GARA EUROPEA

PER LA FORNITURA DI SISTEMI IPERCONVERGENTI PER L'AMMODERNAMENTO DELLE CENTRALI OPERATIVE PER IL SISTEMA INFORMATIVO REGIONALE DELLE EMERGENZE E DELLE URGENZE (EX 118), E SERVIZI CORRELATI

(n. 04/17)

APPENDICE

"DESCRIZIONE DELLO STATO DELL'ARTE"

AL CAPITOLATO REQUISITI TECNICI

Settembre 2017

A. Premessa

Il presente documento contiene una descrizione dello stato dell'arte relativamente all'infrastruttura applicativa ad oggi in uso presso le Centrali Operative del 118.

B. Principali tipologie di server virtuali

Le suite applicative SaveOnLine (PSAP 2° livello) e uNiqUE (CAD 1° livello) condividono oltre all'infrastruttura hardware anche alcune componenti software.

Quanto descritto, dove non specificato, è valido per entrambe le suite.

N.B: Le macchine virtuali di tutte le Centrali Operative del sistema 112/118 sono in fase di migrazione\sostituzione, alcune versioni dei Sistemi Operativi e di MSSQL potrebbero quindi non essere presenti.

Application Server:

- Microsoft Windows 2008 R2 Standard – Suite SaveOnLine
- Microsoft Windows 2012 R2 Standard - Suite uNiqUE

DBMS:

- Microsoft SQL Server 2008 (Standard e Enterprise)
- Microsoft SQL Server 2016 (Standard e Enterprise)

Web Server:

- Microsoft Windows 2008 R2 Standard - Suite SaveOnLine
- Microsoft Windows 2012 R2 Standard - Suite SaveOnLine

Domain Controller:

- Microsoft Windows 2003 Standard
- Microsoft Windows 2008 R2 Standard
- Microsoft Windows 2012 R2 Standard

Proxy Server:

- Linux Debian

C. Relazioni tra Virtual Machine

Elenco relazione tra le VM sia nell'ambito della CO che Cross CO.

C.1. APPLICATION SERVER

Tutti gli Application Server delle CO comunicano tra loro e con i Web Server utilizzando i protocolli:

- http
- https
- ESB
- MSMQ

Comunicano con i DataBase Server utilizzando il protocollo:

- MSSQL

Requisiti di rete ottimali:

- Piena visibilità protocollo IPv4 da e verso le altre VM
- Connessione 100 Mbit o superiore

C.2. DATABASE SERVER

I database server comunicano tra loro utilizzando i seguenti protocolli:

- • http
- • https
- • MSSQL

Sistemi di replica dei dati SQLServer:

I database delle suite sono sottoposti a backup di tipo transazionale ogni 15 minuti. Il full backup viene effettuato una volta al giorno. Ogni centrale periferica (Cuneo, Alessandria e Novara) implementa la replica dei dati verso la CO di Torino, mentre

per il DataBase di Torino è implementato il mirroring verso la CO di Cuneo. L'interscambio dei dati avviene rete MPLS.

Requisiti di rete ottimali:

- • Piena visibilità protocollo IPv4 da e verso le altre VM
- • Connessione 100 Mbit o superiore

C.3. WEB SERVER

Comunicano con gli application Server utilizzando i seguenti protocolli:

- • http
- • https

Comunicano con i Database Server utilizzando il seguente protocollo:

- MSSQL

Requisiti di rete ottimali:

- Piena visibilità protocollo IPv4 verso i DC
- http\s e MSSQL verso Application Server e DataBase Server
- Connessione 100 Mbit o superiore

C.4. DOMAIN CONTROLLER

Tutte la VM inserite nel dominio Active Directory e i Domain Controller comunicano tra loro con i seguenti protocolli (Elenco estratto da Documentazione Microsoft):

Protocol and Port	AD and AD DS Usage	Type of traffic
TCP and UDP 389	Directory, Replication, User and Computer, Authentication, Group Policy, Trusts	LDAP
TCP 636	Directory, Replication, User and Computer, Authentication, Group Policy, Trusts	LDAP SSL
TCP 3268	Directory, Replication, User and Computer, Authentication, Group Policy, Trusts	LDAP GC
TCP 3269	Directory, Replication, User and Computer, Authentication, Group Policy, Trusts	LDAP GC SSL
TCP and UDP 88	User and Computer Authentication, Forest	Kerberos

	Level Trusts	
TCP and UDP 53	User and Computer Authentication, Name Resolution, Trusts	DNS
TCP and UDP 445	Replication, User and Computer Authentication, Group Policy, Trusts	SMB,CIFS,SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc
TCP 25	Replication	SMTP
TCP 135	Replication	RPC, EPM
TCP Dynamic	Replication, User and Computer Authentication, Group Policy, Trusts	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS
TCP 5722	File Replication	RPC, DFSR (SYSVOL)
UDP 123	Windows Time, Trusts	Windows Time
TCP and UDP 464	Replication, User and Computer Authentication, Trusts	Kerberos change/set password
UDP Dynamic	Group Policy	DCOM, RPC, EPM
UDP 138	DFS, Group Policy	DFSN, NetLogon, NetBIOS Datagram Service
TCP 9389	AD DS Web Services	SOAP
UDP 67 and UDP 2535	DHCP	DHCP, MADCAP
UDP 137	User and Computer Authentication,	NetLogon, NetBIOS Name Resolution
TCP 139	User and Computer Authentication, Replication	DFSN, NetBIOS Session Service, NetLogon

Requisiti di rete ottimali:

- Piena visibilità protocollo IPv4 da e verso le altre VM
- Connessione 100 Mbit o superiore

C.5. Proxy Server:

Comunica con tutte le altre VM con il protocollo:

- webproxy (3128)

Requisiti di rete ottimali:

- Piena visibilità protocollo IPv4 da e verso le altre VM
- Connessione 100 Mbit o superiore

D. Data Protection:

La data protection è demandata ai sistemi interni del motore DBMS SQL Server (profilazione accessi, backup e replica), le comunicazioni da e verso le basi dati possono essere implementate con protocollo SSL.

E. Scenari di disaster previsti

E.1. Scenario 1: Indisponibilità della Rete Telefonica.

Tale scenario implica l'impossibilità da parte di una CO (118) o CUR (112) di acquisire i flussi telefonici in ingresso.

In questo scenario, verrà attivato nella Centrale uno switch sulla rete telefonica (a cura del gestore della Fonia), che provvederà ad instradare i flussi entranti in Centrale dirottandoli dalla CO in fault, alla CO di backup (Torino è il backup per tutte le CO e Saluzzo per Torino).

Dal momento in cui le chiamate arriveranno alla CO di backup, gli operatori potranno effettuare le operazioni di gestione dell'evento.

Tale procedura non necessiterà di alcun intervento tecnico da parte del personale Regola se il fault è relativo alle CUR, mentre necessità di una riconfigurazione delle competenze nell'applicativo uNiqUE se il fault si verifica in una CO.

E.2. Scenario 2: Fault dell'infrastruttura IT

Tale scenario prevede l'indisponibilità dell'infrastruttura virtuale o fault applicativo.

La rete LAN deve essere funzionante, come la connessione MPLS.

A prescindere dal problema specifico, in questo scenario la C.O. in fault si trova impossibilitata all'uso del proprio sistema informatico.

In casi simili il piano di continuità consente di proseguire con l'attività di Centrale senza necessariamente trasferire il personale nella C.O. di backup.

Utilizzando la rete dati MPLS le PdL della C.O. in fault verranno riconfigurate per utilizzare i servizi applicativi presenti sull'infrastruttura della CO di backup I tecnici reperibili effettueranno una riconfigurazione delle PDL.

In questo caso non è necessario richiedere una modifica dell'instradamento telefonico.

Al termine della procedura, tutti i servizi (fonia e applicativi) saranno tornati disponibili al personale della C.O. in fault.

Nel caso in cui la rete MPLS non disponibile dovrà essere utilizzato lo scenario 1 con il trasferimento degli operatori nella CO di backup a discrezione dei responsabili della CO e\o CUR.

E.3. Scenario 3: Fault completo di C.O.

Tale scenario prevede la totale indisponibilità delle infrastrutture della C.O., sia essa causata da disastri naturali, black-out o altri eventi imprevisti dovrà essere utilizzato lo scenario 1 con il trasferimento degli operatori nella CO di backup a discrezione dei responsabili della CO e\o CUR.

E.4. Principali operazioni per il ripristino dei servizi

- Fault Applicativo: Vedi scenario 3
- Fault di un nodo del Cluster: Il cluster sopporta la perdita di un nodo, verranno avviate le normali procedure per un guasto HW
- Fault di nodo standalone: Vedi scenario 3
- Fault di un'intera centrale operativa: Vedi scenario 3

F. Backup Virtual Machine

Non sono disponibili soluzioni di backup automatiche. Viene effettuato, quando ritenuto necessario, l'export della\delle VM interessate.

G. Backup dei dati

Ad oggi la ridondanza fisica dei dati è garantita da un servizio di remote backup fornito da CSI Piemonte attraverso una soluzione basata su Networker 8.2.4 e un repository basato su soluzione Datadomain di backup su file centralizzato in CSI.

In particolare vengono copiati i dati di 6 virtual machine dislocate presso la sede di Grugliasco, sulle quali vengono depositate le copie dei dati provenienti dalle altre centrali ed esportate in CSI secondo la seguente pianificazione:

- 1 giornaliero incrementale, (lun-ven) retention per 21 gg
- 1 settimanale (il sabato) retention 3 mesi.
- 1 full (il primo sabato del mese) retention 1 anno.

H. Altri sistemi di backup

In CSI Piemonte inoltre è in uso una differente soluzione di backup basata su Veam 9.5, ad oggi utilizzata in contesti diversi da quello 112/118.

Tale prodotto potrebbe essere adottato in uno scenario futuro quale strumento privilegiato per garantire la ridondanza fisica dei dati e definire nuove modalità operative.