server multipli. Ideale per supportare il failover a tecnologie in cluster.
- **Data mirroring.** E' una replica a basso livello dei dati verso un supporto uguale come tipo e capacità ma situato in una località remota. E' una caratteristica che consente la creazione di siti di disaster recovery, che saranno esaminati in seguito



Sono opzioni standard, classificate a livelli per i **Reduntant Array of Inexpensive Disks (RAID).**
Non devono **mai essere utilizzati in sostituzione del backup**

Le tecniche utilizzate sono **striping** e **mirroring**.

RAID 0 – striping del disco. I dati sono suddivisi in blocchi da 64 Kbyte (**stripe unit**) e distribuiti in ordine fisso ed in modo uniforme su tutti I dischi dell'array. Una sequenza di stripe unit e' detta **stripe o strip**. RAID 0 **non è fault tolerant** perchè non c'è ridondanza del dato. Offre vantaggi in termini di utilizzo dello spazio (creando piccole partizioni) e **migliori performance**, perchè ci sono più controller del disco

RAID 1 – mirroring del disco. La partizione viene duplicate su un altro disco. Il disco è protetto da danneggiamento perchè il dato è sempre duplicato.
Ne consegue che:

1. Spazio utile: 50% **(-)**
2. Overhead in scrittura: 100% **(-)**
3. Read enhancement: 0%
4. **High availability (+)**

RAID 3 – Error correction code (ECC) come parità. Si memorizza lo **stripe unit + componente di controllo degli errori**, implementato come controllo di parità. Si differenzia dal RAID 2 (non trattato qui) che utilizza un ECC puro che quindi memorizza anche il dato di controllo e recupero dell'errore. Quindi RAID 3, che utilizza un solo disco per memorizzare la parità, necessita di meno spazio del RAID2, circa 85% dello spazio disponibile. Non molto usato nella pratica.

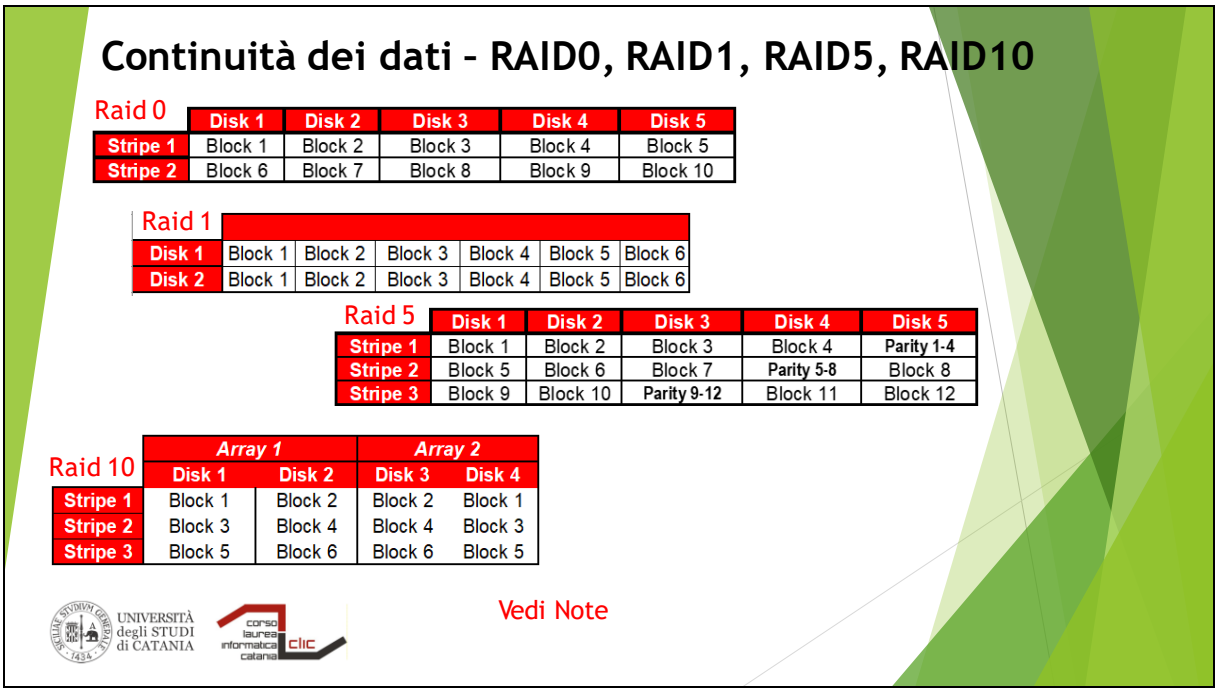
RAID 5 – Striping con parità. E' il Sistema più noto di fault tolerance. **Lo striping dei dati e le informazioni di parità sono distribuiti su tutti i dischi. Inoltre, I dati di parità sono sempre su di un disco diverso dal blocco a cui si riferisce**. Il numero elevato di controller aumenta la performance in lettura.
Ne consegue che:

1. Spazio utile: 65% - 85%
2. Overhead in scrittura: 110% - 400%
3. Assicura **performance elevate in lettura (read) e high availability**

RAID 10 – Striping con mirroring. Lo striping avviene su tutti i dischi dell'array. L'array è duplicato.
Ne consegue che:

1. Spazio utile: 50%
2. Overhead in scrittura: 100%
3. High availability

L'alta affidabilità del dato è garantita.



Si veda anche «IBM – Il mainframe», Appendice C – I sottosistemi di storage

Esiste anche il **RAID6 a doppia parità**, quindi con una ridondanza dei dati di parità. Offre una maggiore protezione rispetto al RAID5 ma al costo di una intera unita disco per memorizzare il controllo di parità. Inoltre la fase di scrittura rallenta ulteriormente

Esempio. Avendo a disposizione 4 array da 200GB l'uno, lo spazio utile sarà di 600GB, perchè l'equivalente di un'intera unità è dedicato alla parità.

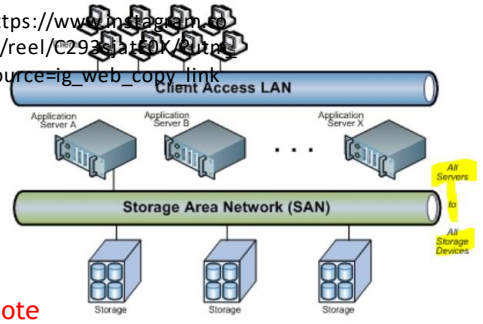
Come le informazioni di "Parita" permettono di ricostruire dati "perduti" a causa di un fault di un disco (RAID 5):

- Si suppong che il disco no. 1 vada In fault
- Di conseguenza I blocchi 1, 5 e vanno perduti.
- **Per ricostruire correttamente la stripe (striscia) 1 (blocco 1) allora basta combinare I blocchi 2, 3, 4 e le informazioni di parita' 1-4**
- Si opera analogamente ricostruire le striscie no. 2 e 3.
- Se a causa di un fault di un disco si perdono alcune informazioni di parita', si ricostruiscono combinando tutti I blocchi della striscia, che sono memorizzati in dischi differenti.

Continuità dei dati - Storage Area Network

- **Storage Area Network - SAN [13]**
  - Oltre a 13, visionare anche note SAN-NAS I-O.pdf
- ✓ Storage condiviso, **accessibile a tutti i server**
- ✓ **Ideale per High Availability e Load Balancing**
- ✓ Dispositivo dedicato
- ✓ **High-Speed Connection**

https://www.instagram.com/reel/C292sJatE0X/?utm_source=ig_web_copy_link



UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

Vedi Note

Una tecnologia SAN consente di implementare lo storage condiviso tra I nodi di un cluster oppure di una batteria di server in Load Balancing.

- SAN utilizzano solitamente tecnologia su fibra ottica (Fibre Channel o FC) ed il Fibre Channel Protocol (FCP) per gli open systems. Varianti di tipo proprietario sono utilizzate per i mainframes.
- Possono utilizzare anche il protocollo Fibre Channel over Ethernet (FCoE) per trasportare il traffico FC su reti Ethernet ad alta velocità e quindi far convergere l'infrastruttura di rete per protocolli IP e storage sugli stessi cablaggi.
- Ancora, possono essere usati la Internet Small Computing System Interface (iSCSI), per realtà aziendali medio piccolo con costi minori della FC ed anche InfiniBand, usata in ambienti ad elevate prestazioni
- Infine attraverso gateways si possono spostare dati tra diverse tecnologie SAN

Le due seguenti definizioni sono fornite al solo scopo di chiarire gli acronimi utilizzati. Non faranno parte dei test di esame.

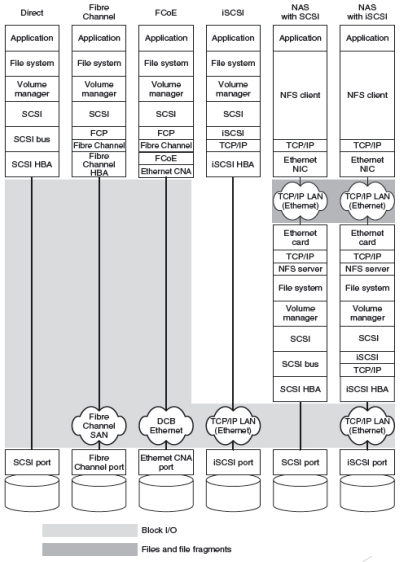
InfiniBand (IB) è una struttura di interconnessione unificata in grado di gestire sia I / O di archiviazione, I / O di rete e comunicazione interprocesso (IPC). Può interconnettere array di dischi, SAN, LAN, server e server di cluster, fornire elevata larghezza di banda e

trasmissione a bassa latenza su distanze relativamente brevi e supportare canali I / O ridondanti in una o più reti Internet, in modo che i data center possano ancora funzionare quando si verificano errori sulle reti locali.
InfiniBand viene utilizzato principalmente in scenari di comunicazione input / output di basso livello. Inoltre, la modalità di trasmissione e i media di IB sono abbastanza flessibili. Può essere trasferito da una lamina di filo di rame del circuito stampato nell'apparecchiatura e interconnesso con Active Optical Cables (AOC) e Direct Attach Cables (DAC) .

Fibre Channel over Ethernet (**FCoE**) permette di mappare i frame Fibre Channel su una rete IEEE 802.3 full-duplex. In questo modo è possibile utilizzare le connessioni 10 gigabit Ethernet per il trasporto dei pacchetti Fibre Channel senza modificare il protocollo e le funzionalità Fibre Channel. Per operare, FCoE ha bisogno di una rete lossless ethernet che garantisca un trasporto senza perdita di pacchetti indispensabile al trasporto del traffico SCSI che è incapsulato all'interno dei pacchetti Fibre Channel.

Continuità dei dati - Network Attached Storage

- **Network Attached Storage (NAS)**
  - ✓ File server condiviso in rete
  - ✓ Installazione immediata
  - ✓ Supportano High Availability e Load Balancing
  - ✓ Poco adatti ad uso DBMS per le performance inferiori
  - ✓ Connessi ai server attraverso una LAN



Vedi Note

Nei dispositivi SAN - Fibre Channel, FCoE e iSCSI - lo scambio di dati tra server e dispositivi di archiviazione è basato su blocchi. Fibre Channel fornisce prestazioni ottimali per lo scambio di dati tra server e dispositivo di archiviazione. Per contro le reti di archiviazione sono più difficili da configurare.

I server NAS sono file server chiavi in mano. Possono essere usati solo come file server, dove mostrano le loro caratteristiche ottimali. I server NAS hanno sono utilizzati n modo limitato per i DBMS, a causa delle prestazioni ridotte.

File storage
Nello storage di file - chiamato anche storage a livello di file o basato sui file - i dati vengono archiviati all'interno di una cartella.
Per accedere a un determinato dato occorre indcare il percorso (path) su cui è stato archiviato. I dati archiviati in file vengono organizzati e recuperati mediante una quantità limitata di metadati che dice al computer la posizione esatta in cui si trova il file.
Si tratta di un catalogo per i file di dati e la struttura è gerarchica.
Il file storage è solitamente usato per i Network Attached Storage (NAS).

Block storage
Lo storage a blocchi divide i dati in blocchi e li archivia separatamente.

A ogni blocco di dati viene assegnato un identificativo univoco, che permette a un sistema di storage di collocare i dati in posizione ottimale. E' anche possibile distribure i blocchi su sistemi operativi diversi: alcuni in un ambiente Linux altri su Windows e così via.
Lo storage a blocchi è spesso configurato in modo da separe i dati dall'ambiente dell'utente e distribuirli in ambienti più adatti ai dati. Nel momento in cui i dati vengono richiesti, il software di storage di base riassembla i blocchi di dati da questi ambienti e li restituisce all'utente.
Questo rende **il block storage adatto ad ambienti storage area network (SAN)** e richiede di essere collegato ad un server.
Poiché lo storage a blocchi utilizza percorsi multipli, a differenza dello storage di file, il recupero dei dati è molto più rapido.
L'indipendenza e la divisibilità che caratterizzano ogni blocco li rendono accessibili in un sistema operativo diverso, offrendo all'utente la massima libertà di configurazione dei dati.
Lo storage a blocchi è un sistema efficiente, affidabile e facile da usare e gestire. È particolarmente adatto per le applicazioni che gestiscono una grande quantità di transazioni e per quelle che implementano database di grandi dimensioni perché lo storage a blocchi è più efficace quando i dati da archiviare sono molti.

Continuità dei dati - Data mirroring

- Data mirroring
  - ✓ Consiste nella **copia integrale** del file su di una installazione separata
  - ✓ Si applica a file di sistema ed a file di dati di business
  - ✓ Equivale alla ridondanza RAID1
  - ✓ Può essere a livello di disco o di array di dischi
  - ✓ Può essere effettuato in modo sincrono o asincrono

Vedi Note

Il beneficio del data mirroring di tutto il disco garantisce una elevate disponibilità del dato. Tuttavia si paga in termini di :

1. Costi di hardware: equivale al RAID 1 quindi occorre duplicare lo spazio disponibile
2. Costi di rete, perchè i dati devono transitare sulla rete e quindi impegnare la banda passante
3. Rallentamento delle operazioni, se la doppia scrittura avviene contestualmente (sincrona) ad opera dello stesso DBMS

E' una componente fondamentale delle configurazioni di disaster recovery.

Alcune soluzioni commerciali, ad esempio Oracle Data Guard, trasferiscono solo i redo log del DBMS applicando le transazioni concluse con successo alla copia del DB. Quindi si parte da una copia iniziale allineata e le due istanze sono tenute aggiornate simultaneamente con uno scarso traffico di rete.
E' possible effettuare il mirroring anche a livello di array, perchè una soluzione RAID10 potrebbe essere vulnerabile ad un guasto a livello di array. Una soluzione commerciale di questo tipo è Oracle Automatic Storage Management (Oracle ASM).

Per comodità si riporta la definizione e le caratteristiche del RAID 1

RAID 1 – mirroring del disco. La partizione viene duplicate su un altro disco. Il disco è protetto da danneggiamento perchè il dato è sempre duplicato.

Ne consegue che:

1. Spazio utile: 50%
2. Overhead in scrittura: 100%
3. Read enhancement: 0%
4. High availability

Altri punti di vulnerabilità: single point of failure

- **Single Point of Failure (SPOF)** – E' un elemento software o hardware la cui perdita risulta nella perdita integrale del servizio
- Disegnando un sistema High Availability, occorre tenere presente di tutti gli SPOF:
  - ✓ Errore umano
  - ✓ Server
  - ✓ Connettività di rete (cablaggio)
  - ✓ Schede di rete
  - ✓ Disco di sistema (OS root disk)
  - ✓ Disco dati di business
  - ✓ Alimentazione elettrica (power source)
  - ✓ Scheda di interfacciamento al disco
  - ✓ Sistema Operativo
  - ✓ Software applicativo

Altri punti di vulnerabilità: SPOF

COMPONENTE	RIMEDI PER ELIMINARE LO SPOF
Server	Failover Cluster, server bilanciati
Load Balancer Hardware	Failover Cluster
Connettività di rete (cablaggio)	Schede di rete LAN ridondanti e sottoreti differenti.
Schede di rete	Schede di rete LAN ridondanti e sottoreti differenti.
Disco di sistema (OS root disk)	Dischi RAID
Disco dati	Dischi RAID
Alimentazione elettrica (power source)	Alimentazione elettrica sdoppiata e gruppi di continuità (UPS) su entrambe
Scheda di interfacciamento al disco	Schede ridondanti secondo il modello di disco in uso
Sistema Operativo	Failover e sistema applicativo disegnato per il riavvio automatico
Software applicativo	Failover e sistema applicativo disegnato per il riavvio automatico
Errore umano	1. Failover 2. Automatizzare tutto il possibile. 3. Documentare le procedure di emergenza

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Backup e Recovery

- **Database backup**
  - ✓ Salvataggio dei file fisici utilizzati per memorizzare e ripristinare il database
  - ✓ Il salvataggio può avvenire su disco o su un supporto offline tipo un nastro o cartuccia
  - ✓ I file sono:
    - Data file
    - Control file
    - Redo/journal logs
- **Altri backup**
  - ✓ Software applicativo, dei relativi file di configurazione e dei file di sistema
  - ✓ File dati diversi dai data file del DBMS, ad es. i file VSAM del mainframe
  - ✓ Qualsiasi file critico per il funzionamento del sistema deve essere salvato in modo sicuro

UNIVERSITÀ degli STUDI di CATANIA — corso laurea informatica CLIC

Vedi Note

- Data file – Sono i dati ed i metadati del DBMS
- Control file – E' un file di sistema creato al momento della creazione dell'istanza del DB. Definisce alcune caratteristiche dell'istanza del DB, ad esempio: database name, name e location dei data files e redo log files, timestamp della creazione del database, current log sequence number, checkpoint information. Senza control file non è possibile la recovery del DB. Si dovrebbero creare due o più copie del control file.
- Redo o journal log (nomenclatura variable secondo il fornitore). File che contengono tutte le modifiche effettuate ad un DB mentre avvengono.
  https://docs.oracle.com/cd/B28359_01/server.111/b28310/onlineredo001.htm#ADMIN11303
  https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-ver15
- Il software applicativo deve essere salvato, assieme ai file della specifica configurazione in produzione
- Inoltre deve essere soggetto a salvataggio qualsiasi tipo di file cruciale per la disponibilità dell'applicativo.

Backup e Recovery

❑ **Tipi di supporto per il backup (Backup device and media)**

I dispositivi ed i supporti per il backup devono essere scelti in base ai seguenti criteri:

- ✓ **Tipo Standard**: supporti particolari richiedono a loro volta manutenzione e supporto specifico
- ✓ **Capacità**: si deve garantire adeguato spazio
- ✓ **Velocità**: si deve garantire adeguata velocità di backup e restore
- ✓ **Prezzo**: il dispositivo ed il supporto devono garantire un costo ragionevole (ad esempio la cartuccia costa meno dei supporti di rete remoti)

UNIVERSITÀ degli STUDI di CATANIA — corso laurea informatica CLIC

Vedi Note

Esistono vari tipi di dispositive e supporti adatti al backup.
La Scelta della tecnologia deve essere adeguata alla necessità di business. Seguono alcuni esempi:

- Lettori di supporti magnetici: nastri e cartucce
- Hard disk asportabili
- SAN
- Dischi ottici: CD-ROM, CD-RW, DVD-RW
- Dischi a stato solido (SSD): flach drive, memory stick

Backup e Recovery

❑ **Schemi di backup**

Gli schemi di backup principali sono:

1. **Full Backup (sempre lento)**
2. **Incremental backup:**
   - Salvare modifiche rispetto all'ultima versione salvata da un full backup o un incremental backup.
   - (+) veloce in fase di backup, a parte il primo backup full
   - (-) lento in fase di ripristino in quanto richiede applicazione sequenziale di tutti i backup incrementali
3. **Differential backup**
   - Salvare modifiche rispetto all'ultima versione salvata in un full.
   - (-) lento in fase di backup
   - (+) meno lento in fase di ripristino

Full Plus Incremental Backup Schema							
	Day1	Day2	Day3	Day4	Day5	Day6	Day7
File 1	x	x					
File 2	x		x				
File 3	x			x			
File 4	x				x		

Full Plus Differential Backup Schema							
	Day1	Day2	Day3	Day4	Day5	Day6	Day7
File 1	x	x	x	x	x		
File 2	x		x	x	x		
File 3	x			x	x		
File 4	x				x		

UNIVERSITÀ degli STUDI di CATANIA — corso laurea informatica catania CLIC

Vedi Note

Gli schemi di backup principali sono:

1. Full Backup: copia integrale di tuttti i file oggetto del ciclo backup/restore. Il vantaggio è di avere un unico repository. Lo svantaggio è la lentezza delle attività
2. *Incremental backup: consiste nel salvare i dati/file che sono nuovi o modificati* ***rispetto all'ultimo full o incremental bkp****. Molto veloce il backup ma il restore richiede l'applicazione sequenziale di tutte* le copie incrementali
3. Differential backup: consiste nel salvare i dati/file che sono nuovi o modificati **rispetto all'ultimo full**. Il restore è più veloce dell'incremental, perchè richiede di portare in linea solo l'ultimo full ed i differenziale. Il backup è più lento e richiede più spazio.

Infine occorre anche tenere presente la necessità di **ruotare i supporti di backup** in modo da conservare i backup settimanali, mentre si riutilizzano i supporti giornalieri.

Alla fine del mese l'ultimo settimanale rimane il master backup del mese precedente. Questo schema è detto «grandfather-father-son»

Fonti consultate: Certified Information System Auditor (CISA): Review Manual - **Information Systems Audit and Control Association (ISACA)**

Backup e Recovery

❑Recovery

- Il recovery dalle copie di backup è un'attività critica.
- Occorre sempre effettuare **test periodici** del buon funzionamento del recovery dei dati/file.
- Le procedure di recovery devono essere:
  - **Documentate accuratamente**
  - Conservate anche in una **copia di backup** in un sito remoto e sicuro
  - **Testate periodicamente e aggiornate all'occorrenza**

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Il backup è inutile senza un efficace recovery.
Occorre documentare le procedure di recovery e conservarne una copia in ambiente sicuro e separato dal sito operativo, protetto anche da accessi fisici indesiderati.
Inoltre occorre effettuare dei test delle procedure per accertarsi che funzionin. Occorre ricordare che: '**Il backup funziona sempre, il restore non funziona quasi mai (e sono guai)'.**

Disaster Recovery (DR)

❑ Definizione di disastro

Evento che causa il **blocco dell'operatività di sistemi informatici critici**, con un impatto rilevante sull'operatività dell'organizzazione e procurano un **danno esteso e permanente alle strutture di calcolo.**

Possibili cause:

1. Terremoti
2. Inondazioni
3. Incendi
4. Tornado
5. Interruzioni dell'alimentazione elettrica o del gas a seguito di uno o più eventi precedenti
6. Attacchi terroristici o hacker, virus informatici

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Fonti consultate: Certified Information System Auditor (CISA): Review Manual - Information Systems Audit and Control Association (ISACA)

Disaster Recovery (DR) - Classificazione dei sistemi

- **Critical**
  - Il sistema va rimpiazzato con uno identico.
  - Operazioni **non riproducibili manualmente.**
  - Tolleranza alla indisponibilita' molto bassa.
  - Costo inoperativita' molto alto.
- **Vital**
  - La funzione puo' essere eseguita **manualmente per periodi di tempo molto brevi.**
  - Bassa tolleranza alla indisponibilita'.
  - Costo inoperabilita': alto, con possibile attesa del ripristino fino a 5 gg.
- **Sensitive**
  - La funzione puo' essere eseguita **manualmente per periodi di tempo prolungati.**
  - Tolleranza alla inoperativita': media.
  - Costo inoperabilita: medio, con costi aggiuntivi relativi a personale addizionale.
- **Non sensitive**
  - La funzione puo' essere eseguita manualmente, con basso impatto.
  - Richiede pochi sforzi per il riallineamento.

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Vedi Note

Fonti consultate: **Certified Information System Auditor (CISA): Review Manual - Information Systems Audit and Control Association (ISACA)**

Ogni società dovrebbe avere una strategia complessiva di continuità dei servizi, sulla base della quale definire un **piano dettagliato di continuità (BCP)**
Deve contenere:

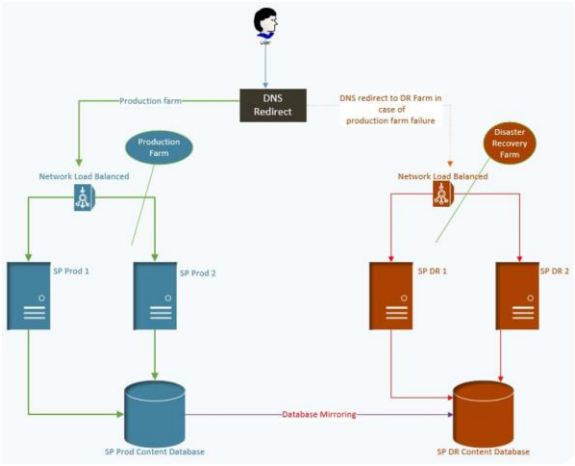
- **Risk assessment**: identificare i sistemi che supportano i processi aziendali critici
- Business impact: analizzare il costo della perdita dei sistemi critici
- Sviluppare il piano per ripristinare le funzionalità IT (Detailed recovery plan – DRP) – Questo contiene le procedure operative di rispristino in base all'architettura prescelta per il Disaster Recovery
- Sviluppare un piano di dettaglio per far funzionare i processi critici nel periodo di crisi (Business continuity Plan BCP)

Inoltre il piano deve essere collaudato (test) ed i risultati analizzati per modificarlo ed aggiornarlo

Fonti consultate: **Certified Information System Auditor (CISA): Review Manual - Information Systems Audit and Control Association (ISACA)**

Disaster Recovery (DR)

- Il **DNS** si occupa di reindirizzare le richieste degli utenti al sito di DR
- I dati sono mantenuti allineati in real-time con il data mirroring

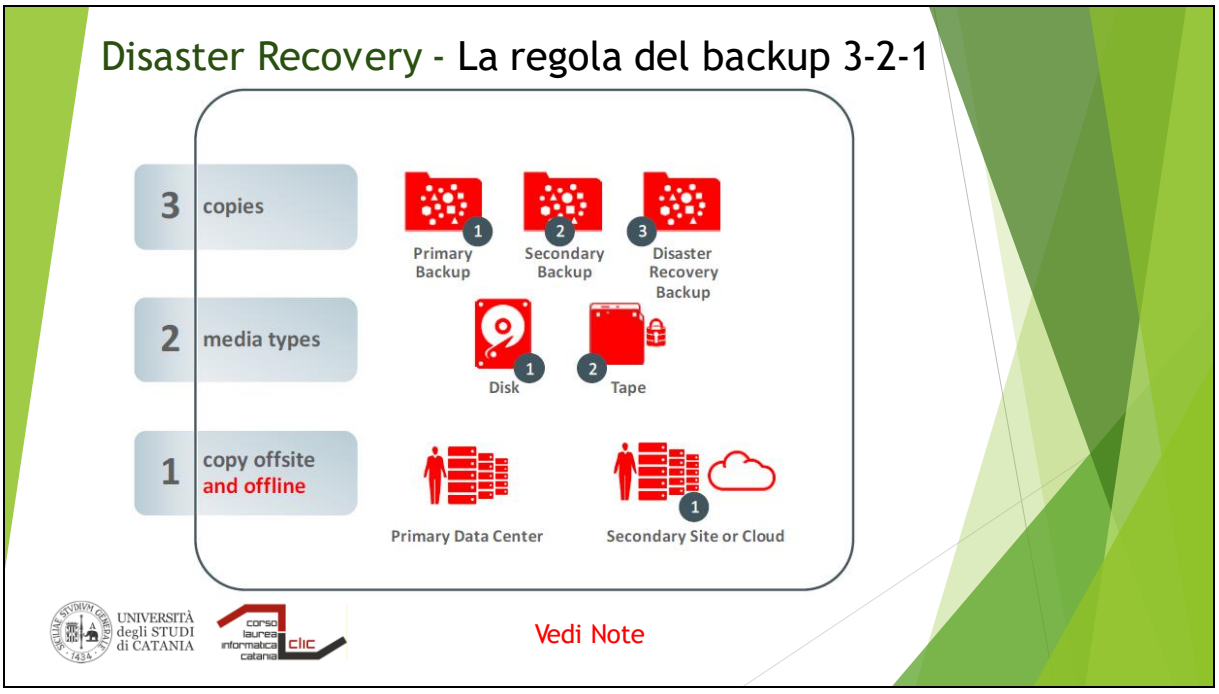


Vedi Note

Lo schema rappresenta il sistema Microsoft Sharepoint ma viene utilizzato a solo scopo di esempio essendo semplice ma completo.

Durante la fase di downtime del sito primario (in blu) si modifica il puntamento del DNS in modo che gli utenti possano continuare a puntare all'indirizzo abituale, che però viene reindirizzato al sito secondario.

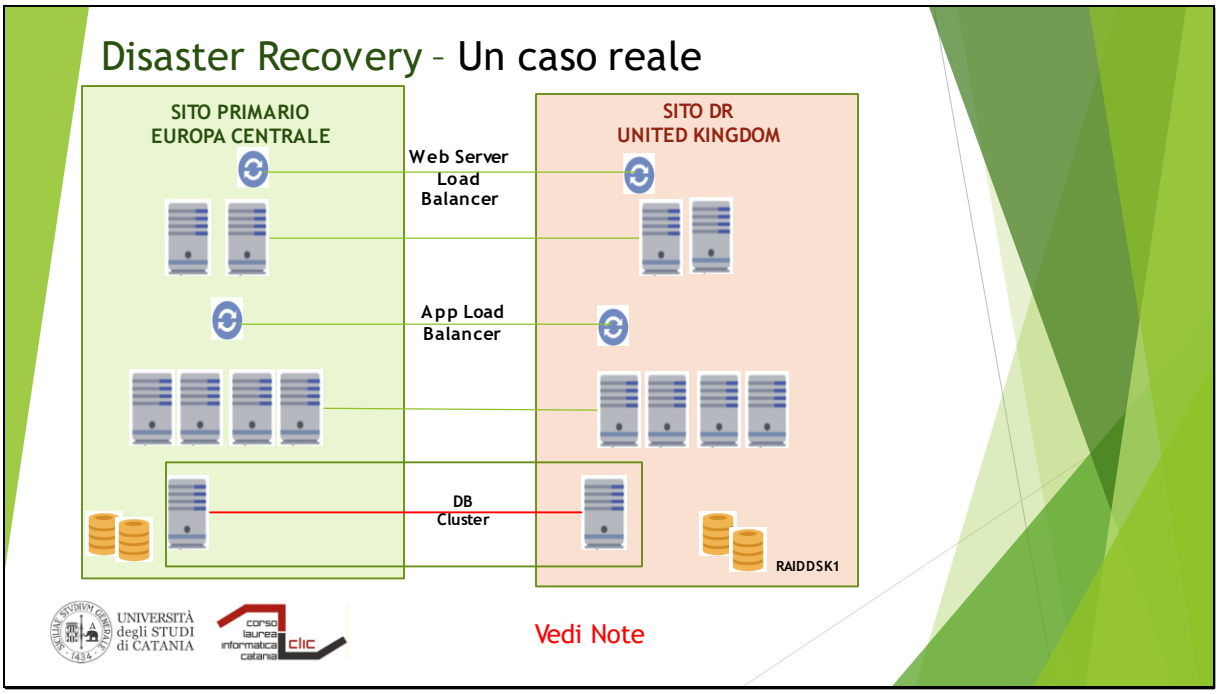
I dati sono stati tenuti aggiornati con tecniche di data replication, oppure esistono beckup che possono ripristinare il dato nei tempi previsti



La regola del backup 3-2-1 stabilisce che:

1. **Ci siano sempre tre copie dei dati**
2. **Si utilizzino due diverse tecnologie di memorizzazione (media type)**
3. **Una copia dei dati sia fuori sede e fuori linea (offline)**

Esempi. Un attacco hacker potrebbe consistere nel prendere il controllo di un utente amministratore IT che distrugge i dati e le copie in linea di backup.
Una copia offline oppure online ma situata in un sito remoto non accessibile direttamente dal sito primario oppure ancora offline (nastro) ed in u sito remoto, sono tecniche che proteggono da attacchi di questo tipo.



La Web Server FARM è composta da **quattro server Web**, due in esecuzione nel sito United Kingdom e due in esecuzione in Europa Centrale.
--> Distribuzione geografica dei server.

Tutti i server Web (LB) sono in esecuzione contemporaneamente nella **configurazione ACTIVE/ACTIVE**. Questa configurazione può garantire la massima disponibilità per il livello Web.

La stessa strategia è stata implementata per il livello del server delle applicazioni. **Otto Application Server sono bilanciati tra i due siti.**

Il cluster del DBMS è installato su un file system esportato via NFS dal NAS (Network Area Storage).
L'elevata disponibilità dei file system è garantita dal mirroring dell'archiviazione.

Il **database gira come singola istanza ACTIVE/PASSIVE su due nodi di un cluster PoweHA**, con un nodo in GB e uno in Europa centrale.
L'archiviazione dei dati è replicata online da EMC SRDF [18] (Symmetrix Remote Data Facility). SRDF garantisce la replica dei dati del database dal sito primario al sito secondario.

In caso di disastro, PowerHA comanda ad EMC di rendere scrivibili i dischi, che si trovano su un array di archiviazione secondario. Quindi i nodi del cluster secondario possono avviare l'istanze DB.

L'architettura implementata per i componenti di cui sopra (Web, App e DBMS) **rappresenta una soluzione ottimale in termini di massima disponibilità.**

Domande di test

Domande di test

Domanda 12
Un sistema in HA deve garantire:

1. Che non sia mai raggiunta la soglia di disponibilità del 99.99%.
2. Che il planned downtime sia almeno il 30% del tempo totale di lavoro.
3. Fronteggiare il downtime causato da una qualsiasi ragione e mitigarne gli effetti.
4. Adeguare la capacità elaborativa ad un livello di carico crescente.

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Risposta: 3
Risposta 4 errata perchè è relativa alla scalabilità
Ris 1 e 2 sono l'opposto di requisiti di un sistema HA

Domande di test

Domanda 13
Le tecnologie in uso per la continuità dei processi sono (scegliere due risposte):

1. Failover Services, tramite i Failover clusters
2. Reverse proxy
3. Scalable Services tramite Load balancing
4. Switch multiporta

Risposte: 1 e 3
Risposta 2 errata perchè è relativa agli accessi alla rete Internet
Ris 4 non ha nessun senso

Domande di test

Domanda 14
Alcune caratteristiche di Failover service che gira su di un cluster (scegliere tutte le opzioni corrette)

1. Se fallisce il riavvio sullo stesso nodo, il server logico viene riavviato automaticamente su un nodo attivo
2. Esiste una sola istanza del processo attiva ad un certo istante
3. Il failover ad un altro nodo richiede l'intervento utente
4. Il failover ad un altro nodo non richiede riconfigurazione client
5. Il failover non avviene se la macchina ha meno di 4GB RAM

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Risposte: 1, 2 e 4
Risposta 3 errata
Risposta 5 non ha nessun senso

Domande di test

Domanda 15
Durante failover occorre fermare il sistema e riconfigurare l'indirizzo di rete del server logico

1. Vero. Altrimenti gli utenti non riescono a puntare alla macchina di failover
2. Vero. Esiste uno script di sistema che si lancia in batch per ripulire i registry del server ed assegnare un nuovo IP
3. Vero. A sistema fermo si configura l'Alias e si riavvia
4. Falso. L' IP alias consente di spostare un server logico ad un server fisico differente

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic catania

Risposta: 4 – si veda «Failover di un server logico»

Domande di test

Domanda 16
Il cluster software management controlla la disponibilità dei nodi e dei servizi attivi nel cluster tramite:

1. Chiamate continue tramite Address Resolution Protocol
2. Inviando broadcast di rete a tutti i sottositemi disco per verificarne il tempo di risposta
3. Heartbeat connection
4. E' il nodo che cade che invia una richiesta al cluster software management

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Risposta: 3 – si veda «Cluster management software»

Domande di test

Domanda 17

Un volume di dischi condiviso ed accessibile da tutti i server del cluster:

1. Deve essere dimensionato in modo da supportare il mirroring
2. E' un requisito fondamentale di un cluster e tutti i nodi ne sono proprietari simultaneamente
3. E' un requisito fondamentale di un cluster per la gestione del failover
4. E' opzionale purchè ogni server abbia un disco privato di almeno 1 TB

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

Risposta: 3 – si veda «Cluster management software»

Domande di test

Domanda 18

In caso di indisponibilità di un servizio su un nodo, per il failover si procede come segue:

1. L'operatore spegne e riavvia il server dove è avvenuto il malfunzionamento
2. Il cluster software management rileva il problema, tenta un riavvio sullo stesso server e, se fallisce, sposta il server logico su un altro nodo del cluster
3. L'operatore avvia il server passivo e monta un nastro di backup
4. Il cluster lancia un comando di shutdown/immediate al DB server e riavvia il server logico sul nodo passivo

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

Risposta: 2 – si veda «Cluster management software»

Domande di test

PROBLEMA 1
Si considerino le tre applicazioni seguenti:

A – **Applicazione CRM di call centre**. L'applicazione è disponibile H24 ed il suo DB server in media richiede 4 CPU@2GHz al 65% di carico e 32 GB RAM. Si osserva un pattern ricorrente di picco al Lunedi, Mercoledi e Venerdi tra le 9 e le 12 del mattino: la richiesta sale a 4 CPU@2GHz al 90% di carico e 40 GB RAM
B – **Applicazione Loyalty.** L'applicazione è disponibile 5x12. Durante il giorno il carico online in media richiede 1 CPU@2GHz al 15% di carico e 2 GB RAM. Durante la notte quando gira il batch bisettimanale di calcolo dei punti, la richiesta sale a 4 CPU@2GHz all' 80% di carico e 38 GB RAM
C – **Applicazione sito web di consultazione**. L'applicazione è disponibile H24. Il carico non eccede mai 1 CPU@2GHz al 5% di carico e 512MB RAM

Si scelga una soluzione e si commenti:

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Domande di test

PRoblema no. 1 - opzioni

1. Cluster di TRE NODI configurato come segue:
   - 4 CPU@2GHz + 48 GB RAM per nodo;
   - Un server logico per UNA SOLA applicazione attiva;
   - Passivo per un altro nodo;
   - App. A attiva su nodo N1, Failover su N3
   - App. B attiva su nodo N2, Failover su N1
   - App. C attiva su nodo N3, Failover su N2

2. Cluster di DUE NODI configurato come segue:
   - 8 CPU@2GHz + 80 GB RAM
   - App. A attiva su nodo N1, Failover su N2
   - App. B e C attive su nodo N2, Failover su N1

3. Cluster a DUE NODI, configurato come segue:
   - 6 CPU@2GHz e 78 GB RAM per nodo
   - App. A attiva su nodo N1, Failover su N2
   - App. B e C attive su nodo N2, Failover su N1

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

Domande di test

Problema no. 1 - risposte

1. Cluster TRE NODI / 4 CPU@2GHz + 48 GB RAM – Soluzione possibile ma molto costosa perché le macchine che ospitano B e C sono fortemente sottoutilizzate
2. Cluster a due nodi, ognuno con 8 CPU@2GHz e 80 GB RAM – soluzione ottimale.
   (a) Al picco diurno sono richieste:
   - 4 CPU@2GHz al 90% + 1 CPU@2GHz al 15% + 1 CPU@2GHz al 5%
   - 40GB + 2 GB + 512MB RAM

   (b) Al picco notturno sono richieste:
   - **4 CPU@2GHz al 65% + 4 CPU@2GHz all' 80% + 1 CPU@2GHz al 5%**
   - 32GB + 38 GB + 512MB RAM

   Quindi nel caso (b) circa 150% di 4CPU= 6CPU ma che sarebbero al 100%. Quindi con 8CPU e 80GB RAM rimane sufficiente headroom per ulteriori picchi temporanei
3. Cluster a due nodi, ognuno con 6 CPU@2GHz e 78 GB RAM. Non è possibile. Al limite assoluto del 100% applicativo senza contare servizi di sistema operativo.

Domanda: Cosa succede se la RAM fisica va al 100% ** vedi note **

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Se la RAM fisica va al 100%, il sistema operativo comincia ad usare lo swap su disco per farsi spazio in memoria centrale, riducendo drasticamente la performance. Se inoltre la CPU è al 100% il sistema diventa lentissimo («si sdraia»)

Domande di test: note

- Come **misurare la percentuale di utilizzo della cpu** da parte di un processo?
- Linux: **cpustat** (autore Colin Ian King)
- ES: $ cpustat –g –n 5 –a
  - -a calcola percentuale totale rispetto a tutti i core. ES: una misurazione del 20% su un core per un sistema a 4 core vale il 5% su tutti i core
  - -n 5 richiede il campionamento sui 5 processi che richiedono piu CPU
  - -g calcola il "grand total" ovvero la media di tutti i tempi di CPU del processo sull'intera durata del campionamento.

Domande di test

Domanda 19

Il numero massimo di ore di downtime per un'applicazione 24x365, con una percentuale di availability contrattuale >= 99% sarà:

1. Variabile in funzione del MTBF
2. Dipendente dalle condizioni stabilite nel contratto
3. Sempre maggiore di 200 ore/anno
4. Sempre minore stretto di 100 ore/anno

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Risposta: 4 – si veda «Misurare la High Availability»

Domande di test

Domanda 20
Quando ci sono più unità dello stesso tipo, il valore totale del MTBF:

1. E' la somma di tutti i MTBF quindi più alto del valore singolo
2. E' il valore massimo del MTBF tra i componenti delle unità: ad es. disco, ventole, alimentatori
3. E' il MTBF diviso per il numero di unità, diventando quindi molto più basso
4. E' indifferente se le unità sono in LB

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania clic

Risposta: 3 – si veda «Misurare la High Availability
»

Domande di test

Domanda 21
Sistemi scalabili o anche load balanced (**due risposte**):

1. Processi applicativi che possono essere istanziati più volte su più application servers
2. Esiste una sola istanza del processo attiva ad un certo istante
3. Se un Processo fallisce su di un server le nuove connessioni saranno reindirizzate ad un altro server
4. Girano su cluster a due o più nodi

Risposte: 1 e 3 – Le altre risposte siriferiscono ai failover services - si veda «Scalable Service – Load Balancing»

Domande di test

Problema no. 2
Si consideri lo scenario applicativo seguente:

Applicazione CRM di call centre.

- L'applicazione serve al picco **5000 utenti connessi**, di cui **500 concorrenti.**
- L'applicazione richiede **0.5CPU@2.5GHz e 5GB RAM per servire 50 utenti concorrenti.**
- Tutti gli utenti connessi ma non concorrenti richiedono ulteriori 5GB di RAM. Si assume che il carico ottimale di CPU non ecceda il valore di 80%.
- L'applicazione è **mission critical** e come processo puo' essere istanziato più volte.

Si scelga una soluzione e si commenti:

Domande di test

Problema no. 2 – Calcolo requisiti

- **500 utenti concorrenti**
- 0.5cpu@2.5 ghz * 10 = 5 CPU@2.5 ghz
- 5gb ram * 10 = 50 gb
- Restanti utenti connessi
- 5gb ram

TOT: 5 CPU@2.5 ghz + 55gb RAM al 100%

Carico/configurazione ottimale: Picco <= 80% risorse

- 5CPU/08 = 6.25CPU ~ **6CPU**
- 55/0.8 = 68gb ram ~ **64gb**

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic catania

Domande di test

Problema no. 2 – Opzioni

- **Un** NODO 6 CPU@2.5GHz e 64 GB RAM che funge da server applicativo.
  - ?
- DUE NODI 4 CPU@2.5GHz e 32 GB RAM: carico in load balancing sui due nodi che fungono da server applicativi
  - ?
- TRE NODI 3 CPU@2.5GHz e 32 GB RAM: Carico in load balancing sui tre nodi server applicativi.
  - ?

Domande di test

Problema no. 2 – Commenti

- **Un** NODO 6 CPU@2.5GHz e 64 GB RAM che funge da server applicativo.
  - !! NO High availability! Cade il nodo, nessuna applicazione
- DUE NODI 4 CPU@2.5GHz e 32 GB RAM: carico in load balancing sui due nodi che fungono da server applicativi
  - !! Se cade un nodo, carico supererebbe il 100% delle risorse durante i picchi di carico
- TRE NODI 3 CPU@2.5GHz e 32 GB RAM: Carico in load balancing sui tre nodi server applicativi.
  - OK. Se cade un nodo, avremo a disposizione 6 cpu e 64 gb di ram complessivi in load balancing..

Domande di test

Problema no. 3

Un server di rete dispone di 3 unità disco da 5TB l'una. Quale strategia offre la soluzione di fault tolerance più economica per i dati di rete memorizzati sul server e richiede un tempo massimo inferiore ad un'ora?
Si scelga una soluzione e si commenti:

1. RAID Livello 0
2. Backup su nastro
3. Raid Livello 5
4. Raddoppio delle unità disco di pari caratteristiche

Domande di test

Problema no. 3 - Risposte

Un server di rete dispone di 3 unità disco SCSI da 5TB l'una. Quale strategia offre la soluzione di fault tolerance più economica per i dati di rete memorizzati sul server e richiede un tempo massimo inferiore ad un'ora?
Si scelga una soluzione e si commenti:

1. RAID Livello 0
   - NO. Non fornisce fault tolerance (solo striping!)
2. Backup su nastro
   - NO. Troppo lento..
3. Raid Livello 5
   - OK. Striping + parita (fault tolerance, spazio disponibile85% circa)
4. Raddoppio delle unità disco di pari caratteristiche
   - NO. Soluzione troppo costosa

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

Risposta 1 – Errata. RAID 0 o striping del disco non garantisce una fault tolerance; infatti non fornisce ridondanza del dato

Risposta 2 – Errata. Il backup su nastro è un sistema semplice ed economico per ridurre al minimo il rischio di perdita dei dati. Tuttavia può essere troppo lenta in fase di backup e riprirstino per soddisfare i requisiti

Risposta 3 - **Corretta**. RAID 5, striping con parità, è ilmetodo più comune per garantire la fault tolerance. RAID 5 copia i dati di parità su tutti i dischi per poter ricostruire sempre il dato corrotto di un disco. La perdita di capacità è minore o uguale al 35%

Risposta 4 – Errata. Duplicare i dischi, aggiungendo i rispettivi controller, consentirebbe di creare una copia dei dati di tutti i dischi. Questa soluzione non rispetta i criteri di economicità richiesti

Domande di test

Problema no. 4

Si consideri lo scenario seguente.

La società telefonica W dispone, tra le altre, di due applicazioni per le quali deve essere garantita l'alta disponibilità.

1. **Applicazione di call centre e vendita**. Applicazione operativa **H24**, che deve garantire una disponibilità del **99.95%**. Il DB dell'applicazione è installato sul nodo A di un cluster Active-Active
2. **Applicazione per fornire alla Magistratura i dati di traffico per indagini penali.** L'applicazione è di tipo 8x5 (8 ore 5 gg a settimana) ma in caso di richieste della Magistratura, il dato deve essere messo a disposizione entro le 24 ore successive. Il DB dell'applicazione è installato sul nodo B dello stesso cluster del Call Center (punto 1)

Domande di test

Problema no. 4 (cont.)

I **due nodi del cluster** sono dimensionati in modo che in caso di **failover** di un nodo, **il secondo nodo regge il carico**, seppur con la **CPU al 98% e la RAM al 95%**

Il caso. Un system administrator cancella per errore una parte dei file di sistema da una cartella del DBMS del sistema di Call Centre che, successivamente, ha avuto un arresto inatteso.
Il sistema di failover ha riavviato il servizio sul nodo B ed il servizio è stato ripristinato. Durante il giorno, la CPU mostra occasionali picchi di carico al 100% e la memoria RAM rimane sotto al 98% di occupazione.

In seguito **saranno proposte 4 differenti procedure di ripristino** del nodo A.

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

Domande di test

Problema no. 4 - Risposte

1. **Durante la notte si procede con lo shutdown del cluster. Si effettua il restore dei file di sistema del DB sul nodo A**, che ripristina la funzionalità dell'applicazione di call center.
   - La durata totale prevista delle operazioni è di 3 ore (< 0.05%) .
   - Si riavvia il cluster con il Call Centre tornato sul nodo A
2. **La Magistratura emette un'ordinanza per il ripristino immediato della funzionalità del nodo A.**
3. **Durante la notte si procede con lo shutdown del cluster. Si effettua il restore dei file di sistema del DB di call center su entrambi i nodi.**
   - Successivamente si riavvia il cluster con il Call Centre tornato sul nodo A.
   - La durata totale prevista delle operazioni è di 7 ore

Domande di test

Problema no. 4 (risposte)

4. Si effettua il restore dei file di sistema del DB sul nodo A, senza arrestare il cluster, mentre le applicazioni funzionano.

- Successivamente si effettua il **test di funzionamento del servizio DBMS** che conferma il ripristino la funzionalità dell'applicazione di call center.
- **Non è necessario curarsi della durata dell'operazione**, che viene effettuata durante il giorno.
- Si effettua **lo switch del server logico del DB Call Centre sul nodo A.**
- Non sono necessarie ulteriori azioni.

Domande di test

Problema no. 4: Commenti alle risposte

1. Arresto del cluster. Errata. Non è necessario fermare tutto il cluster. L'operazione sarebbe contenuta nel tempo di arresto totale annuale al 99.95, di 4 ore. Inutile sprecare tutta la finestra disponibile per un'azione non richiesta.

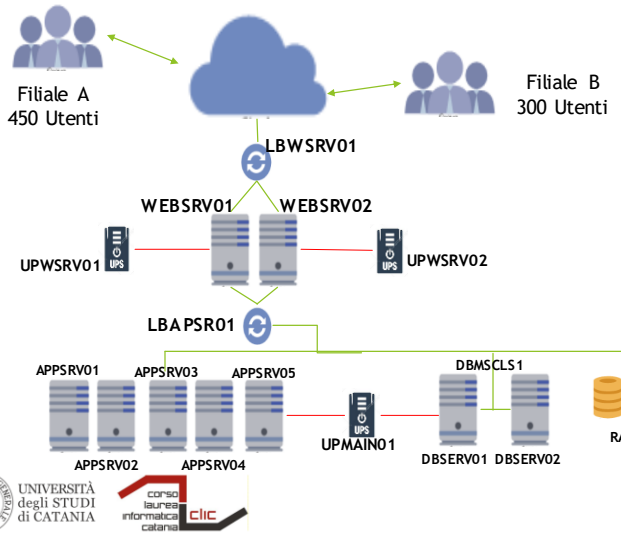
2.Ordinanza della Magistratura. Errata. Per l'utente o chi usufruisce del servizio, la configurazione HA è trasparente.

3.Arresto del cluster e ripristino file su entrambi nodi – Errata. Rispetto alla 1, si ripristinano i file anche sul nodo «sano» è l'operazione comunque sarebbe in eccesso sul max downtime annuale.

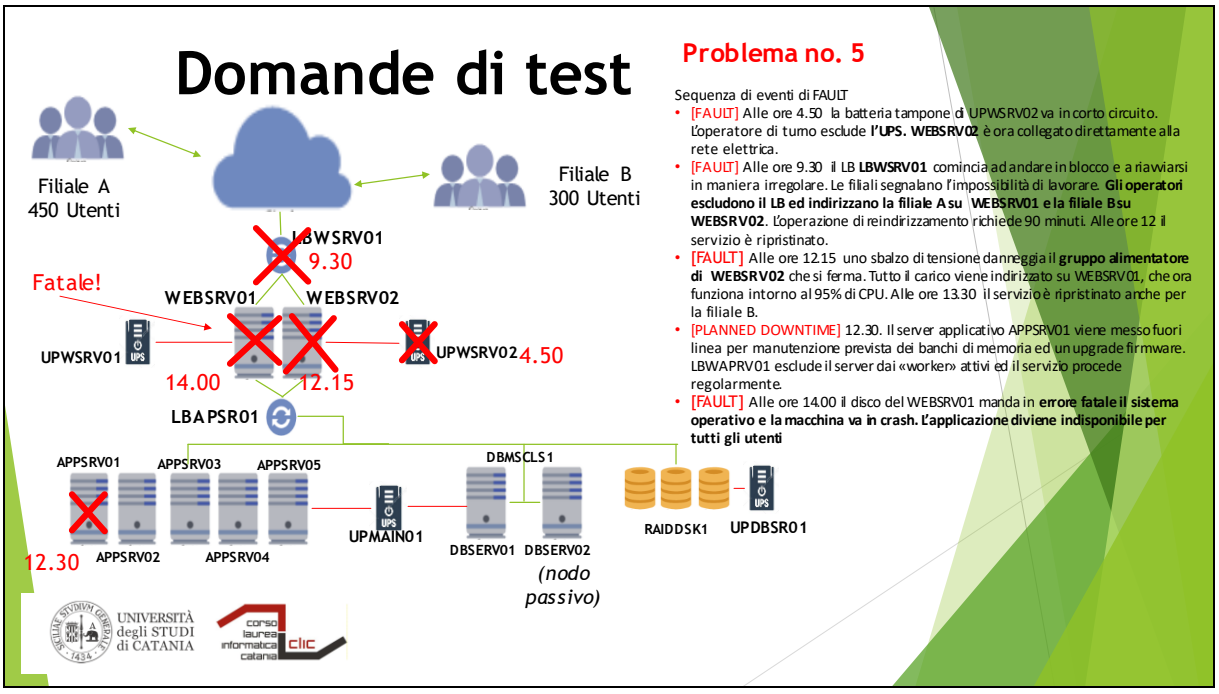
4.Ripristino file sul nodo A a servizi aperti. Corretta. I**l sistema sta lavorando più o meno come previsto in condizioni di failover** (occasionali picchi di carico al 100% e la memoria RAM che rimane sotto al 98% di occupazione). E' quindi possibile effettuare l'operazione durante il giorno. Consigliabile effettuare lo switch durante la notte per avere un impatto minore sul numero di utenti connessi.

Domande di test

Problema no. 5



- Applicazione 12x5x52 settimane, al 99.5% di disponibilità, per un **downtime totale ammesso di 16 ore.**
- Totale utenti: **750**
- **Due web server in LB** (LBWSRV01 – **SPOF!**): WEBSRV01, WEBSRV02. Il singolo web server ha 2 CPU e può reggere 800 utenti al 100% delle risorse.
- Ogni web server ha il suo **alimentatore UPS**: **UPWSRV01, UPWSRV02**
- Cinque **application server in LB** (LBAPSRV01): **APPSRV01, APPSRV02, APPSRV03, APPSRV04, APPSRV05.**
- Tre application server possono reggere 800 utenti al 90% delle risorse. Ogni application server ha 4 CPU.
- Un **cluster** ospita il **DBMS** server (6 CPU): DBMSCL1, che si appoggia ad un **gruppo di dischi** in configurazione **RAID**. **Carico medio 65%, con picco all' 80%**.
- Tutti gli application server, cluster e dischi hanno un'alimentazione in **continuità UPS**
- Il disco interno del WEBSRV01 si avvicina al limite del suo MTBF (!!)



Sequenza di eventi (legge di Murphy)

- Alle ore 4.50 am la batteria tampone di UPWSRV02 va in corto circuito. L'operatore di turno esclude l'UPS. WEBSRV02 è ora collegato direttamente alla rete
- Alle ore 9.30 am il LB LBWSRV01 comincia ad andare in blocco e a riavviarsi in maniera irregolare. Le filiali segnalano l'impossibilità di lavorare. Gli operatori escludono il LB ed indirizzano la filiale A su WEBSRV01 e la filiale B su WEBSRV02. L'operazione di reindirizzamento richiede 90 minuti. Alle ore 12 il servizio è ripristinato
- Alle ore 12.15 pm uno sbalzo di tensione danneggia il gruppo alimentatore di WEBSRV02 che si ferma. Tutto il carico viene indirizzato su WEBSRV01, che ora funziona intorno al 95% di CPU. Alle ore 1.30 pm il servizio è ripristinato anche per la filiale B.
- Il server applicativo APPSRV01 viene messo fuori linea per manutenzione prevista dei banchi di memoria ed un upgrade firmware. LBWAPRV01 esclude il server dai «worker» attivi ed il servizio procede regolarmente.
- Alle ore 2 pm il disco del WEBSRV01 manda in errore fatale il sistema operativo e la macchina va in crash. **L'applicazione diviene indisponibile per tutti gli utenti**

Domande di test

Problema no. 5 - risposte

1. L'Amministratore Delegato comunica al Direttore Vendite che le filiali non lavoreranno per 72 ore, per dare tempo di riparare l'hardware.
2. Entro 48 ore il LB LBWSRV01 ed i WEBSRV01 e WEBSRV02 saranno riparati, consentendo il riavvio completo delle funzionalità.
   - NO. Soluzioni 1 e 2 implicano tempi di downtime superiori a quelli ammessi ovvero 16 ore.
3. Si installa un web server WEBSRV03 sul nodo fisico passivo DBSERV02:
   - Tutto il carico delle filiali viene indirizzato su DBSERV02
   - Il servizio riprende in circa 1.5 ore
   - Tempo di intervento OK + Semplicita di intervento.
   - Manca alta disponibilita.
   - Se nodo primario DB andasse in failover sul nodo secondario: in condizioni di massimo carico 6CPU al 65% = 3.9 CPU + 2 CPU (webSRV) al 100% quindi andrebbe sotto stress al picco

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

1. Errata – Viola il limite ammesso del downtime
2. Errata – Viola il limite ammesso del downtime
3. Ok – Minimo tempo di intervento e massima semplicità di intervento,macchina sovradimensionata rispetto alla necessità (6 CPU contro 2 CPU/100% per reggere tutto il carico). Manca alta affidabilità. Anche in caso di failover del nodo primario del DB la macchina reggerebbe il carico: 6CPU al 65% = 3.9 CPU + 2 CPU. Andrebbe sotto stress al picco, con CPU oltre il 100% e processi accodati per l'esecuzione.
4. Tecnicamente possibile - Si veda 'Sequenza SYN- SYN/ACK – ACK' – e fornirebbe alta disponibilità. Più complessa e lunga nell'esecuzione. Tutta la giornata sarebbe quasi interamente perduta.
5. Tecnicamente possibile - Si veda 'Sequenza SYN- SYN/ACK – ACK' – e fornirebbe alta disponibilità. Più complessa e lunga nell'esecuzione. Tutta la giornata sarebbe quasi interamente perduta. Più veloce della soluzione 4

Domande di test

Problema no. 5 - risposte

4. Si installano i) quattro nuovi web server WEBSRV03 - WEBSRV06 su tutti gli application server operativi APPSRV02- APPSRV05 + ii) bilanciamento da LBAPSRV01 esistente. Il servizio riprende dopo 4 ore, perchè occorre anche riconfigurare il load balancer.
   - (-)Soluzione più complessa e lunga (4 ore vs 1.5 ore per soluzione no. 3).
   - (+)Alta disponibilita
5. Si installa un i) web server WEBSRV03 sul nodo fisico passivo DBSERV02 ed un web server ii) WEBSRV04 sull'application server APPSRV05. I web server vengono bilanciati da LBAPSRV01. Il servizio riprende dopo 3.5 ore, perchè occorre anche riconfigurare il load balancer.
   - (-) 3.5 ore vs 1.5 ore per soluzione no.3 vs 4 ore per soluzione no. 4
   - (+) Alta disponibilita'.

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

1. Errata – Viola il limite ammesso del downtime
2. Errata – Viola il limite ammesso del downtime
3. Ok – Minimo tempo di intervento e massima semplicità di intervento,macchina sovradimensionata rispetto alla necessità (6 CPU contro 2 CPU/100% per reggere tutto il carico). Manca alta affidabilità. Anche in caso di failover del nodo primario del DB la macchina reggerebbe il carico: 6CPU al 65% = 3.9 CPU + 2 CPU. Andrebbe sotto stress al picco, con CPU oltre il 100% e processi accodati per l'esecuzione.
4. Tecnicamente possibile - Si veda 'Sequenza SYN- SYN/ACK – ACK' – e fornirebbe alta disponibilità. Più complessa e lunga nell'esecuzione. Tutta la giornata sarebbe quasi interamente perduta.
5. Tecnicamente possibile - Si veda 'Sequenza SYN- SYN/ACK – ACK' – e fornirebbe alta disponibilità. Più complessa e lunga nell'esecuzione. Tutta la giornata sarebbe quasi interamente perduta. Più veloce della soluzione 4

Domande di test

Domanda 24
Si considerino i dischi RAID. La soluzione che ottimizza l'utilizzo dello spazio disco disponibile, la velocità di accesso in scrittura e garantisce l'alta disponibilità é:

1. RAID 10 (ovvero 1+0)
2. RAID 0
3. RAID 5
4. RAID 7

Domande di test

Domanda 24 – risposta corretta
Si considerino i dischi RAID. La soluzione che ottimizza l'utilizzo dello spazio disco disponibile, la velocità di accesso in scrittura e garantisce l'alta disponibilità é:

1. RAID 10 (ovvero 1+0 – non ottimizza lo spazio)
2. RAID 0 (solo performance)
3. RAID 5
4. RAID 7 (non esiste)

Domande di test

Domanda 25
Quando si progetta un sistema applicativo in alta disponibilità, occorre concentrarsi principalmente sul software ed i server. Altri Single Point of Failure (SPOF) possono essere eliminati in seguito

1. Possibile. E' credenza comune in azienda che il costo di una arresto temporaneo non valga l'investimento iniziale
2. Falso. Molti componenti possono causare arresti anche prolungati del sistema con costi enormi (ad es. alimentazione elettrica, errore umano, dispositivi di rete)
3. Falso. Bisogna sempre prevedere il backup e recovery
4. Falso. E' necessario che la latenza di rete non ecceda i 100 ms

Domande di test

Domanda 25

Quando si progetta un sistema applicativo in alta disponibilità, occorre concentrarsi principalmente sul software ed i server. Altri Single Point of Failure (SPOF) possono essere eliminati in seguito

La risposta corretta è la 2:

Falso. Molti componenti possono causare arresti anche prolungati del sistema con costi enormi (ad es. alimentazione elettrica, errore umano, dispositivi di rete)

Esistono infatti molti SPOF ed ognuno può causare danni non stimabili a priori in caso di arresto. Disegnando un sistema HA occorre tenere presente tutti i SPOF:

- ✓ Server
- ✓ Load Balance
- ✓ Connettività di rete (cablaggio)
- ✓ Schede di rete
- ✓ Disco di sistema (OS root disk)
- ✓ Disco dati
- ✓ Alimentazione elettrica (power source)
- ✓ Scheda di interfacciamento al disco
- ✓ Sistema Operativo
- ✓ Software applicativo
- ✓ Errore umano

Domande di test

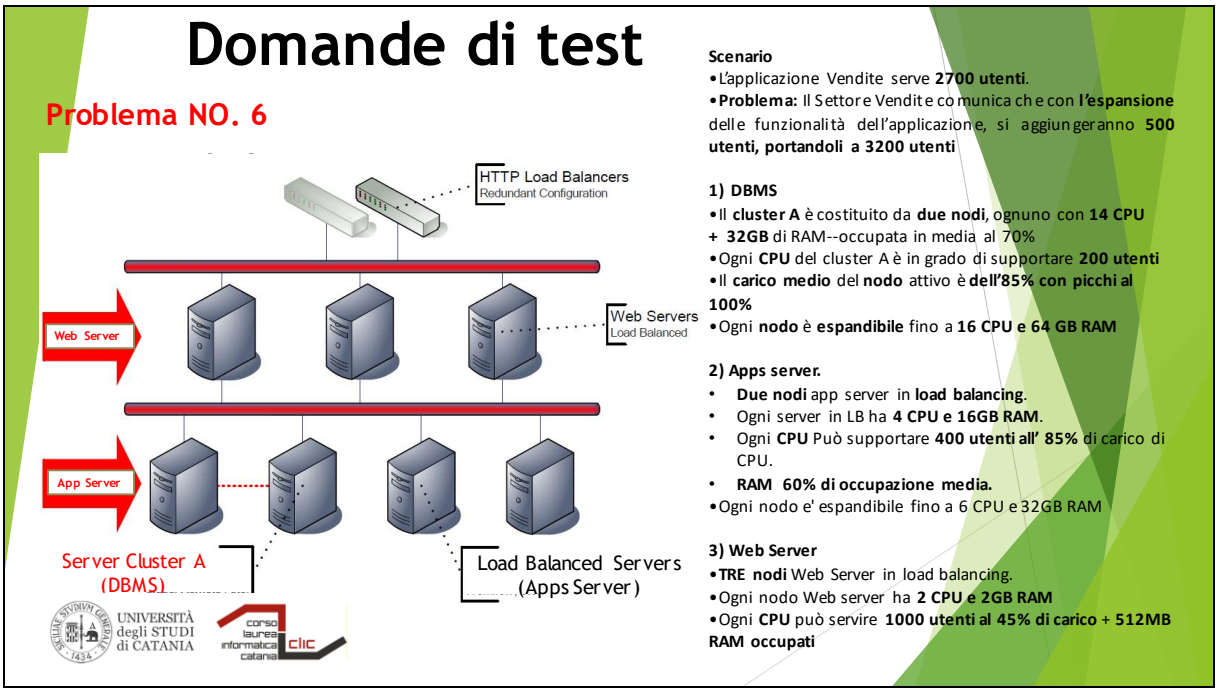
Domanda 26
..... è lento nell'operazione di backup però è la scelta ottimale per velocizzare l'intero Restore.
Si scelga l'opzione corretta.

1. Full Backup
2. Incremental backup
3. Differential backup

Domande di test

Domanda 26
..... è lento nell'operazione di backup però è la scelta ottimale per velocizzare l'intero Restore.
Si scelga l'opzione corretta.

1. Full Backup
2. Incremental backup
3. Differential backup. E' più lento dell'incremental nella fase di backup ma in caso di ripristino, una volta applicata la copia integrale iniziale, con una sola copia del differenziale si riallinea la situazione.



Scenario

- L'applicazione Vendite serve 2700 utenti. Il Settore Vendite comunica che con l'espansione delle funzionalità dell'applicazione, si aggiungeranno 500 utenti, portandoli a 3200 utenti

DBMS

- Il cluster A è costituito da due nodi, ognuno con 14 CPU e 32GB RAM, in media occupata al 70%
- Ogni nodo è espandibile fino a 16 CPU e 64 GB RAM
- Il carico medio del nodo attivo è dell'85% con picchi al 100%
- Ogni CPU del cluster A è in grado di supportare 200 utenti

Apps Server

- Ci sono due Application Server in load balance. Ogni server in LB ha 4 CPU e 16GB RAM.
- Ogni CPU Può supportare 400 utenti all' 85% di carico di CPU. La memoria lavora intorno al 60% di occupazione media.
- E' possibile espandere gli application server fino a 6 CPU e 32GB RAM

Web Server

- Ci sono tre Web Server in load balancing. Ogni Web server ha 2 CPU e 2GB RAM
- Ogni CPU può servire 1000 utenti al 45% di carico e 512MB RAM occupati

Domande di test

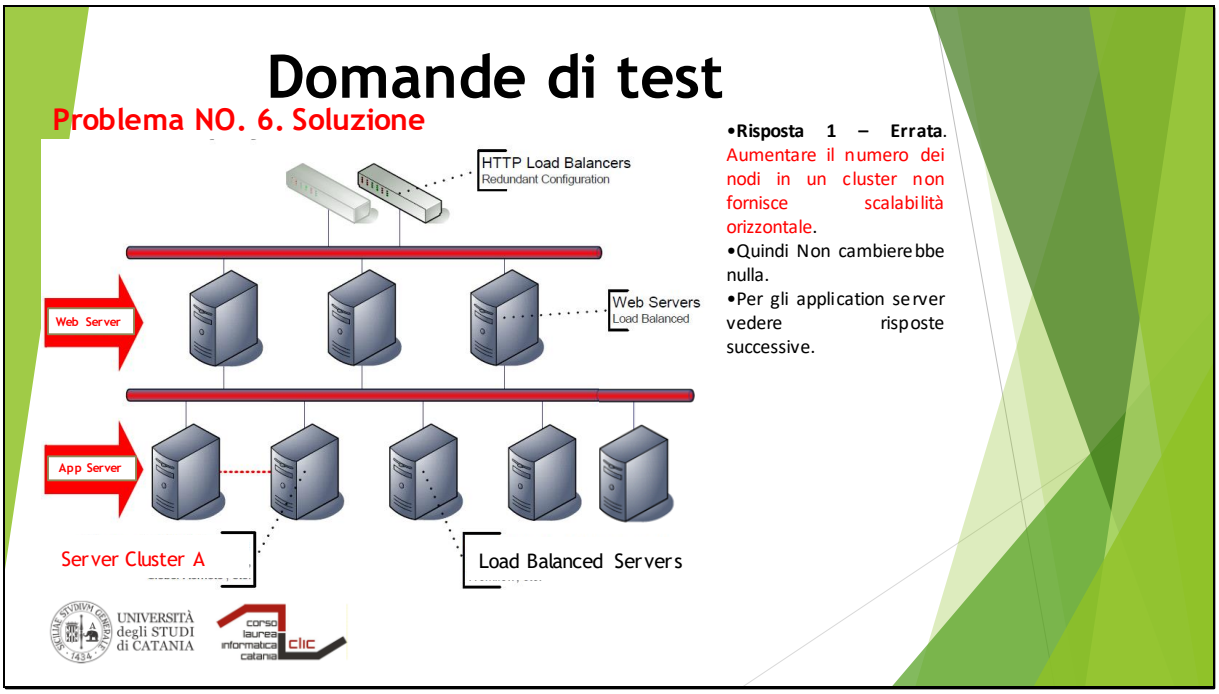
Problema NO. 6

Al fine di supportare l'aumento a 3200 utenti:

1. Si raccomanda di:
   - **modificare il DB cluster, aggiungendo un nodo con 14 CPU e 32GB RAM**. Si otterrebbe in tal modo un cluster a **tre nodi.**
   - Occorre poi **espandere ogni application server ad 6 CPU** lasciando invariata la RAM.

2. Si raccomanda di:
   1. espandere ogni **nodo del cluster**, portandolo a **16 CPU e 48GB RAM.**
   2. Occorre poi espandere ogni **application server a 6 CPU** lasciando invariata la RAM.

3. Si raccomanda di:
   1. sostituire i nodi del cluster A con **due server con 20 CPU e 48GB RAM per nodo.**
   2. Occorre poi espandere ogni **application server a 6 CPU** lasciando invariata la RAM.
   3. Infine si dovrebbe **aggiungere un altro server portando il numero totale a tre in LB**, per evitare che la perdita di una macchina renda il sistema inutilizzabile



Scenario

- L'applicazione Vendite serve 2700 utenti. Il Settore Vendite comunica che con l'espansione delle funzionalità dell'applicazione, si aggiungeranno 500 utenti, portandolo a 3200 utenti

Risposte

- **Risposta 1 – Errata**. Aumentare il numero dei nodi in un cluster non fornisce scalabilità orizzontale. Non cambierebbe nulla. Per gli application server vedere risposte successive

- **Risposta 2 – Errata**. La scalabilità verticale raggiungendo il massimo dell'espansione h/w del nodo, teoricamente possibile, lascerebbe il sistema in sofferenza e non ci sarebbe più modo di fronteggiare aumenti temporanei di carico o di scalare verticalmente.

  Gli application server con due soli server, anche dopo l'espansione al massimo delle capacità, non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

  DBMS

  - Il cluster A è costituito da due nodi, ognuno con 14 CPU e 32GB RAM, la quale RAM in media e' occupata al 70%
  - Ogni nodo è espandibile fino a 16 CPU e 64 GB RAM
  - Il carico medio del nodo attivo è dell'85% con picchi al 100%

- Ogni CPU del cluster A è in grado di supportare 200 utenti

3200 Utenti con 200 utenti/CPU indicano la necessità di 16 CPU. Proiettando il carico attuale avremmo ancora un carico medio del nodo attivo all'85% con picchi al 100%.

Quindi espandendo al massimo la macchina il sistema sarebbe in sofferenza e non avrebbe più modo di scalare verticalmente.

Per quanto riguarda la RAM, il valore medio effettivo usato da 2700 utenti connessi è il 70% di 32GB ossia circa 22.4 GB, cioè circa 8.5 MB per connessione.

Per 3200 utenti servirebbero 26.6 GB. Pertanto sarebbe consigliabile un'espansione a 48GB per avere un margine di sicurezza.

- **Risposta 3 – Corretta**. Si deve aumentare la potenza del server del DBMS cambiando macchina. Per gli application server si scala verticalmente ed orrizzontalmente, aggiungendo un altro server da 6 CPU e 16GB RAM. Infatti due soli server non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

Apps Server

- Ogni server in LB ha 4 CPU e 16GB RAM.
- Ogni CPU Può supportare 400 utenti all' 85% di carico di CPU. La memoria lavora intorno al 60% di occupazione media.
- E' possibile espandere gli application server fino a 6 CPU e 32GB RAM

3200 Utenti con 400 utenti/CPU indicano la necessità di 8 CPU. Proiettando il carico attuale avremmo ancora un carico medio all'85%. Occorre aumentare il numero di CPU a 6 per avere headroom.

La RAM dovrebbe essere espansa come segue: 0.6 * 16GB = 9.6GB utilizzati. Ogni utente richiede: 9.6GB / 1350 = 7.2 MB. Quindi 3200 utenti richiederebbero circa 24GB, ovvero 12GB per macchina. Quindi il valore attuale di capacità di RAM si dimostra sufficiente. Tuttavia si consiglia di espandere la RAM a 24 GB per macchina, per affrontare picchi di carico inattesi.

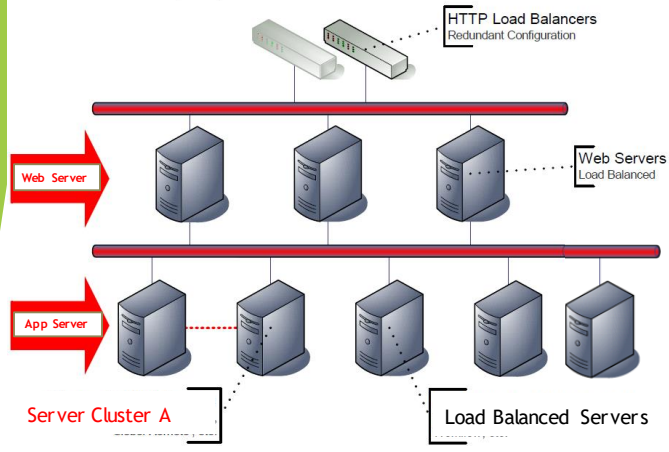
Web Server

- Ogni Web server ha 2 CPU e 2GB RAM
- Ogni CPU può servire 1000 utenti al 45% di carico e 512MB RAM occupati

L'aumento di carico non rappresenta un problema per il rapporto carico/potenza attuale

Domande di test

Problema NO. 6. Soluzione



UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic

- **Risposta 2 – Errata:**
- **DBMS - situazione attuale**
  - Il cluster A è costituito da due nodi, ognuno con 14 CPU e 32GB RAM, la quale RAM in media e' occupata al 70%
  - Ogni CPU del cluster A è in grado di supportare 200 utenti.
  - Il carico medio del nodo attivo è dell'85% con picchi al 100%.
  - Ogni nodo è espandibile fino a 16 CPU e 64 GB RAM

DBMS. CPU:

- **3200 Utenti con 200 utenti/CPU indicano la necessità di 16 CPU.**
- Proiettando il carico attuale avremmo ancora un carico **medio del nodo attivo all'85% con picchi al 100%.**
- Quindi espandendo al massimo la macchina il sistema **sarebbe in sofferenza e non avrebbe più modo di scalare verticalmente.**

DBMS. RAM:

- il valore medio effettivo usato da 2700 utenti connessi è il 70% di 32GB ossia circa 22.4 GB, cioè circa 8.5 MB per connessione.
- **Per 3200 utenti servirebbero 26.6 GB. Pertanto sarebbe consigliabile un'espansione a 48GB** per avere un margine di sicurezza.

CONCLUSIONI: La scalabilità verticale ottenuta mediante l'espansione al massimo delle potenzialità h/w del nodo, teoricamente possibile, **lascerebbe il sistema in sofferenza e non ci sarebbe più modo di fronteggiare aumenti temporanei di carico o di scalare verticalmente.**

Scenario

- L'applicazione Vendite serve 2700 utenti. Il Settore Vendite comunica che con l'espansione delle funzionalità dell'applicazione, si aggiungeranno 500 utenti, portandolo a 3200 utenti

Risposte

- **Risposta 1 – Errata**. Aumentare il numero dei nodi in un cluster non fornisce scalabilità orizzontale. Non cambierebbe nulla. Per gli application server vedere risposte successive

- **Risposta 2 – Errata**. La scalabilità verticale raggiungendo il massimo dell'espansione h/w del nodo, teoricamente possibile, lascerebbe il sistema in sofferenza e non ci sarebbe più modo di fronteggiare aumenti temporanei di carico o di scalare verticalmente.

  Gli application server con due soli server, anche dopo l'espansione al massimo delle capacità, non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

  DBMS

  - Il cluster A è costituito da due nodi, ognuno con 14 CPU e 32GB RAM, la quale RAM in media e' occupata al 70%
  - Ogni nodo è espandibile fino a 16 CPU e 64 GB RAM
  - Il carico medio del nodo attivo è dell'85% con picchi al 100%

- Ogni CPU del cluster A è in grado di supportare 200 utenti

3200 Utenti con 200 utenti/CPU indicano la necessità di 16 CPU. Proiettando il carico attuale avremmo ancora un carico medio del nodo attivo all'85% con picchi al 100%.

Quindi espandendo al massimo la macchina il sistema sarebbe in sofferenza e non avrebbe più modo di scalare verticalmente.

Per quanto riguarda la RAM, il valore medio effettivo usato da 2700 utenti connessi è il 70% di 32GB ossia circa 22.4 GB, cioè circa 8.5 MB per connessione.

Per 3200 utenti servirebbero 26.6 GB. Pertanto sarebbe consigliabile un'espansione a 48GB per avere un margine di sicurezza.

- **Risposta 3 – Corretta**. Si deve aumentare la potenza del server del DBMS cambiando macchina. Per gli application server si scala verticalmente ed orrizzontalmente, aggiungendo un altro server da 6 CPU e 16GB RAM. Infatti due soli server non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

Apps Server

- Ogni server in LB ha 4 CPU e 16GB RAM.
- Ogni CPU Può supportare 400 utenti all' 85% di carico di CPU. La memoria lavora intorno al 60% di occupazione media.
- E' possibile espandere gli application server fino a 6 CPU e 32GB RAM

3200 Utenti con 400 utenti/CPU indicano la necessità di 8 CPU. Proiettando il carico attuale avremmo ancora un carico medio all'85%. Occorre aumentare il numero di CPU a 6 per avere headroom.

La RAM dovrebbe essere espansa come segue: 0.6 * 16GB = 9.6GB utilizzati. Ogni utente richiede: 9.6GB / 1350 = 7.2 MB. Quindi 3200 utenti richiederebbero circa 24GB, ovvero 12GB per macchina. Quindi il valore attuale di capacità di RAM si dimostra sufficiente. Tuttavia si consiglia di espandere la RAM a 24 GB per macchina, per affrontare picchi di carico inattesi.

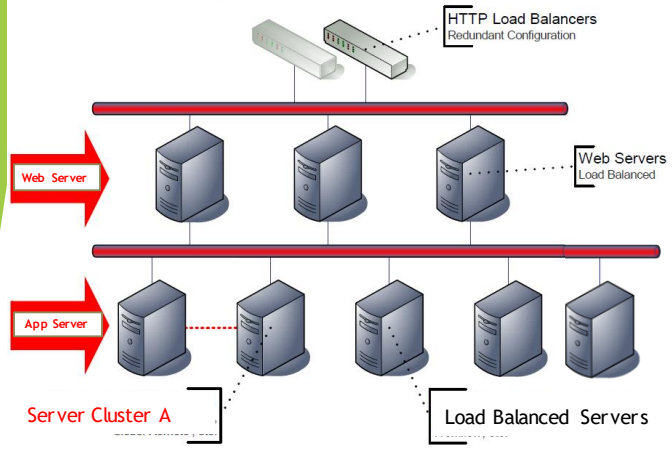
Web Server

- Ogni Web server ha 2 CPU e 2GB RAM
- Ogni CPU può servire 1000 utenti al 45% di carico e 512MB RAM occupati

L'aumento di carico non rappresenta un problema per il rapporto carico/potenza attuale

Domande di test

Problema NO. 6. Soluzione



•Risposta 3 – Corretta:

I) Si aumenta la potenza del server del DBMS cambiando macchina.

II) Per gli application server si scala verticalmente ed orizzontalmente.

I) DBMS (cambiare macchina)
20 CPU + 48 GB per nodo
20 CPU per 3200 utenti (16CPU richieste) OK
48 GB RAM OK (26.6 gb richiesti) OK

II) APP Servers
- Ogni server in LB ha 4 CPU e 16GB RAM.
- 400 utenti per CPU all' 85% di carico di CPU.
- RAM al 60% di occupazione media.
- CPU:
  - 3200 / (400 utenti/CPU) = 8 CPU: con 4+4 CPU si avrebbe ancora carico medio all'85%.
  - Dunque espansione a 6 CPU per avere headroom oltre i 3200 utenti (scalabilita verticale)
  - + 1 server (scalabilita' orizzontale) per affrontare la caduta di un nodo.
- RAM:
  - 0.6 * 16GB = 9.6GB utilizzati.
  - 9.6GB / (2700/2 cioe' 1350) = 7.2 MB.
  - 3200 utenti x 7.2m = 24GB, ovvero 12GB per macchina.
  - Quindi i 16 GB attuali si dimostrano sufficienti. Tuttavia si consiglia di espandere la RAM a 24 GB per macchina, per affrontare picchi di carico inattesi.

III) Web Server
- 2 CPU (max 1000 utenti al 45%) + 2GB RAM per nodo
- 512MB RAM occupati per 1000 utenti

--> L'aumento di carico non rappresenta un problema per il rapporto carico/potenza attuale

Scenario

- L'applicazione Vendite serve 2700 utenti. Il Settore Vendite comunica che con l'espansione delle funzionalità dell'applicazione, si aggiungeranno 500 utenti, portandolo a 3200 utenti

Risposte

- **Risposta 1 – Errata**. Aumentare il numero dei nodi in un cluster non fornisce scalabilità orizzontale. Non cambierebbe nulla. Per gli application server vedere risposte successive

- **Risposta 2 – Errata**. La scalabilità verticale raggiungendo il massimo dell'espansione h/w del nodo, teoricamente possibile, lascerebbe il sistema in sofferenza e non ci sarebbe più modo di fronteggiare aumenti temporanei di carico o di scalare verticalmente.

  Gli application server con due soli server, anche dopo l'espansione al massimo delle capacità, non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

  DBMS

  - Il cluster A è costituito da due nodi, ognuno con 14 CPU e 32GB RAM, la quale RAM in media e' occupata al 70%
  - Ogni nodo è espandibile fino a 16 CPU e 64 GB RAM
  - Il carico medio del nodo attivo è dell'85% con picchi al 100%

- Ogni CPU del cluster A è in grado di supportare 200 utenti

3200 Utenti con 200 utenti/CPU indicano la necessità di 16 CPU. Proiettando il carico attuale avremmo ancora un carico medio del nodo attivo all'85% con picchi al 100%.

Quindi espandendo al massimo la macchina il sistema sarebbe in sofferenza e non avrebbe più modo di scalare verticalmente.

Per quanto riguarda la RAM, il valore medio effettivo usato da 2700 utenti connessi è il 70% di 32GB ossia circa 22.4 GB, cioè circa 8.5 MB per connessione.

Per 3200 utenti servirebbero 26.6 GB. Pertanto sarebbe consigliabile un'espansione a 48GB per avere un margine di sicurezza.

- **Risposta 3 – Corretta**. Si deve aumentare la potenza del server del DBMS cambiando macchina. Per gli application server si scala verticalmente ed orrizzontalmente, aggiungendo un altro server da 6 CPU e 16GB RAM. Infatti due soli server non garantirebbero l'alta disponibilità, in caso di perdita di un nodo

Apps Server

- Ogni server in LB ha 4 CPU e 16GB RAM.
- Ogni CPU Può supportare 400 utenti all' 85% di carico di CPU. La memoria lavora intorno al 60% di occupazione media.
- E' possibile espandere gli application server fino a 6 CPU e 32GB RAM

3200 Utenti con 400 utenti/CPU indicano la necessità di 8 CPU. Proiettando il carico attuale avremmo ancora un carico medio all'85%. Occorre aumentare il numero di CPU a 6 per avere headroom.

La RAM dovrebbe essere espansa come segue: 0.6 * 16GB = 9.6GB utilizzati. Ogni utente richiede: 9.6GB / 1350 = 7.2 MB. Quindi 3200 utenti richiederebbero circa 24GB, ovvero 12GB per macchina. Quindi il valore attuale di capacità di RAM si dimostra sufficiente. Tuttavia si consiglia di espandere la RAM a 24 GB per macchina, per affrontare picchi di carico inattesi.

Web Server

- Ogni Web server ha 2 CPU e 2GB RAM
- Ogni CPU può servire 1000 utenti al 45% di carico e 512MB RAM occupati

L'aumento di carico non rappresenta un problema per il rapporto carico/potenza attuale

LINK NOTEVOLI

1. Esempio di ownership del disco - **Cluster Shared Volumes (CSV): Disk Ownership**
https://techcommunity.microsoft.com/t5/failover-clustering/cluster-shared-volumes-csv-disk-ownership/ba-p/371352#

2. Oracle Solaris cluster
https://www.oracle.com/solaris/technologies/cluster-overview.html

3. HP Service Guard
https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c02960047

4. **Microsoft MSCS**
https://docs.microsoft.com/en-us/previous-versions/windows/desktop/mscs/cluster-service

5. CISCO - Network Address Translator (NAT) – FAQ
https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica clic catania

LINK NOTEVOLI

6. World Wide Web Consortium (W3C)
www.w3.org

7. Scalabilità orizzontale e verticale (flash)
https://www.ibm.com/blogs/cloud-computing/2014/04/09/explain-vertical-horizontal-scaling-cloud/

8. Oracle High Availability suite
https://www.oracle.com/database/technologies/high-availability.html

9. IBM Data Mirroring, PowerHA
- https://www.ibm.com/support/knowledgecenter/en/SSEPEK_10.0.0/trbshoot/src/tpc/db2z_recoverdisasterdatamirroring.html
- https://www.ibm.com/support/knowledgecenter/ST5GLJ_8.2.3/com.ibm.storage.ssic.help.doc/f2c_pprcover_1mrmsp.html
- https://www.ibm.com/support/knowledgecenter/SSPHQG_7.2/concept/ha_concepts_hacmp.html

UNIVERSITÀ degli STUDI di CATANIA

corso laurea informatica catania CLIC

LINK NOTEVOLI

11. Architecting Modern Data Platforms by Jan Kunigk; Lars George; Paul Wilkinson; Ian Buss – Cap 12 – High Availability

12. Application Delivery and Load Balancing in Microsoft Azure- By Derek DeJonghe and Arlan Nugara

13. Khattar, Ravi Kumar, et al. *Introduction to Storage Area Network, SAN*. IBM Corporation, International Technical Support Organization, 1999.

ISACA - Information Systems Audit and Control Association.
14. https://www.isaca.org/credentialing/cisa

LINK NOTEVOLI

TBF
nda.linearcollider.org/event/7132/contributions/35511/subcontributions/1178/atta
nts/2937/43483/MTBF_and_availability_primer.pdf

lean Time Between Failure: Explanation and Standards
e page teaching)

eter M. Chen, Edward K. Lee, Garth A. Gibson, Randy H. Katz, and David A. Patterson.
. **RAID: high-performance, reliable secondary storage**. ACM Comput. Surv. 26, 2 (June
), 145–185.
doi.org/10.1145/176979.176981

Dell EMC SRDF (backup per disaster recovery, alta disponibilita e migrazione dati)
://www.delltechnologies.com/asset/en-ca/products/storage/technical-
rt/docu95482.pdf