



Comune di Casatenovo

Piano di continuità operativa e disaster recovery

Versione 2.0 del 28 agosto 2023



Sede Operativa - Via Per Cabiato 122, 22066 Mariano Comense (CO)
Tel. +39 031 74.49.59 - +39 0362 31.42.26 Fax +39 031 40.36.944
info@consutek.it - www.consutek.it

Mariano Comense, 28/08/2023

Con la presente il sottoscritto Bologna Daniele, responsabile tecnico della Società scrivente, con sede legale in Via Fiamma 27, Milano e sede operativa in Via Per Cabiato 122 Mariano Comense,

DICHIARA

che presso il Comune di Casatenovo, è in uso un sistema di Disaster Recovery.

Questo sistema, basato sul software Vsphere Replication di Vmware, esegue le immagini complete delle VM (Virtual Machine) del server centrale ogni 15 minuti in modo incrementale e tali immagini vengono salvate nel datastore di un server replica del server principale.

Inoltre c'è un ulteriore software, Active Image Protector, che esegue una copia completa dei dati del server giornalmente alle ore 19:00, copiandole in un'unità NAS locale che, a sua volta, giornalmente alle ore 22:00, esegue una copia verso una macchina Linux locale per la remotizzazione dei backup. Infatti quest'ultima macchina, in schedulazione notturna, invia in replica i backup ad un sistema di server remotizzati sui quali vengono archiviati i dati, in due location distinte.

Per le specifiche tecniche di funzionamento dei sistemi di Disaster Recovery e Backup si rimanda ai manuali di procedura interna.

Consutek Srl

Dott. Ing. Daniele Bologna



ConsuTek S.r.l.



Sistema di disaster recovery

Il sistema informativo centrale del comune di Casatenovo è basato su due server vmWare, entrambi sincronizzati con il server replica attraverso il software Vsphere Replication di VMware.

Il primo server è dotato di dischi in Raid ed è rigorosamente collegato sotto unità UPS, sul quale alloggiato le seguenti macchine virtuali (VM):

- Controller di dominio di rete su sistema operativo Windows SRV 2019 Standard;
- Server Ufficio Sociale su sistema operativo Windows SRV 2008 R2;
- Server OpenVPN su sistema operativo Linux FreeBSD;

Il secondo server, anch'esso dotato di dischi raid e collegato sotto UPS, sul quale alloggia la seguente VM:

- Server di posta basato su sistema operativo Linux.

Tali macchine virtuali vengono replicate da Vsphere Replication di VMware (software di disaster recovery) che esegue le immagini complete delle VM (Virtual Machine) del server centrale ogni 15 minuti in modo incrementale e tali immagini vengono salvate nel datastore di un server replica del server principale.

Inoltre c'è un ulteriore software, Active Image Protector, che esegue una copia completa dei dati del server giornalmente alle ore 19:00, copiandole in un'unità NAS locale che, a sua volta, giornalmente alle ore 22:00, esegue una copia verso una macchina Linux locale per la remotizzazione dei backup.

Tale macchina effettua una sincronizzazione, in schedulazione notturna, verso un sistema di server remoti (in due location differenti) sui quali vengono remotizzati i consolidamenti giornalieri effettuati da ActiveImage Protector. La remotizzazione avviene tramite la creazione di una VPN (Virtual Private Network), e i dati vengono trasmessi cifrati con una chiave di crittografia a 2048 bit. Il trasferimento sulle macchine remote posiziona i pacchetti dati in due aree distinte, la prima pubblica, intesa ad accesso del cliente per mezzo di user e password (accesso eseguibile sempre e



Sede Operativa - Via Per Cabiato 122, 22066 Mariano Comense (CO)
Tel. +39 031 74.49.59 - +39 0362 31.42.26 Fax +39 031 40.36.944
info@consutek.it - www.consutek.it

solo in canale cifrato con relativa chiave di crittografia), la seconda privata dove nemmeno il cliente per sicurezza può accedere, in modo tale da scongiurare eliminazioni dei pacchetti e degli storici inavvertitamente da parte del cliente.

Un ulteriore server presente in comune, viene impiegato per alloggiare altre due macchine virtuali e sono:

- Sistema di backup interno che effettua la remotizzazione verso i siti esterni;
- Sistema telefonico (Centralino VOIP);

Nel caso di questo server, non viene effettuata nessuna replica, in quanto la VM del centralino è una macchina statica, ovvero non contiene dati variabili e/o variati nel tempo.

Le configurazioni e l'immagine sono salvate e replicate ed in caso di guasto o perdita delle configurazioni si procede al ripristino.

Per quanto riguarda la macchina di Backup si creerebbe una ridondanza di dati.

In sintesi in questo momento il comune effettua sui suoi sistemi centrali (1° e 2° SERVER) un backup delle VM (Virtual Machine) ogni 15 Minuti, tale backup viene salvato nel datastore di un server replica del server principale dotato di dischi configurati in RAID.

Inoltre c'è un ulteriore software, Active Image Protector, che esegue una copia completa dei dati del server giornalmente alle ore 19:00, copiandole in un'unità NAS locale che, a sua volta, giornalmente alle ore 22:00, esegue una copia verso una macchina Linux locale per la remotizzazione dei backup.

Punti deboli:

1) UNITA LOCALI - Rischio Basso

Uno dei punti deboli è la presenza locale dei dati fino al trasferimento in schedulazione notturna. La criticità di questo nodo è data dalla presenza di hardware che potrebbe essere soggetto a guasti, oltre all'esposizione dell'hardware a possibili eventi esterni. Il rischio si evidenzia nella frazione di tempo che intercorre tra una sincronizzazione remota e la successiva. Se accadesse un evento di elevata importanza al CED e/o agli apparati locali, si potrebbe perdere il lavoro di una giornata.



Sede Operativa - Via Per Cabiato 122, 22066 Mariano Comense (CO)
Tel. +39 031 74.49.59 - +39 0362 31.42.26 Fax +39 031 40.36.944
info@consutek.it - www.consutek.it

Soluzione

I punti citati possono essere applicati singolarmente e/o insieme.

- a. Il rischio in questo caso si può mantenere basso con una politica di manutenzione periodica programmata e con la sostituzione in periodi non inferiori ai 18/24 mesi delle unità di memorizzazione (HD);
- b. Si può prevedere la sincronizzazione remota più volte nella giornata in modo da garantire lo spostamento più frequente sulle aree remote, abbassando così il rischio di assenza di dati a poche ore e non più ad una giornata.

2) UTENTI DELLA RETE - Rischio Alto

In questo caso il rischio si divide in due aspetti, uno comportamentale ed uno tecnico, comunque in relazione tra di loro.

Il primo aspetto è, purtroppo, l'abitudine delle utenze locali malgrado sia sempre buona norma, di non salvare dati solo sulle aree condivise e dedicate del server. Questo determina un'elevata assenza di dati e documenti, elaborati dagli utenti nei backup, e comunque ne determina la presenza non costante.

Soluzione

Il sistema di backup è stato implementato con il salvataggio giornaliero dei dati locali di tutti i client della rete che vengono salvati nel NAS e, in schedulazione notturna, replicati in remoto.

Il secondo aspetto è una politica comportamentale nell'uso degli strumenti informatici.

Soluzione

Introdurre un regolamento d'uso degli strumenti informatici che aiuti l'utente ad identificare e evitare quanto più possibile le situazioni a rischio. Educare l'utente ad utilizzare le aree disco dei server.