Città metropolitana di Venezia
Area amministrazione digitale

Procedure di Backup e Recupero dei dati

Sommario

1 Introduzione

Nel presente documento vengono descritte le procedure di backup che l'ente ha messo in atto per preservare i sistemi dal rischio di perdita di dati e per adempiere a quanto previsto dal GDPR Reg. UE 679/2016 in relazione alla protezione dei dati personali.
Nonostante il regolamento europeo sulla Privacy non faccia riferimento direttamente alle procedure di "Back-up" dei dati personali, esso fa parte delle misure universalmente riconosciute tra le misure di sicurezza adottate dalle aziende e dagli enti. Più specificatamente, però, le procedure di backup rientrano tra le previsioni del Capo IV Sez 2 descriventi gli Obblighi del Titolare per la Sicurezza del Trattamento, ove all'art 32 si prevede al comma 1, che il "*Titolare del trattamento" e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

a) *[….]*
b) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
c) *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
d) *[….]*

Infine, al comma 2, "*nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*".

2 Descrizione dell'infrastruttura di Città metropolitana di Venezia

Città metropolitana di Venezia (CMVE) è dotata di un Data Center realizzato su un'infrastruttura di virtualizzazione basata su tecnologia VmWare. La quasi totalità dei servizi all'utenza è erogata con server virtuali: tutti i sistemi sono dislocati nel Data Center centrale sito in Marghera Venezia – Parco Tecnologico Vega Pleiadi ubicato al di fuori delle sedi dell'ente, mentre alcuni servizi infrastrutturali essenziali rimangono comunque ancorati alle sedi degli uffici principali. Nella tabella sottostante viene riportata la consistenza dei sistemi nelle sedi dell'ente:

Site	Indirizzo	Nr. Server Virtuali
Data Center VEGA	Parco Tecnologico Vega – Venis Marghera	150
Centro Servizi	Via Forte Marghera 191 Mestre	13
Palazzo Cà corner	San Marco 2662 Venezia	7
POLIZIA Ex Abital	Via Catene 95, Marghera	4

Tabella 1:Consistenza dei sistemi

Tutti i server di CMVE vengono sottoposti a procedure automatiche di salvataggio dati.
Le postazioni di Lavoro degli utenti non sono invece sottoposte a procedure di backup: gli utenti sono tenuti a depositare tutti i loro dati negli spazi di rete adeguatamente protetti da specifiche "policy" e "access list", necessari ad evitare accessi non autorizzati.
Il servizio informatica dell'ente si fa carico dei processi di salvataggio ed è a disposizione dell'utenza per supportarli nelle eventuali necessità di ripristino dei dati.

3 Il software di backup

La soluzione software utilizzata da CMVE per il salvataggio dei sistemi virtuali VmWare è Veeam Backup. Il sistema consente di eseguire backup incrementali e completi ad intervalli di tempo regolari pianificati dall'amministratore di sistema. L'interfaccia del sistema consente la gestione dei processi di backup pilotando centralmente l'esecuzione delle procedure anche dei servizi presenti in siti differenti: le procedure prevedono la predisposizione di job di salvataggio relativi a singoli o gruppi di server. A consuntivo è possibile produrre report sullo stato delle attività eseguite.
Il software viene "manutenuto" in efficienza grazie ad un contratto di assistenza che è rinnovato con cadenza annuale e garantisce la disponibilità degli aggiornamenti software e delle ultime release stabili dell'applicazione rese disponibili dal produttore.
In sintesi, l'architettura del sistema prevede un server virtuale centrale per la gestione/schedulazione dei processi di salvataggio e dei "proxy server" necessari ad accelerare i processi di backup soprattutto nei siti remoti: i dati vengono depositati su storage di backup dedicati.

4 Storage di backup

Al fine di garantire la separazione tra ambiente di backup e ambiente di produzione, i salvataggi vengono riversati su storage dedicati. Gli storage di backup sono di tipo Synology e sono configurati con batterie di dischi in configurazione RAID 6. Gli storage vengono mantenuti costantemente aggiornati implementando le ultime release stabili dei firmware disponibili. I sistemi sono coperti da un contratto di manutenzione che prevede la sostituzione delle componenti danneggiate entro 24 h dalla segnalazione. L'integrità dei sistemi viene tenuta costantemente sotto controllo grazie ad un servizio di monitoraggio che prevede l'invio di report sullo stato degli archivi RAID;
L'accesso agli storage di backup è autorizzato solamente agli amministratori di rete e ai servizi che implementano le procedure di salvataggio.
Nella tabella che segue viene data visibilità della consistenza dei sistemi di backup:

Site	Occupazione Storage di produzione	Storage di Backup
Data Center VEGA	Nr.1 50 Tbyte	Nr. 5 100 Tbyte
Centro Servizi	Nr.1 20 Tbyte	Nr. 1 50 Tbyte
Palazzo Cà corner	Nr.1 5 Tbyte	--
POLIZIA Ex Abital	Nr.1 12 Tbyte	Nr. 1 3 Tbyte

Tabella 2:Consistenza dei Repository di Backup

5 Architettura dei sistemi di backup

CMVE ha individuato il software Veeam quale soluzione per la gestione delle procedure di salvataggio dei sistemi; L'applicazione consente la pianificazione delle attività di backup dei dati consentendo di programmare le finestre temporali di esecuzione dei singoli job di salvataggio (processi di backup) .

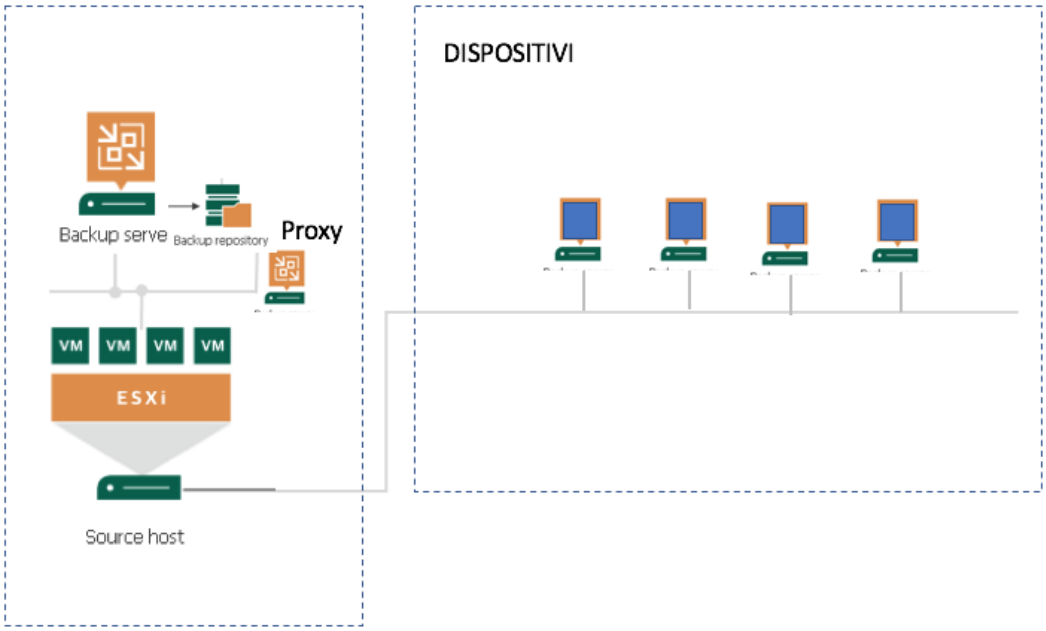

Figura 1: Architettura del sistema

Ogni Job di salvataggio consente di specificare gli elementi che lo caratterizzano ed in particolare è possibile configurare:

- I server sottoposti a backup
- L'ora di esecuzione e la finestra temporale di esecuzione del job
- La Retention dei dati (prima della sovrascrittura)
- Il Repository di destinazione: storage di Backup
- Il tipo di backup: Full o incrementale.

Per ogni sede remota è possibile implementare un server Proxy che consente di accelerare le procedure di salvataggio e comprimere i tempi di esecuzione dei Job

6 Procedure di backup

La politica di backup adottata per i sistemi di CMVE prevede per tutte le Virtual Machine (VM) in produzione un salvataggio settimanale di tipo completo (Full) ed un salvataggio quotidiano di tipo incrementale.

Nel sistema sono stati definiti più processi di salvataggio (job) ogni uno dei quali dedicato ad un insieme di Virtual Machine (VM) definito in funzione del ruolo della dimensione e delle funzionalità operative dei sistemi; a seconda delle criticità e delle dimensioni dei server virtuali, vengono assegnate priorità differenti ai job pianificati nel corso della notte; a seconda del tipo di salvataggio (full o incrementale) i processi, possono impiegare da pochi minuti (backup incrementali di Server con poche variazioni) ad oltre 24h (processi di salvataggio server di dati con backup di tipo full).
Tutti i salvataggi vengono effettuati su supporti disco dedicati (Reposotory di Backup) ed "esterni" (rete separata) rispetto al sistema di virtualizzazione e agli storage di produzione. Oltre alle procedure di salvataggio quotidiano, sono previsti backup mensili di tipo full (completo) su cassetta: i nastri, una volta scritti, vengono posizionati in altra sede rispetto a quella dove sono effettuati i backup disco.

Per garantire maggior consistenza alle procedure di backup e ridurre il rischio di perdita di dati, per i DB Server e per sistemi di dimensioni elevate sono previste ulteriori procedure di salvataggio ed in particolare:

- Sistema DB documentale: oltre al backup di Veeam, viene effettuato un export quotidiano del database in un area non sottoposta a backup: tale area viene salvata su storage esterno alla VM e conservata per 30 gg.
- Motori DB in generale: su tutti i DB server sono pianificati i dump (export) quotidiani di tutti i Database in una specifica area del server non interessata dai DB files. Quotidianamente il job di backup Veeam effettua il salvataggio di tutto il sistema compresa l'area di repository dei Db dump.
- Repository Dati territoriali: il sistema di repository delle ortofoto realizzate con volo aereo del 2015 assieme al DB della macchina fisica che lo ospita viene salvato su apposita area dedicata in storage esterno. Il backup gestito esternamente a Veeam, è pianificato con cadenza giornaliera.

7 Salvataggi su nastro

I salvataggi dati mensili su nastro prevedono l'utilizzo di librerie nastro automatiche in grado di ospitare un elevato numero di cassette. Il sistema Veeam pilota le librerie selezionando i nastri nei quali depositare i backup. La tecnologia utilizzata nelle librerie è di tipo LTO-x.
Nel sistema, le procedure di salvataggio su nastro vengono avviate manualmente da un tecnico di CMVE che le effettua con frequenza mensile; una volta terminati i processi, l'addetto si occupa di rimuovere le cassette dalle librerie e di archiviarle in siti differenti rispetto a quelli nei quali si trovano gli storage di Backup. Per ogni specifico job di backup, viene effettuato il "vault" su nastro dell'ultimo set di backup di tipo Full (completo) eseguito correttamente.
I nastri vengono conservati per 12 mesi.

8 Verifica dei job di backup

Un tecnico si occupa di verificare quotidianamente che le procedure di backup vengano eseguite senza errori. Eventuali anomalie riscontrate vengono sottoposte ad analisi approfondita: qualora

sia necessario, l'operatore dopo aver individuato la causa dell'anomalia, ed averla risolta, procede al riavvio del job di backup monitorandoli sino a completa e corretta esecuzione.
Settimanalmente viene prodotta una relazione di sintesi che riporta lo stato complessivo dell'esecuzione dei processi di backup evidenziando particolari criticità o errori: il report sottoposto al responsabile tecnico dell'ente, viene indagato e qualora necessario sottoposto al tecnico amministratore di sistema per approfondire le eventuali cause.

9 Protezione dei dati condivisi in rete

I dati degli uffici vengono memorizzati su server virtuali dedicati e che hanno il ruolo di FileServer. Sulle aree condivise è stato attivata la funzionalità di Snapshot prevista dal Sistema operativo, che consente di "fotografare" l'immagine del disco in un preciso momento della giornata (2 volte al giorno) e ne registra le variazioni; questa funzionalità è attivata per tutti i dischi presenti nei file server che condividono i dati agli utenti: in tal modo è possibile consentire all'utente finale di recuperare files o versioni precedenti degli stessi, per un periodo di tempo dipendente dallo spazio riservato alla procedura ed indicativamente sino a 2 mesi indietro nel tempo.

10 Procedure e tempi di ripristino

Per ripristino dei dati, si intende il recupero del server o di specifici files contenuti all'interno dello stesso ad uno specifico momento temporale del passato sino ad un numero massimo di 30 gg nel passato.
Il software Veeam consente il recupero completo delle VM allo stato registrato al momento del backup, oppure consente di effettuare il ripristino "granulare" del singolo file o del singolo dato. Analogamente l'applicazione consente il recupero dei database applicativi o di posta, delle singole caselle di posta elettronica sino alle singole email.
Recovery Time Objective (RTO): è il tempo massimo che può trascorrere tra il fermo di un sistema e il recupero della sua operatività. I tempi di ripristino dei dati dipendono dalla dimensione del server (o dei files da recuperare) ed in linea di massima richiedono un'ora ogni 50 Gbyte.
Tentativi di recupero di dati relativi a periodi temporali precedenti il mese potranno essere effettuati sui set di backup ricercandoli sui supporto cassetta effettuati in precisi momenti temporali, e richiederanno un tempo di Ripristino che potrà richiedere dai 4 ai 5 gg.
Recovery Point Objective (RPO): stabilisce la quantità massima di dati a cui la CMVE è disposta a rinunciare a seguito di un problema. Anche se si riferisce a una quantità di dati, si misura sempre in unità di tempo. Infatti, l'ammontare dei dati persi dipende da quanti se ne producono per unità di tempo. Considerato che i backup sono programmati quotidianamente ogni 24h ed iniziano indicativamente di notte, il dato perso, può essere recuperato riferito alla notte precedente e pertanto il ripristino avverrà con i dati al giorno precedente. Sarà possibile ripristinare i dati sino ad un massimo di 30 gg nel passato.

11 BaaS & DraaS

Il servizio di Baas (Backup As a Service) prevede il vaulting dei set di backup in un "contenitore" ubicato in un sito remoto lontano rispetto alla sede nella quale si trovano i dati e i sistemi in produzione.
Il servizio DraaS (Disaster Recovery as a Service) prevede l'attivazione di procedure di Disaster recovery che consentono l'avvio dei sistemi critici in un sito remoto e garantiscono la continuità operativa dei servizi ritenuti essenziali per l'ente.

Le procedure BaaS e Draas, saranno implementate utilizzando il site remoto di Rozzano messo a disposizione da TIM con il contratto quadro SPC Cloud: allo stato attuale le due funzionalità sono in fase di studio e ne è prevista l'attivazione e la realizzazione all'interno del contratto di conduzione del Data Center di CMVE in carico alla società Venis S.p.A.; entro fine 2021 tali funzionalità saranno attivate per entrare in produzione nel corso del 2022.

12 Disaster Recovery

Il piano di disaster recovery di CMVE verrà definito e consolidato nei contenuti e nelle modalità operative non appena verranno messe a regime le procedure Baas e Draas avviate da Venis S.p.A. e che, come specificato al paragrafo precedente, diverranno completamente attive entro l'anno 2022.