

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

INDICE

1. SCOPO, CAMPO DI APPLICAZIONE E RIFERIMENTI.....	2
1.1. SCOPO E CAMPO DI APPLICAZIONE	2
1.2. RIFERIMENTI.....	2
2. MODALITA' OPERATIVE – AMBITO HOSTING DEDICATO	3
2.1 SERVIZI E PROCESSI APPLICATIVI	3
2.2 COMPONENTE SQL SERVER.....	3
2.3 COMPONENTE POSTGRESQL.....	5
2.4 COMPONENTE MONGODB	5
2.5 COMPONENTE TOMCAT.....	6
2.6 GESTIONE FILE SYSTEM.....	6
2.7 CAMBIO PASSWORD DI DOMINIO	6
2.8 GESTIONE VMWARE	6
2.9 GESTIONE SISTEMA OPERATIVO	7
2.10 COMPONENTE REDHAT OPENSIFT	7
2.11 COMPONENTE DOCKER SWARM.....	7
3 MODALITA' OPERATIVE – AMBITO HOSTING CONDIVISO	8
3.1 SQL SERVER.....	8
3.2 POSTGRESQL	9
3.3 REDHAT OPENSIFT	9

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

1. SCOPO, CAMPO DI APPLICAZIONE E RIFERIMENTI

1.1. Scopo e campo di applicazione

Scopo della presente istruzione di lavoro è quello di fornire le modalità operative per la gestione delle richieste di delega di elementi di sistema operativo e di servizi.

La presente istruzione è applicabile all'area Datacenter ed in particolare alla figura dei referenti tecnici sistemisti di realtà Clienti e/o Concessionari e/o Partner che operano nel contesto tecnologico come incaricati dal Cliente finale.

Si specifica che ogni richiesta sarà tracciata a livello TK assistenza e subirà una valutazione di analisi/fattibilità sistemistica.

1.2. Riferimenti

I riferimenti per la procedura sono:

- Norma ISO 9001;
- Norma ISO 27001;
- Manuale di Gestione Qualità e relativi Allegati.

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

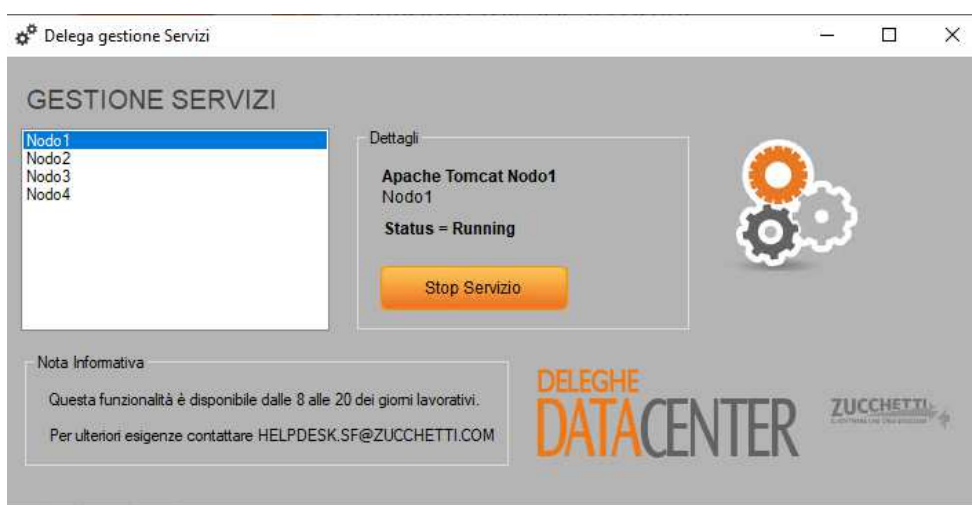
2. MODALITA' OPERATIVE – AMBITO HOSTING DEDICATO

Zucchetti spa ha adottato dei modelli di delega in ambito HOSTING DEDICATO:

2.1 Servizi e Processi Applicativi

E' prevista la delega in ambito **Windows**:

- ✓ Delega Riavvio Servizi con la disabilitazione del monitoraggio fino al giorno lavorativo successivo tramite tool di delega



- ✓ Delega Visualizzazione Processi (simil task manager) tramite tool di delega

E' prevista la delega in ambito **Linux**:

- ✓ Delega Riavvio Servizi con la disabilitazione del monitoraggio fino al giorno lavorativo successivo attraverso script specifici ad esempio: ManageTomcat.sh
- ✓ Delega Visualizzazione Processi tramite comando TOP.

E' possibile valutare la delega totale del servizio con l'implicazione che la struttura di Datacenter non faccia attività di monitoring del servizio e patching del servizio. Eventuali vulnerabilità di sicurezza segnalate dal Datacenter dovranno essere mitigate entro 15gg vulnerabilità alte, 25gg vulnerabilità medie.

2.2 Componente SQL Server

E' possibile installare in ambito Windows l'utility SQL Mgmt Studio e gestire tramite essa tutte le operazioni autorizzate a login con privilegi massimi di DBOwner, a titolo esemplificativo:

- ✓ gestione tabelle/stored procedure

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

- ✓ esecuzione query di inserimento/cancellazione/modifica dati

E' prevista la delega in ambito Windows attraverso Tool di Delega al fine di:

- ✓ effettuare backup/restore da file .bak
- ✓ Settare limiti, opzioni DB e spazi.

- ✓ creare nuovi DB
- ✓ Set db owner
- ✓ Killare lock
- ✓ Kill SPID non di sistema
- ✓ Visualizzare dimensioni disco
- ✓ Snapshot Isolation and Row Versioning (con kill connessioni)
- ✓ Creazione Utente con naming convention standard NOMEDB-1

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

E' possibile valutare la delega totale del servizio con l'implicazione che la struttura di Datacenter non faccia attività di monitoring del servizio e patching del servizio. Eventuali vulnerabilità di sicurezza segnalate dal Datacenter dovranno essere mitigate entro 15gg vulnerabilità alte, 25gg vulnerabilità medie.

Sono previste le seguenti operazioni attraverso richiesta a Helpdesk:

- ✓ creazione/cancellazione/rinomina di Database/Login
- ✓ gestione schedulazione job tramite SQL Server Agent
- ✓ abilitazione profiler con delega privilegio Alter Trace per un periodo temporale di 48h
- ✓ delega privilegio view server state

2.3 Componente PostgreSQL

E' possibile installare in ambito Windows le utility PGAdmin / HeidiSQL / pg_dump / pl-pgsql e in ambito Linux con le utility pgdump / pl-pgsql e gestire tramite esse tutte le operazioni autorizzate a login con privilegi massimi di owner del DB, a titolo esemplificativo:

- ✓ gestione tabelle/stored procedure
- ✓ esecuzione query di inserimento/cancellazione/modifica dati
- ✓ effettuare backup/restore
- ✓ visualizzazione

E' prevista la delega per la visualizzazione dei log tramite script solo in casistiche particolari da analizzare puntualmente.

Sono previste le seguenti operazioni attraverso richiesta a Helpdesk:

- ✓ creazione/cancellazione/rinomina di Database/Login
- ✓ gestione schedulazione job
- ✓ tracciatura query tramite funzionalità Long Query

E' possibile valutare la delega totale del servizio con l'implicazione che la struttura di Datacenter non faccia attività di monitoring del servizio e patching del servizio. Eventuali vulnerabilità di sicurezza segnalate dal Datacenter dovranno essere mitigate entro 15gg vulnerabilità alte, 25gg vulnerabilità medie.

2.4 Componente MongoDB

E' possibile installare la utility mongocli e gestire tramite essa tutte le operazioni autorizzate a login con privilegi massimi di dbAdminAnyDatabase e/o readWriteAnyDatabase

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

E' possibile valutare la delega totale del servizio con l'implicazione che la struttura di Datacenter non faccia attività di monitoring del servizio e patching del servizio. Eventuali vulnerabilità di sicurezza segnalate dal Datacenter dovranno essere mitigate entro 15gg vulnerabilità alte, 25gg vulnerabilità medie.

2.5 Componente Tomcat

E' possibile effettuare le seguenti attività:

- ✓ Accesso a Tomcat Manager da IP specifici
- ✓ Delega riavvio contesti tramite Manager
- ✓ Delega riavvio servizio Tomcat completo tramite ticket
- ✓ Delega totale di Tomcat ma che implica il fatto che la struttura di Datacenter non effettui attività di monitoring del servizio, scansione VA e patching del servizio.
- ✓ Possibilità di cancellare cache di Tomcat (nei vari casi sopra indicati)
- ✓ Delega lettura directory tomcat e scrittura directory webapps

2.6 Gestione File System

Le policy sono le seguenti:

- ✓ Possibilità di abilitazione permessi Lettura/Scrittura in directory applicative
- ✓ Valutazione Creazione di condivisioni solo su richiesta
- ✓ Bonifica massiva dei permessi tramite script FixPerm.sh

2.7 Cambio Password di Dominio

Le policy sono le seguenti:

- ✓ Possibilità di cambio password (non scaduta) tramite link pubblico

2.8 Gestione VMware

In ambiente VMware dedicato, le policy sono le seguenti:

- ✓ Creare VM from scratch
- ✓ Importare VM da immagini OVA
- ✓ Accendere/Spegnere VM
- ✓ Modificare caratteristiche delle VM (CPU, RAM, Spazio disco)
- ✓ Aggiungere/Togliere schede di rete da una VM spenta
- ✓ Aggiungere dischi alle VM spente
- ✓ Aumentare la dimensione dei dischi delle VM
- ✓ Scaricare l'immagine di una VM da spenta

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

- ✓ Creare/rimuovere snapshot
- ✓ Riportare una macchina ad uno snapshot preso in precedenza
- ✓ Inserire annotazioni sulla VM
- ✓ Installare/Disinstallare VMWare Tools
- ✓ Deploy di OVF Templates

2.9 Gestione Sistema Operativo

E' possibile richiedere la delega completa del sistema operativo al massimo per 48 ore a seguito di una valutazione specifica in ambito DC.

Al termine il richiedente è tenuto a compilare un rapportino delle attività svolte che sarà poi verificato dal gruppo sistemistico per controllare se l'operato in fase di delega corrisponde a ciò che è stato dichiarato e che le condizioni base di sicurezza DC siano state mantenute.

In caso di anomalie, verrà data evidenza al richiedente tramite TK/HD e successivamente si andrà a bonificare le configurazioni della macchina valutando gli impatti eventuali sul servizio con il Delegato iniziale.

Eventuali vulnerabilità dovranno essere fixate da parte del richiedente entro massimo 5gg lavorativi dalla segnalazione.

2.10 Componente RedHat OpenShift

E' prevista la delega operativa sulle attività di:

- ✓ Creazione/modifica/eliminazione manifest Kubernetes all'interno di tutto il cluster
- ✓ Creazione/modifica/eliminazione di deployment, pod, secrets, config-map, cronjob, service, route, persistent volume, persistent volume claim, build config...
- ✓ Creazione/modifica/eliminazione di namespace
- ✓ Modifica configurazione di operator

Non è prevista la:

- ✓ Modifica alla configurazione componenti di infrastruttura (nodi, cluster configuration)

E' previsto l'accesso sia attraverso CLI che tramite Web console

2.11 Componente Docker Swarm

E' prevista la delega operativa sulle attività di:

- ✓ Creazione/modifica/eliminazione container
- ✓ Creazione/modifica/eliminazione servizi
- ✓ Creazione/modifica/eliminazione network

Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

- ✓ Creazione/modifica/eliminazione volumi
- ✓ Accesso metriche cluster swarm

Non è prevista la:

- ✓ Modifica alla configurazione componenti di infrastruttura (nodi, cluster configuration)

E' previsto l'accesso attraverso login ai server dedicati oppure da remoto con certificati TLS.

L'interazione con le funzionalità Docker avviene attraverso la Docker CLI, o in alcuni casi interfaccia WEB (Portainer).

3 MODALITA' OPERATIVE – AMBITO HOSTING CONDIVISO

Zucchetti ha adottato dei modelli di delega in ambito HOSTING CONDIVISO:

3.1 SQL Server

E' prevista la delega operativa sulle attività di:

- ✓ gestione tabelle/stored procedure
- ✓ esecuzione query di inserimento/cancellazione/modifica dati

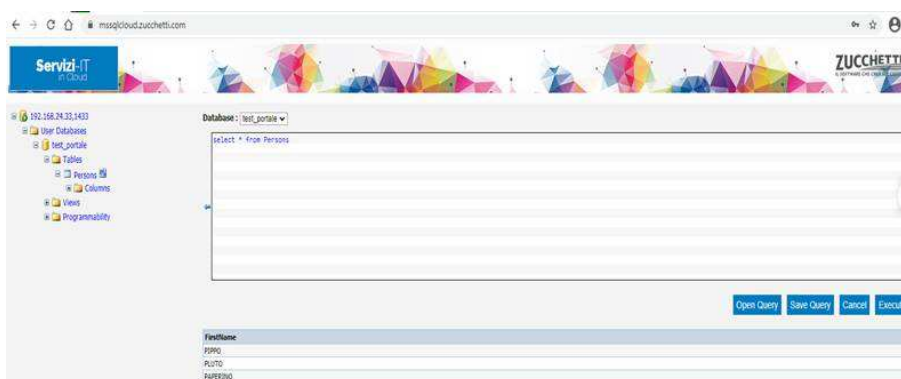
Non è prevista la:

- ✓ creazione/cancellazione/rinomina di Database/Login
- ✓ gestione schedulazione job tramite SQL Server Agent

La gestione dei backup/restore segue il modello standard di Datacenter.

L'attività è stata delegata alla struttura di Helpdesk con la possibilità di effettuare il backup del/i DB richiesti e di fornirli in modalità sicura attraverso un link web. I dettagli sono indicati nel WIKI.

E' previsto l'accesso da interfaccia grafica Web per l'esecuzione di query



Datacenter - GESTIONE DELEGA di SISTEMA e SERVIZI

3.2 PostgreSQL

E' prevista la delega operativa sulle attività di:

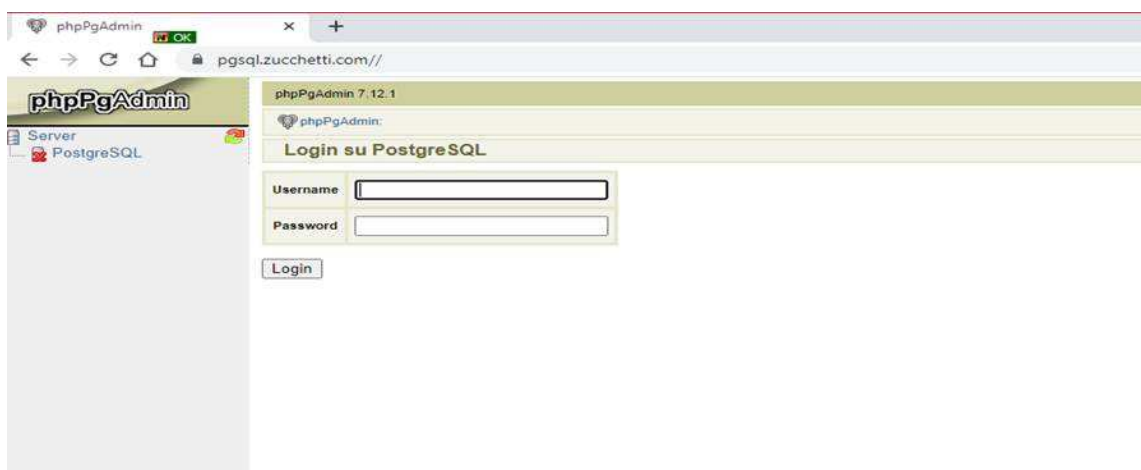
- ✓ gestione tabelle/stored procedure
- ✓ esecuzione query di inserimento/cancellazione/modifica dati

Non è prevista la:

- ✓ creazione/cancellazione/rinomina di Database/Login
- ✓ gestione schedulazione job

La gestione dei backup/restore segue il modello standard di Datacenter.

E' previsto l'accesso da interfaccia grafica Web per l'esecuzione di query



3.3 RedHat OpenShift

E' prevista la delega operativa sulle attività di:

- ✓ Creazione/modifica/eliminazione manifest Kubernetes all'interno di namespace isolato per singolo cliente
- ✓ Creazione/modifica/eliminazione di deployment, pod, secrets, config-map, cronjob, service, route, persistent volume claim, build config...

Non è prevista la:

- ✓ Creazione/modifica/eliminazione di namespace
- ✓ Modifica alla configurazione componenti di infrastruttura (nodi, cluter configuration)