Elementi del progetto

Premessa

Il CLOUD degli Enti Locali rende disponibile quanto necessario per migrare le infrastrutture informatiche oggi attive nei CED dei singoli Enti:

- Server in forma di *Virtual Machine*;
- Spazio Disco;
- Connettività di Accesso;
- Controllo Remoto;
- Servizio di Backup;
- Infrastruttura e Servizio di *Disater Recovery*.

Gli elementi sopra descritti inducono evidenti benefici al servizio nel suo insieme:

- garanzia di un servizio presidiato;
- affidabilità dell'infrastruttra virtuale;
- sicurezza dei dati;
- rispetto delle norme su Sicurezza e Privacy.

Virtual Machine e Spazio Disco

L'infrastruttura descritta al precedente paragrafo garantirà la realizzazione di Server, in forma di *Virtual Machine*, che verranno messi a disposizione degli Enti che ne faranno richiesta. Le *Virtual Machine* potranno essere selezionate scegliendo tra due diverse possibili configurazioni, in base alle risorse che si ritiene necessarie a supportare adeguatamente il servizio ospite:

- VM-tipo-1 : 1CPU, 4GB RAM e 250 GB HD,
- VM-tipo-2 : 2CPU, 8GB RAM e 500GB HD.

Le *Virtual Machine* potranno essere predisposte in due modalità:

- con preinstallato il sistema operativo Linux, messo a disposizione come parte integrante del servizio;
- con operazione di "import" di VM, a partire da un'immagine predisposta dall'utente.

Da evidenziare che **le *Virtual Machine* vengono fornite "vuote"**: **la responsabilità di tutto il software installato nelle succitate VM rimane in carico all'utente, sia in termini di amministrazione dei prodotti sia in termini di utilizzo della corretta modalità di "licensing" e della relativa copertura economica necessaria all'acquisto e alla manutenzione.**

Ogni *Virtual Machine* beneficerà nativamente delle funzionalità garantite dalla piattaforma utilizzata:

- configurazione dei server in modalità cluster, con attivate funzionalità *High Availability*,
- funzionalità snapshot attivata su storage, finalizzata alla garanzia del ripristino della VM,
- monitoraggio dell'infrastruttura con gestione degli allarmi sulle VM e segnalazione all'Ente.

Connettività e servizi di rete

Ciascun Ente o aggregazione di Ente associato al SIAL fruirà di una Virtual LAN dedicata, con indirizzamento privato. Le VLAN saranno configurate in modo da garantire le funzionalità necessarie all'amministrazione dei sistemi coerentemente con la necessaria sicurezza. Gli apparati saranno configurati in modo da consentire le operazioni di seguito riportate :

All'interno di ogni VLAN sarà consentito:

- il colloquio tra le VM appartenenti alla stessa VLAN;
- l'accesso dei dipendenti dell'Ente dalla rete locale ai servizi/applicazioni installati sulle VM appartenente alla VLAN;
- l'amministrazione remota delle VM appartenenti alla VLAN da parte del personale autorizzato dell'Ente;
- la pubblicazione su Internet e/o in Rupar di servizi e di applicazioni installati sulle VM mediante un Reverse Proxy comune.

All'interno di ogni VLAN non sarà consentito:

- il colloquio diretto tra VM di Enti diversi; l'eventuale integrazione con servizi/applicazioni resi disponibili da altri Enti o dal Data Center regionale avverrà unicamente mediante un reverse proxy.

Servizio di Backup

Viene offerto un servizio di Backup/Restore dei dati articolato su più livelli funzionali, tra loro complementari.

1° Livello – SNAPSHOT VM

Il progetto prevede l'utilizzo della funzionalità di "snapshot" che consente di "congelare" una copia dell'intera VM (sistema operativo, configurazioni, sw di base, sw applicativo, file system, …) nel momento stesso in cui viene operata la richiesta. Questa funzionalità viene utilizzata per ricostruzioni complete di server da operarsi in seguito ad eventi di corruzione disastrose.

L'operazione presenta molti aspetti positivi quali la velocità delle operazioni di ripristino, la possibilità di disporre di più snapshot, realizzate in tempi diversi, a fronte di interventi specifici (es. manutenzioni correttive ed evolutive) oppure a cicli preventivativamente concordati (es. giornaliero, bi-giornaliero, settimanale, ecc.).

Presenta anche delle possibili criticità. Innanzi tutto non viene garantita la "consistenza" dei dati per quei prodotti software, tipicamente database, che necessitano dell'esecuzione di operazioni propedeutiche alla

realizzazione di qualsiasi tipologia di backup. Inoltre l'utilizzo delle snapshot deve essere progettato con cura sulla base delle effettive necessità, al fine di impedire l'inutile utilizzo di spazio disco pregiato.

Nel contesto del progetto si ipotizza l'attuazione della "snapshot" con cadenza giornaliera e per una profondità di 3 versioni.

Con questa modalità è possibile recuperare l'intero contenuto del server fino ad un massimo di 3 giorni antecedenti la richiesta di restore.

2° e 3°Livello – BACKUP GIORNALIERO e MENSILE

Per il processo di backup ogni Ente avrà accesso esclusivo ad uno "spazio di memoria" riservato su cui depositare i dati che verranno salvati secondo le modalità di seguito dettagliate.

L'accesso allo "spazio di memoria riservato" potrà avvenire con l'ausilio di protocolli diversi, da scegliersi in base al sistema operativo utilizzato: FTP, NFS, CIFS. Qualsiasi sia la modalità prescelta, la sicurezza sarà garantita da un sistema di autenticazione che prevede l'utilizzo di username e password univoca, con la possibilità di modificare la password in qualsiasi momento tramite interfaccia web.

La struttura del repository di ogni Ente prevederà **tre directory**, i cui dati verranno trattati dal sistema di backup utilizzato presso il datacenter, secondo la logica di seguito riportata.

A. DIRECTORY "Backup_giornaliero".

Area soggetta a solo salvataggio giornaliero, con profondità di 7 giorni.

Con questa modalità è possibile recuperare i dati salvati fino ad un massimo di 7 giorni antecedenti la richiesta di restore.

L'utilizzo di questa directory è consigliata per situazioni dove è necessario proteggere i dati a fronte di perdite o danneggiamento che possono verificarsi nel breve periodo.

B. DIRECTORY "Backup giornaliero e mensile".

Area soggetta a :

1. salvataggio giornaliero, con profondità di 7 giorni;
2. salvataggio mensile, con profondità di 6 entrate (possibilità di ricostruzione fino a 180 giorni precedenti); il salvo mensile verrà effettuato l'ultimo giorno lavorativo del mese, a meno di diverse richieste.

Con questa modalità è possibile recuperare i dati salvati fino ad un massimo di 7 giorni antecedenti la richiesta di restore. Inoltre è possibile recuperare i dati salvati l'ultimo giorno del mese per i sei mesi antecedenti la richiesta di restore

L'utilizzo di questa directory è indicata per aggiungere il salvataggio di un archivio "storico"

C. DIRECTORY "Restore"

Area su cui verranno depositati i dati ripristinati, come da esplicita richiesta degli utenti.

Ogni repository avrà a disposizione uno spazio adeguato alla tipologia del server utilizzato.

Insiel fornirà al referente tecnico dell'Ente lo username e la prima password per accedere al repository: la password andrà cambiata al primo accesso e da quel momento la sua gestione è in carico all'utente che potrà modificarla autonomamente via web.

Al fine di agevolare ulteriormente gli utenti, la mappatura NFS o CIFS del repository sui vari client potrà essere automatizzata tramite batch script per MS Windows e shell script per Linux, forniti da Insiel.

Le due tipologie di Backup, tipo_1 e tipo_2, sono tra loro alternative.

Infrastruttura e servizio di Disaster Recovery

Su esplicita richiesta dell'Ente, per ciascuna *Virtual Machine* installata presso il sito primario, sarà possibile attivarne la replica sul sito di DR. Come già anticipato, l'infrastruttura e il servizio di DR, offerta da progetto in oggetto, dovrà essere accompagnata dal "Piano di Disaster Recovery", attività in carico ad ogni singolo Ente.

La sincronizzazione dei contenuti avverrà utilizzando funzionalità di copia fisica asincrona dei dati (*SnapMirror*) dalla sede principale a quella di DR. L'utilizzo di software specifico garantirà l'automazione dell'orchestrazione delle attività connesse al *Disaster Recovery*, tra cui la gestione del *failover* e *failback*.

Il servizio di DR sarà implementato sulla base dei seguenti valori :

- RPO (*Recovery Point Objective*) = 1giorno (allineamento realizzato tra le ore 20.00 e le ore 24.00 del giorno precedente il "disastro");
- RTO (*Recovery Time Objective*) = 2 giorni (ripristino del servizio entro i 2 giorni successivi al "disastro").

Orario di Servizio

Il servizio in oggetto sarà erogato sulla base delle modalità di seguito elencate, a meno di specifiche richieste, che ne modifichino i livelli di servizio richiesti.

Le VM, a meno di diverse indicazioni, rimarranno accese in modalità 7x24x365, cioè tutti i giorni dell'anno, comprese le giornate festive e prefestive, ma il supporto tecnico/sistemistico e di *service desk* sarà disponibile solamente negli orari riportati nella seguente tabella:

	Giorni lavorativi	Sabato non festivo	Festivo
Service desk	07:00 – 19:00	07:00 – 14:00	No service
Supporto tecnico/sistemistico	08:00 – 18:00	No service	No service

.

Insiel, inoltre, si riserva di operare attività programmata di manutenzione ordinaria e/o straordinaria, nella fasce orarie escluse dalla precedente tabella.

Gli interventi saranno preventivamente comunicati al SIEG.

Il livello di servizio, regolato dagli orari precedentemente citati, deve assicurare una disponibilità pari al 99% su base annua.

Architettura funzionale

La descrizione di dettaglio di ogni singolo elemento del progetto, consente ora una visione d'insieme dell'architettura funzionale.