Contratto Quadro SPC Cloud Lotto 1

Introduzione nuovo servizio

Managed Services

Specifiche di Realizzazione

Gestione	Azienda	Riferimento
REDATTO:	Telecom Italia S.p.A.	
APPROVATO:	Telecom Italia S.p.A. (Mandataria), DXC	
N° allegati:	0	

Telecom Italia S.p.A.
(ing. Giovanni Santocchia)

Firmato digitalmente da:
GIOVANNI SANTOCCHIA
Firmato il 06/12/2017 22:41
Seriale Certificato: 443651
Valido dal 05/12/2016 al 05/12/2019
TI Trust Technologies CA

INDICE

1. REGISTRAZIONE MODIFICHE DOCUMENTO

N° Rev.	Descrizione	Data emissione
0	Prima emissione	19/05/2017
1	Seconda emissione	06/07/2017
2	Terza emissione	20/09/2017

2. GENERALITA'

2.1. Applicabilità

Il documento si applica nell'ambito del Contratto Quadro SPC Cloud Lotto1.

2.2. Assunzioni

Non applicabile.

2.3. Riferimenti

Identificativo	Titolo/Descrizione
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5B Capitolato Tecnico
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5A Capitolato Tecnico Parte Generale
Gara Cloud Lotto 1	Offerta Tecnica del Fornitore Allegato B Relazione Tecnica Lotto 1
Agenzia per L'Italia Digitale	Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni

2.4. Definizioni ed Acronimi

Definizioni/Acronimi	Descrizione
IaaS	Infrastructure as a Service
PaaS	Platform as a Services
RTI	Raggruppamento temporaneo d'Impresa

3. Definizione Componenti

Come indicato nel documento “specifiche del servizio”, i servizi Managed saranno applicati ai seguenti servizi infrastrutturali di SPC CLoud Lotto1:

- Servizio IaaS (Virtual Machine nel seguito VM) applicabile a tutte le modalità previste nel documento “Gara Cloud Lotto 1 Allegato B Offerta tecnica del fornitore”.
  Il servizio si applica anche a tutte le VM standard all’interno dello IaaS VDC
- Servizio PaaS nelle 4 modalità “Solution Stack” previste nel documento “Gara Cloud Lotto 1 Allegato B Offerta tecnica del fornitore” e di seguito elencate:
  - Application Server;
  - Web Server;
  - DBMS;
  - Monitoring

  Il servizio si applica a tutti i solution stack standard delle VM all’interno dello IaaS VDC

L’uso di servizi Managed nel contesto VDC implica l’utilizzo di servizi managed per tutto il VDC.

Nel caso in cui saranno inseriti nuovi PaaS, sarà fornita la descrizione del servizio PaaS Managed associato.

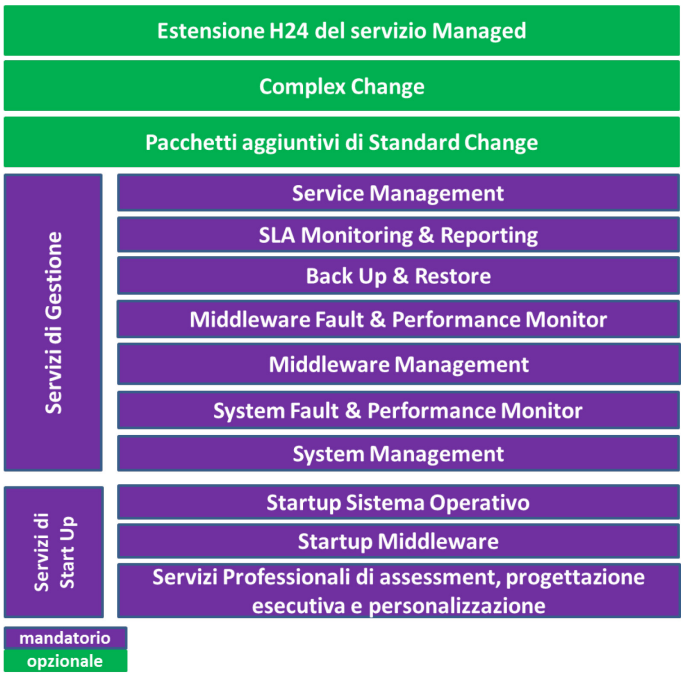
Sono previsti sette profili di gestione per andare incontro a differenti esigenze delle singole Amministrazioni:

- **Profilo IaaS Managed “Entry Level”**
- **Profilo IaaS Managed “Premium Level”**
- **Profilo PaaS Managed Web**
- **Profilo PaaS Managed Application**
- **Profilo PaaS Managed DataBase Standard**
- **Profilo PaaS Managed Database Enterprise**
- **Profilo PaaS Managed Monitor**

I servizi Managed dovranno essere contrattualizzati per tutti i tenant appartenenti al singolo contratto come dettagliato nel documento “specifiche del servizio” al par. 3.2.
I servizi Managed saranno erogati in coerenza con le indicazioni riportate nel documento “Misure Minime di sicurezza ICT per le PA” di cui alla circolare AgID n.1/2017 pubblicata in GU serie generale n.79 del 4 Aprile 2017.

3.1. Componenti del servizio

Una vista complessiva delle componenti del servizio Managed, è rappresentata dal seguente schema i cui singoli elementi sono descritti nel documento specifiche del servizio.



Schema funzionale generale dei Managed Services

3.2. Correlazione Componente Requisito

Nello schema seguente è riportata in modalità tabellare l'associazione tra le componenti base del servizio ed i profili di servizio previsti. Nella tabella seguente e nel seguito del documento con il termine middleware si fa riferimento ai quattro profili PaaS previsti dal Lotto 1: Web Server, Application Server, DB e Monitoring.

Componenti del servizio	Profilo IaaS Managed	Profilo PaaS Managed
Service Management	Incluso	incluso
SLA monitoring & Reporting	incluso	incluso
Back Up & Restore	Incluso	incluso
Middleware Fault & Performance Monitor	Non incluso	incluso
Middleware Management	Non incluso	Incluso
Start Up Middleware	Non incluso	Incluso
System Fault & Performance Monitor	incluso	Incluso
System Management	incluso	Incluso
Servizi Professionali di Assessment, Progettazione esecutiva e personalizzazioni	incluso	Incluso

4. Realizzazione del servizio

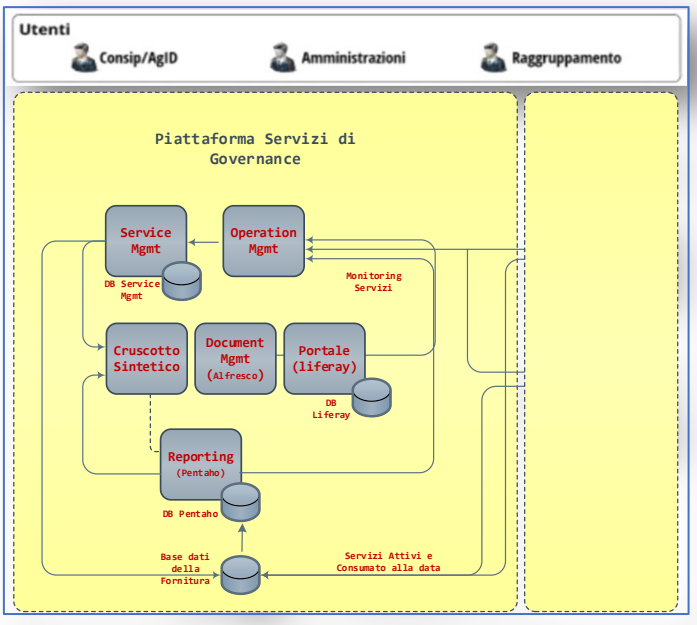
Di seguito saranno presentate tutte le componenti tecnologiche previste per la realizzazione del servizio.

4.1. Architettura Generale

L'architettura della piattaforma tecnica per l'erogazione dei servizi Managed è la stessa di quella prevista per i servizi previsti nel Capitolato Tecnico della gara SPC Cloud Lotto1 e comprende diverse componenti divise nei due macro domini:

- Piattaforma dei Servizi di Governance;
- Piattaforma dei servizi Cloud.

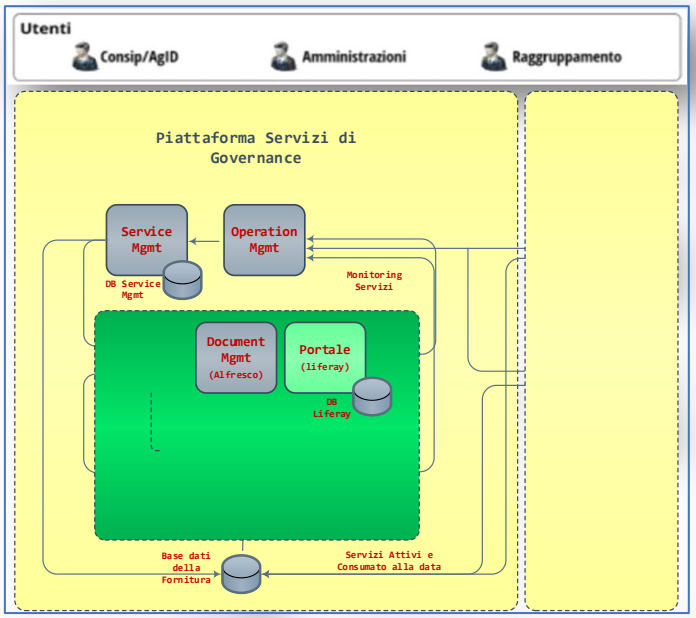
La figura seguente illustra i due domini e i principali flussi 'di servizio' tra le diverse componenti architetturali. Nei paragrafi successivi si descrivono gli interventi da realizzare sulle componenti di ciascuna delle due piattaforme per l'erogazione del servizio Managed.



Architettura di riferimento della Piattaforma

4.1.1. Portale di Governance

Il portale è realizzato tramite una personalizzazione della piattaforma Liferay Portal 6.2, nella versione community. Attraverso il Portale è possibile accedere sia ai servizi SPC Cloud Lotto 1, sia alle funzioni della Piattaforma di Governance.
Dal punto di vista infrastrutturale, l'ambiente è installato su una coppia di sistemi virtuali: un sistema ad uso di Liferay DB, l'altro per la componente Liferay Portal. Entrambi i nodi sono configurati con sistema operativo Ubuntu-14.04.3-server-amd64.



Portale di Governance

Il Portale rappresenta il punto di ingresso univoco alla Piattaforma dei Servizi e di Governo della Fornitura, per i Referenti delle Amministrazioni e di Consip/Agid.
In particolare rappresenta il punto di accesso verso i sistemi di gestione dei servizi, per i servizi di virtualizzazione sono previste due opzioni:

- **Unmanaged** (in attuale convenzione);
- **Managed**.

Dipendentemente dalla tipologia dell'opzione del servizio, sul portale saranno disponibili le seguenti funzionalità di gestione del servizio:

Per servizi con opzione **Unmanaged**, rimangono invariate le funzionalità già in convenzione, ossia:

- La console Horizon, per la gestione dei servizi di virtualizzazione;
- Ambiente di Service Management per la gestione delle richieste e l'help desk;
- Il sistema di rappresentazione della reportistica e del cruscotto sintetico (Penthao);
- Il sistema di gestione documentale per la condivisione della documentazione di servizio, della gestione e quella tecnica;

Per i servizi di virtualizzazione con opzione **Managed**:

- Ambiente di Service Management per la gestione delle richieste e l'help desk;
- Il sistema di rappresentazione della reportistica e del cruscotto sintetico (Penthao);
- Il sistema di gestione documentale per la condivisione della documentazione di servizio, della gestione e quella tecnica;

Per l'opzione Managed l'accesso alla console Horizon sarà abilitato al solo Cloud Provider che gestirà il servizio di virtualizzazione.
Allo scopo di dotare l'Amministrazione di uno strumento in sola lettura per controllare il proprio parco macchine e verificarne lo stato, sarà fornito un accesso web based ad una Console Centralizzata di Monitoraggio con una dashboard che:

- fornirà la visibilità del perimetro dell'Amministrazione, mediante un elenco degli oggetti infrastrutturali gestiti;
- per ogni oggetto infrastrutturale, sarà possibile produrre i dati di utilizzo near real-time (performance) con metriche customizzabili dall'utente stesso.

Per i servizi di virtualizzazione **Managed**, sono previsti sette profili:

Profilo IaaS Managed "Entry Level". Il Profilo si riferisce alla macchina virtuale gestita con i seguenti Sistemi Operativi:

- Windows;

Profilo IaaS Managed "Premium Level". Il Profilo si riferisce alla macchina virtuale gestita con i seguenti Sisitemi Operativi:

- Linux.

Profilo PaaS Managed Web. Il Profilo si riferisce alla macchina virtuale gestita con i seguenti tipologie di middleware:

- Web Server IIS;
- PHP
- Apache;

Profilo PaaS Managed Application. Il Profilo si riferisce alla macchina virtuale gestita con una delle seguenti tipologie di Middleware:

- Tomcat;
- Jboss
- Oracle Weblogic;

Profilo PaaS Managed DataBase Standard. Il Profilo si riferisce alla macchina virtuale gestita con una delle seguenti tipologie di Middleware:

- MySQL;
- PostGreSQL;
- SQL Server;
- Oracle Standard Edition
-

Profilo PaaS Managed DataBase Enterprise. Il Profilo si riferisce alla macchina virtuale gestita con la seguente tipologia di Middleware:

- Oracle DBMS Enterprise Edition;

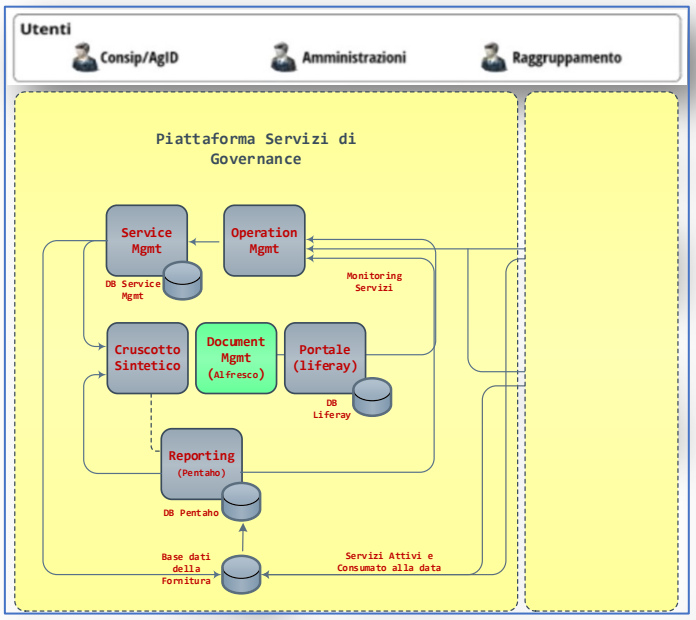
Profilo PaaS Managed Monitor. Il Profilo si riferisce alla macchina virtuale gestita con una delle seguenti tipologie di Middleware:

- Pandora FMS;
- CACTI;
- ZABBIX

4.1.2. Gestione Documentale

Il Sistema di Gestione Documentale è realizzato su piattaforma Liferay. La piattaforma è divisa in più repository documentali, con una struttura su tre livelli:

- **Repository livello informativo**, di libero accesso ai Referenti di Consip/AgID e delle Amministrazioni contraenti, che ospita documenti di interesse generale sul contesto della fornitura e sui servizi e i documenti pubblici;
- **Repository livello operativo centrale**, riservato ai soli Referenti di Consip/AgID, che contiene i documenti relativi alla gestione del Contratto Quadro;
- **Repository di livello esecutivo**, uno per ogni Amministrazione contraente, ad uso esclusivo, con i documenti relativi alla gestione dei Contratti Esecutivi.



Document management

Nel dettaglio, la configurazione dell'ambiente è la seguente:

- **Livello Informativo:** contiene documenti relativi ad Informazioni generali, relativi sia alle Amministrazioni che a Consip/Agid.
    - Il Repository contiene le seguenti cartelle:
        - Documenti sui servizi;
        - Contesto della Fornitura;
        - Catalogo di riferimento.

- **Livello Operativo Centrale:** contiene documenti relativi al Contratto Quadro, riservati a Consip/Agid.
    - Il Repository contiene le seguenti cartelle:
        - Documenti contrattuali;
        - Documenti Comitato di Gestione;
        - Reportistica 'storica'
        - Informative periodiche.

- **Livello Esecutivo:** Contiene documenti relativi alle singole Amministrazioni che hanno sottoscritto contratti. Ogni amministrazione ha il proprio repository.
    - Il Repository contiene le seguenti cartelle:
        - Contratto;
        - Verbali;
        - Comunicazioni;
        - stato di avanzamento.

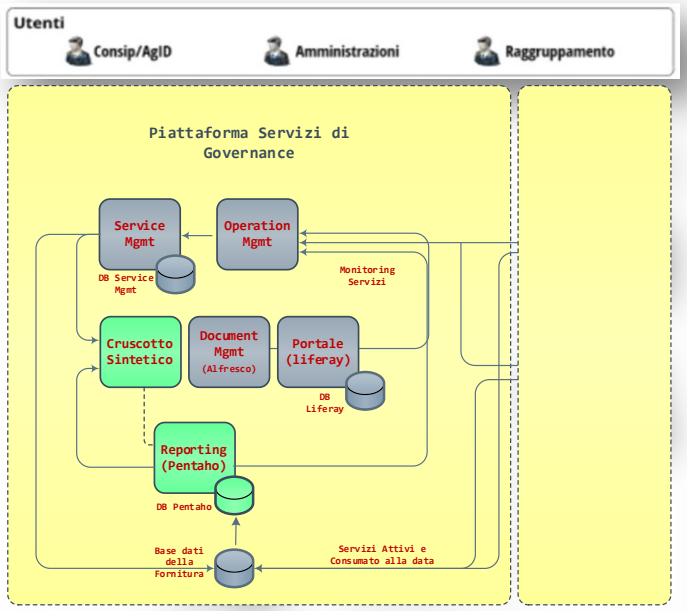
Nell'ambito del livello esecutivo saranno resi disponibili i documenti relativi alla reportistica contrattuale dei servizi Managed (SLA/KPI).

La piattaforma prevede inoltre la produzione automatica della seguente tipologia di report.

- **SLA Summary: c**ontiene un riepilogo di tutti i livelli di servizio conseguiti nel periodo di osservazione con riferimento agli SLA contrattualizzati.
- **Riepilogo Attività Svolte:** contiene in forma tabellare i dati di dettaglio di tutti i ticket lavorati e chiusi nel periodo di osservazione.

4.1.3. Cruscotto Sintetico e Reporting

Il Cruscotto Sintetico e le funzioni di Reporting sono basati sulla piattaforma di Business Intelligence e Reporting Penthao.



Cruscotto sintetico e Reporting

4.1.3.1. Cruscotto Sintetico

Il Cruscotto Sintetico riconosce due profilazioni:

- una, ad uso degli Utenti Consip/AGID. Rende disponibili informazioni 'trasversali' rispetto alle singole Amministrazioni, con una vista "per servizio";
- una seconda profilazione è ad uso delle Amministrazioni, con una vista 'verticale' sui servizi acquistati.

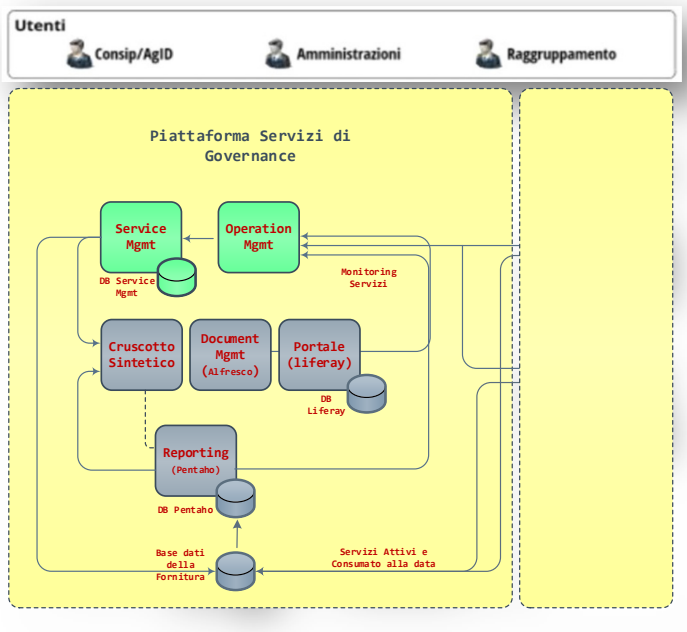
Il Cruscotto ha lo scopo di fornire una vista sintetica degli indicatori relativi a:

- Prestazioni generali dei singoli servizi acquistati;
- Consumo dei singoli servizi.

In aggiunta alle funzionalità disponibili nell'attuale convenzione SPC Cloud, anche per le richieste di Change/Gestione relative al servizio di virtualizzazione con opzione Managed contrattualizzato (vedi template specifiche del servizio e di controllo), sarà disponibile l'informazione relativa al 'consumato' (richieste di change/gestione evase) alla data rispetto al valore complessivo della Fornitura in corso, e relativi indicatori.

4.1.4. Piattaforma di System e Service Management

La piattaforma di System e Service Management ospita i servizi di Monitoraggio, Help Desk e Self Ticketing.



Service Management

I principali elementi che compongono l'infrastruttura sono:

- Help Desk e Self Ticketing;
- Monitoraggio applicativo;
- Monitoraggio componenti di rete;
- Monitoraggio nodi infrastrutturali;
- Console centralizzata di gestione degli eventi di monitoraggio.

4.1.4.1. Help Desk e Self Ticketing

L'Utente dell'Amministrazione accederà alle funzioni di Help Desk e Self Ticketing, utilizzando i canali di comunicazione già in essere nell'attuale convenzione.
Oltre a quanto previsto per i servizi unmanged (informazioni e supporto, segnalare incident o per effettuare richieste), sarà possibile anche segnalare le richieste di gestione per i servizi managed sulla base di un catalogo definito nel documento template specifiche del servizio.
Le richieste di gestione sui servizi Managed saranno registrate e gestite sul portale di Ticketing come Richieste di Change. La registrazione potrà essere fatta o attraverso la funzionalità di Self Ticketing o tramite Numero Verde dello SPOC.
Nel caso di registrazione della Change tramite Numero Verde dello SPOC, la richiesta sarà comunque visibile e gestibile nella sezione di Self Ticketing dell'Amministrazione.

Pertanto, una qualunque richiesta di modifica sul servizio di virtualizzazione Managed (richiesta di modifica infrastrutturale e/o di software di Sistema Operativo o Middleware) sarà classificata, sul sistema di Self Ticketing, come Richiesta di Change.

Il sistema di Gestione Ticketing traccerà tutti gli stati e tempi di lavorazione della Change fornendo i dati a:

- Sistemi di produzione della reportistica per il calcolo degli SLA/KPI contrattualizzati;
- Cruscotto sintetico per il monitoraggio dell'andamento degli indicatori contrattuali.

Per i dettagli sulla tipologia di Change gestibili far riferimento al documento "specifiche del servizio".

4.1.4.2. Monitoraggio e console centralizzata di gestione eventi

Per consentire un'efficace gestione operativa è necessario impostare un monitoraggio che permetta la rilevazione di alert ed in alcuni casi di intervenire per ovviare a malfunzionamenti e ridurre i rischi per le Amministrazioni.

La soluzione individuata è di tipo agent-based e prevede l'utilizzo del software Zabbix (o equivalente).

Questa modalità permette di correlare gli eventi in caso di malfunzionamenti generalizzati per poter più rapidamente isolare il problema ed arrivare alla individuazione di cause e relativa soluzione.
Il modello architetturale prevede che, su ciascun server di ciascun tenant gestito, sia attivo un Agent al quale è garantito un interfacciamento bidirezionale con un Manager.
Lo Zabbix Agent è descritto al seguente link nel quale è possibile trovare tutti i requisiti di installazione e attivazione per piattaforme supportate: https://www.zabbix.com/documentation/3.4/manual/concepts/agent.

Il Manager Zabbix funge da elemento di aggregazione e analisi del traffico di monitoring proveniente dagli agent e gestisce l'inoltro di tale traffico alle consolle di monitoraggio. Queste ultime sono presidiate dai sistemisti preposti al controllo e gestione dei tenant OpenStack.
A discrezione del Cloud Provider, il Manager potrà essere dedicato ad un tenant o condiviso da più tenant comunque inerenti la sola piattaforma OpenStack SPC. In caso di Manager Zabbix condiviso, la separazione sarà garantita:

- a livello di infrastruttura da interconnessioni separate e dedicate per ogni singolo tenant;
- a livello logico dall'applicativo Zabbix che consentirà di mantenere i dati separati.

Il rapporto tra Agent e Manager Zabbix dipenderà sempre dal numero di VM contenute nel tenant dell'Amministrazione che necessitano di monitoraggio (al crescere del numero di VM da monitorare, sarà dedicato un Server Zabbix Manager alla specifica Amministrazione).

Il Server Zabbix Manager sarà implementato all'interno di un Project OpenStack distinto da quello della specifica Amministrazione e condividerà una External Network col tenant dell'Amministrazione.

Attraverso tale External Network condivisa sarà garantito il dialogo tra Agent e Manager.

Il Project del cliente e quello di Monitoring o Management dello Zabbix Manager condivideranno la "Monitoring Network" e il dialogo tra le parti sarà sempre filtrato via security groups definiti nel project Cliente (saranno di fatto concessi solo flussi noti da VM verso Zabbix Manager dedicato e viceversa).

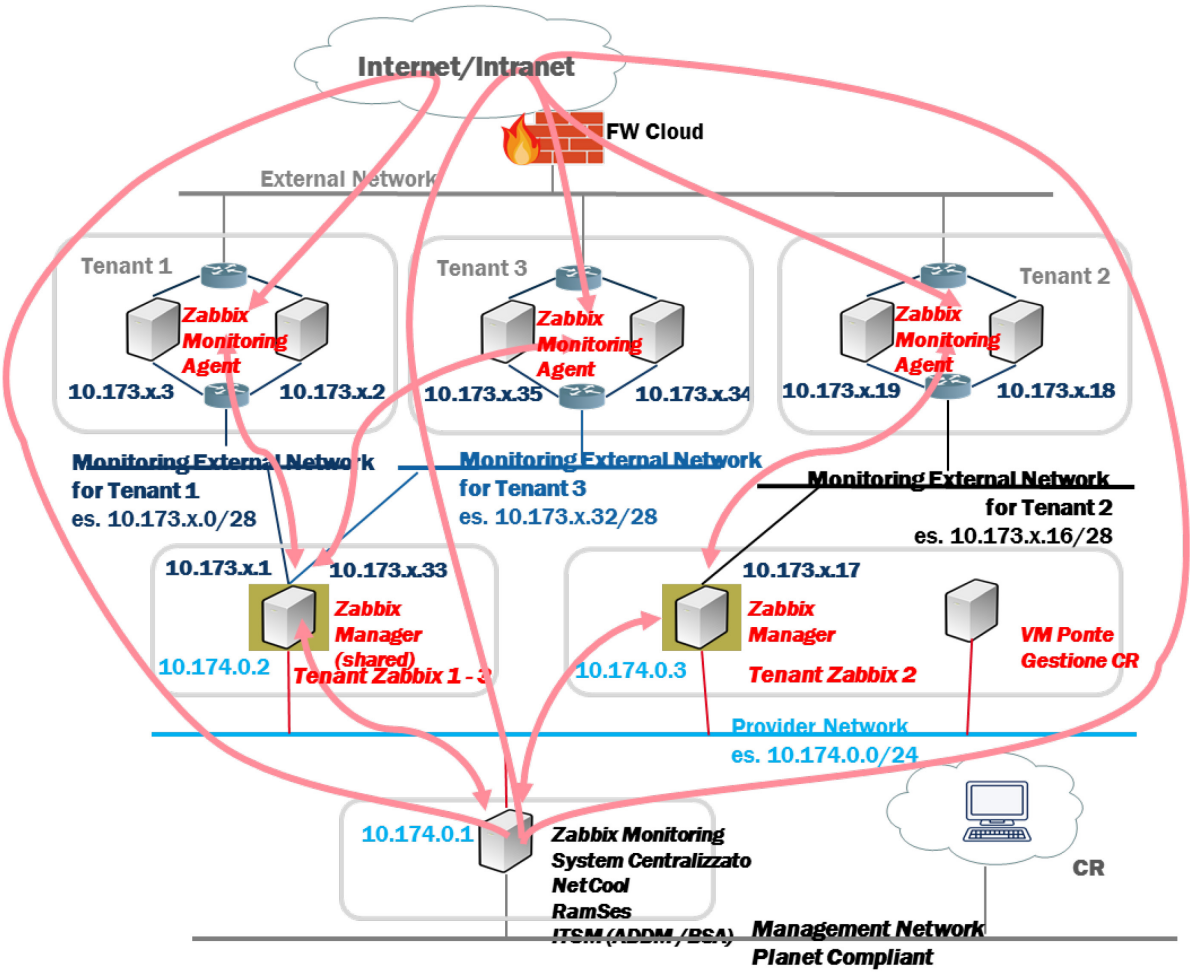
Ogni Server Zabbix Manager istanziato avrà poi una connessione ad una Provider Network grazie alla quale sarà garantito un accesso controllato agli stessi elementi costituenti la piattaforma di monitoraggio e gestione degli specifici tenant delle Amministrazioni.
In particolare sarà controllato ogni accesso ai Server Zabbix Manager tramite un sistema applicativo di controllo e registrazione delle attività svolte dagli addetti IT descritto nel seguito del documento .

Grazie a tale sistema di controllo, è possibile tracciare qualunque attività svolta dagli addetti IT sugli stessi Zabbix Manager o sulle singole VM dei tenant delle Amministrazioni sia in modalità SSH, sia RDP, sia tramite l'utilizzo della dashboard Horizon.

I Zabbix Manager, aggregatori del traffico di monitoraggio del singolo tenant, saranno messi in comunicazione con i sistemi di back-end interni del RTI necessari all'erogazione dei servizi Managed (correlatori degli eventi, repository delle policy di monitoraggio, asset manager, etc.) implementando opportuni filtraggi ed utilizzando una Provider Network.

I server Zabbix Manager avranno pertanto anche la funzionalità di disaccoppiare l'ambiente centralizzato di back-nd preposto per la gestione del servizio con i Tenant delle singole Amministrazioni.

Di seguito un modello di architettura di monitoraggio:



4.1.4.3. Architettura Zabbix - piattaforma centralizzata degli allarmi

Di seguito è descritto un approfondimento dei sistemi e tecnologie individuate per il monitoraggio della soluzione.
ZABBIX è una soluzione finalizzata a controllare i sistemi dall'interno ed all'occorrenza anche da remoto in analogia con quanto è possibile fare per i più comuni apparati di rete.

Zabbix effettua la verifica costante del funzionamento e delle prestazioni di HW/OS/Middleware con l'intento di rilevare e segnalare, in maniera proattiva, possibili condizioni che potrebbero determinare il degrado o il blocco dei servizi erogati.

In una configurazione standard Zabbix è in grado di segnalare:

- superamento di determinate soglie su utilizzo di risorse quali CPU, memoria, spazio disco;
- presenza/assenza/numerosità di determinati processi running sul sistema;
- presenza/assenza/stato di determinati servizi (applicabile per Windows);
- analisi di determinati logfile per determinare situazioni di errore;
- analisi degli elementi del Event Viewer di windows.

L'architettura di prodotto prevede una componente Manager centralizzata (ZABBIX Manager) ed una componente distribuita (ZABBIX Agent), attiva sui sistemi target.

Nella piattaforma integrata adottata dal RTI il Manager Zabbix inoltra le segnalazioni verso la piattaforma di Event Management centralizzata di back end.

Tale piattaforma centralizzata permette le seguenti funzioni:

- Normalizzazione delle segnalazioni in un unico repository centralizzato di eventi
- Correlazione degli eventi, secondo regole personalizzabili, che consentono:
  - la de-duplicazione degli eventi (gestione unica istanza di eventi duplicati e ricorrenti);
  - la chiusura automatica degli eventi relativi ad anomalie risolte;
  - root-cause analysis e cioè l'individuazione dell'evento primario (causa) tra un insieme di più eventi secondari (effetto).
- Arricchimento degli eventi di allarme con le informazioni logistiche, amministrative e di business inerenti la risorsa oggetto della segnalazione;
- Visualizzazione, in real-time, di un insieme di segnalazioni originate da sorgenti eterogenee e distribuite.

4.1.5. Backup & Restore delle VM

L'attivazione del servizio gestito delle VM IaaS, PaaS prevede l'implementazione del backup dei sistemi con profili legati ai volumi salvati descritti nel servizio BaaS:

La retention massima prevista per le informazioni è di 90 giorni con limite legato al profilo dei volumi selezionato comprensivo anche di salvataggi on-demand.

Le policy di back up applicate per tale servizio saranno le seguenti:

- Back up incrementale giornaliero;
- Back up full settimanale.

Qui di seguito si specifica il tipo di ripristino assicurato dal restore:

- backup dell'intero file system della vm;
- viene garantito il ripristino della vm all'ultimo backup effettuato secondo le policy sopradefinite;
- viene garantita una consistenza di tipo "crash-consistency";
- permette una gestione puntuale per il restore di singoli file.

Il servizio di back up & restore, nei servizi managed, sostituisce la modalità di back up della VM basata su snapshot attualmente implementata per i servizi unmanaged.

4.1.6. Sicurezza degli ambienti OpenStack

In questo paragrafo sono descritte, con particolare riguardo alla sicurezza logica, le caratteristiche degli ambienti OpenStack che saranno messi a disposizione per l'implementazione del servizio.
Per ogni Amministrazione sarà ritagliata una porzione logica delle risorse infrastrutturali (rete, sicurezza, server farm e storage) e sarà garantita la separazione logica degli ambienti assegnati a ciascuna Amministrazione proprio dalla tecnologia OpenStack che consente appunto la completa segregazione dei tenant.

Sottosistemi Storage

Per eliminare il rischio di downtime dovuti a guasti hardware, la piattaforma OpenStack è completamente diskless. Questo significa che i server non includono alcun disco locale e i dati sono memorizzati esclusivamente in una Storage Area Network (SAN) ingegnerizzata per i servizi di storage.
La SAN implementata nei DC attraverso l'interconnessione di storage array e DirectorFC garantisce assenza di Single Point Of Failure, monitoraggio preventivo degli errori per limitare i failure di sistema, possibilità di sostituire o aggiungere componenti hw senza completo fermo del sistema, possibilità di aggiornare il firmware minimizzando i fermi del sistema.

La soluzione assicura:

- **Separazione Fisica**. Separazione fisica delle infrastrutture SAN di Boot e Dati;
- **Separazione Logica**. Partizionamenti logici delle risorse Storage Box e SAN Switch;
- **Alta Affidabilità**. Componenti fisici ridondati, dischi configurati in RAID5 e dischi hot-spare così da garantire continuità anche in caso di problemi hardware;
- **Scalabilità.** L'infrastruttura è in grado di supportare richieste di workload addizionale sia allocando nuove risorse (scalabilità orizzontale) sia incrementando le capacità delle risorse già disponibili (scalabilità verticale).

Isolamento VM

Sono utilizzate le migliori tecnologie di virtualizzazione attualmente presenti sul mercato che garantiscono una separazione logica dei sistemi operativi che impedisce la visibilità dei dati tra Amministrazioni che utilizzano la stessa piattaforma condivisa.
La virtualizzazione di OpenStack alloca le risorse in maniera intelligente isolando completamente le macchine virtuali dal sottostante layer fisico. Pertanto una singola virtual machine non può utilizzare tutte le risorse o causare il crash dell'host fisico.

La tecnologia OpenStack fornisce uno strato software che si pone tra l'hardware del sistema ed il sistema operativo in modo tale da costituire ambienti fisici virtuali completi e separati l'uno dall'altro, definiti "virtual machine". Questi sono a tutti gli effetti visti come 'n' piattaforme x86 coesistenti su un unico sistema fisico, realizzando pertanto una sorta di "partizionamento" logico.
La singola applicazione può operare nella "virtual machine" assegnata, in modo completamente indipendente dalle altre, nelle rispettive distinte partizioni. La logica di virtualizzazione consente accesso diretto alle risorse hardware.
Il risultato è avere più applicazioni che operano su uno stesso sistema fisico, in ambienti completamente separati, con un utilizzo delle risorse ottimizzato in quanto la condivisione consente di creare combinazioni di applicazioni con profili di carico diversi, tali da massimizzare il tempo di utilizzo della CPU.

4.1.7. Hardening della soluzione

I sistemi installati in Cloud presso il Data Center nonché gli apparati installati on premise presso le Amministrazioni, prima dell'esercizio vengono "hardenizzati".

L'hardening consiste nell'attuazione di tecniche che permettono di irrobustire una piattaforma, considerando tutti gli aspetti del sistema informatico, dall'autenticazione degli utenti, sino all'integrità dei dati e del file system, passando per una configurazione congrua del kernel, il tutto al fine di eliminare le vulnerabilità comuni e ridurre al minimo il numero di servizi di base che sono disponibili.

Al fine di massimizzare la sicurezza delle piattaforme pertanto si avviano i processi di:

- ***hardening post-installazione****:*

  per le piattaforme gestite viene effettuato solo una volta, alla fine del setup, nella fase di delivery, prima di rilasciare la piattaforma predisposta; per i sistemi interni viene effettuato prima del collaudo definitivo.

- ***hardening periodico***:

  viene eseguita più volte, durante l'esercizio dei sistemi interni, la verifica dello stato di patching in relazione ai security alert rilevanti; in caso si ritenga necessaria sarà effettuata un'attività di hardening dei sistemi.

4.1.8. Modalità di accesso cliente alle VM

Relativamente ai servizi di virtualizzazione, sia Unmanaged che Managed, per l'accesso ai server ai fini della gestione in base all'opzione contrattualizzata, le Amministrazioni potranno optare tra due modalità di accesso:

1. Accesso diretto da internet su interfaccia di rete pubblica del server virtuale via SSH o RDP Modalità prevista nel servizio base;
2. Accesso via VPN configurata sul tenant del server virtuale. Modalità potrà essere adottata aderendo a servizi aggiuntivi di sicurezza.

La modalità 1 prevede la generazione e scambio delle chiavi di autenticazione tra client dell'amministrazione e server la cui gestione e configurazione è demandata alla Control Room solo per servizi Managed.

La modalità 2 garantisce un livello di sicurezza più elevato. Per la modalità 2, il Cloud provider predisporrà un servizio di VPN terminata direttamente all'interno del tenant del server dell'Amministrazione. Nella fattispecie, all'interno del tenant dell'Amministrazione sarà implementato, dalla Control Room del cloud Provider, un VPN Concentrator esposto su Internet tramite Floating IP address, attraverso il quale si potrà stabilire l'accesso alle VM e alle Applicazioni dell'Amministrazione mediante tunnelling VPN.

Il VPN Concentrator sarà configurato dalla Control Room in termini di Security Group e Routing IP affinchè possa consentire l'accesso agli indirizzi IP privati delle VM/Applicazioni all'interno del tenant della Amministrazione.

Il VPN Concentrator utilizzato sarà gestito ed amministrato dal Provider. L'Amministrazione dovrà sempre richiedere via Ticketing (Richiesta di Change) al Provider di abilitare determinate configurazioni per garantire l'accesso ad eventuali partner tecnologici terzi per la gestione VM/Applicazioni.

Per i servizi Managed il Cloud Provider renderà disponibile alle Amministrazioni differenti profilature di utenze sulla base del profilo di servizio contrattualizzato:

- Utenza RTI per la gestione delle risorse infrastrutturali, dei sistemi operativi e dei solution stack (erogazioni profili PaaS);
- Utenza per l'Amministrazione per la gestione degli applicativi dell'Amministrazione

Nel caso in cui l'Amministrazione contrattualizzi solamente il Profilo IaaS managed oppure, nell'ambito della fattibilità che sarà effettuata dal RTI a seguito della ricezione del piano dei fabbisogni, emerga l'impossibilità di gestire il PaaS, saranno resi disponibili due differenti profili di utenze di amministrazione dei sistemi:

- Utenza RTI per la gestione delle risorse infrastrutturali e dei sistemi operativi (erogazioni profilo IaaS managed);
- Utenza per l'Amministrazione per la gestione del Middleware e degli applicativi dell'Amministrazione.

4.1.9. Modalità di controllo degli accessi alle VM da parte degli addetti IT

La sicurezza delle informazioni e dei processi aziendali che ne consentono l'utilizzo in ambito IT ha come obiettivo primario la protezione dei dati e degli elementi presenti all'interno dei sistemi informatici aziendali.
Deve pertanto essere assicurato l'accesso logico alle risorse informatiche in modalità sicura, attraverso la definizione di un corretto processo di gestione delle utenze e dei relativi privilegi, per l'accesso ai sistemi informatici e per il trattamento dei dati in essi presenti; tale accesso logico deve avvenire nel pieno rispetto delle normative vigenti e dei principi di sicurezza e salvaguardia dei dati, adottati dal RTI.
Per far ciò, sarà utilizzato un framework per l'applicazione dei requisiti di controllo degli accessi e tracciamento dell'operatività da parte degli addetti IT su tutte le componenti dell'infrastruttura di rete e IT.
Il framework utilizzato sposta il paradigma di applicazione delle misure di sicurezza dal target al mediatore, implementando gli interventi solo su quest'ultimo, che rappresenta il tramite per l'accesso ai sistemi.

Di seguito le caratteristiche principali:

- Gestione delle utenze degli Addetti IT per l'accesso ai Sistemi Operativi, Database e Applicazioni;
- Garanzia di una corretta profilazione degli accessi e dei privilegi assegnati agli Addetti IT garantendo i principi di Segregation of Duties derivanti da policy e linee guida aziendali;
- Garanzia del rispetto dei vincoli legislativi (a.e. 196/03; Provvedimenti Garante, ISO27001etc,) e delle policy di sicurezza aziendali;
- Garanzia circa l'uniformità della user experience e delle modalità di amministrazione delle infrastrutture di rete ed IT;
- Autorizzazione e autenticazione per l'accesso ai singoli target, con la possibilità di applicare la strong autentication;
- Workflow autorizzativo secondo il processo indicato dalle policy aziendali consolidate per l'assegnazione/rimozione di utenti e relativi privilegi;
- Monitoraggio e campagne di verifica periodiche sulla corretta abilitazione delle utenze;
- Tracciamento delle attività svolte dagli utenti abilitati.