

## PROCEDURA DI INSTALLAZIONE SERVER PaaS

### Elenco server di infrastruttura della piattaforma PaaS

Di seguito si riporta l'elenco delle macchine necessarie per installare la piattaforma PaaS.

Segue il dettaglio per l'installazione dei servizi nelle singole VM.

- **WEBUI (2 VM):** portale PaaS
- **Database:** DMBS per archiviazione dati di funzionamento della PaaS
- **Business Layer (2 VM):** contiene il servizio di orchestrazione
- **Proxy Apache:** proxy per le macchine del Business Layer e della WebUI
- **Cloudify (1 VM shell in orchestrator + 1 VM Manager per project utente)**
- **Monitoring - Zabbix (3 VM)**
- **DNS:** server DNS per la gestione dei domini usati nella PaaS
- **EJBCA:** macchina per la gestione di una certification authority
- **Mail server:** macchina che fornisce un mail server
- **Repository - Template/Ricette:** contiene i template Heat e le ricette Cloudify
- **Playsms:** eroga un servizio di SMS
- **SMS gateway modem:** dispositivi hardware corredato di SIM per l'invio di SMS.
- **Maven (Opzionale):** solo per sviluppo codice
- **Idp PaaS:** macchina che ospita l'IdP della piattaforma PaaS

La presente guida si trova all'interno della cartella **CONFIGURAZIONI**, all'interno della quale sono presenti delle sottocartelle contenenti, ognuna, la guida all'installazione dello specifico componente della piattaforma PaaS al quale si riferiscono (Figura 1).

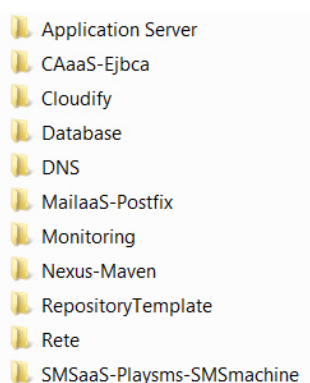


Figura 1 - Struttura della directory

Le macchine da installare sono tutte relative al project Orchestrator, tranne la macchina Cloudify Manager che va nel project/tenant associato **ad ogni** workgroup. Per quanto riguarda la rete, si rimanda alla relativa documentazione presente nella sottocartella **“Rete”**.

## 0. Configurazioni comuni ai singoli server di Infrastruttura

Per ciascuna VM creata, aggiornare ora e data in modo da sincronizzare la visualizzazione dei log di sistema, per le problematiche legate ai token/sicurezza, etc... (WEBUI, BizLayer, Database ...).

Utilizzare i seguenti comandi:

```
sudo touch /etc/cron.daily/ntpdate
echo ntpdate ntp1.inrim.it | sudo tee -a /etc/cron.daily/ntpdate
sudo chmod 755 /etc/cron.daily/ntpdate
echo "Europe/Rome" | sudo tee /etc/timezone
sudo dpkg-reconfigure --frontend noninteractive tzdata
```

Si fa notare che il seguente Security Group, che si trova di default nelle installazioni di OpenStack, non verrà utilizzato:

- default
  - ALLOW IPv4 icmp from 0.0.0.0/0
  - ALLOW IPv4 to 0.0.0.0/0
  - ALLOW IPv6 from default
  - ALLOW IPv6 to ::/0

## 1. WEBUI SERVER

**Descrizione servizio: UI layer** (User Interface): fornisce una web console per la gestione dei servizi attivati dall'utente (lista dei servizi, risorse consumate da ciascun servizio, performance, costi)

**Nome macchina (suggerito):** pr01www01

**Flavor:** 4 CPU - 8 RAM - 20GB disk

**O.S + tool base:** Ubuntu 14.04 – JDK 7 – Tomcat

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM

http-trusted

```
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
```

JVM-development

```
ALLOW IPv4 8787/udp from 0.0.0.0/0
ALLOW IPv4 8787/tcp from Orchestrator/subnet
```

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

#### JMX-monitoring

ALLOW IPv4 9990/tcp from 0.0.0.0/0  
ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 8000/tcp from 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 9999/tcp from 0.0.0.0/0

**Osservazioni:** ai fini dell'utilizzo del portale PaaS, si può abilitare o meno la console di amministrazione di tomcat, alla quale si può accedere come amministratore oppure con user con ruoli minori. Questa configurazione deve essere effettuata in uno specifico file sul server (tomcat-users.xml file). Nel caso si voglia abilitare tale funzionalità, è possibile trovare le informazioni all'interno dei file di configurazione e guide di installazione relative al portale.

**Guida all'installazione dei servizi:** Vedere manuale di installazione sotto la cartella:

*CONFIGURAZIONI → Application Server → Tomcat → doc : [Configurazione per il Portale Tomcat](#)*

Nel documento è specificato il pacchetto saml da importare sul server. Il pacchetto si trova dentro la cartella *Application Server Tomcat → saml\_configuration*; nella cartella è presente anche la guida per configurare il SSO tramite IDP SAML

L'URL del portale web va registrato sul server DNS che gestisce il dominio in uso. Ad esempio, se il dominio è *dominio.it*, sul server DNS che gestisce tale dominio va inserito un record A con l'IP del server che ospita il portale e l'URL con cui raggiungere il portale (es. portale.*dominio.it*).

Valutare a livello di esposizione del sito, quale dominio si vuole avere. Una volta deciso, configurarlo con il certificato opportuno, ed abilitare HTTPS (es. con porte 443 od 8443)

*Esecuzione del deploy del portale su application server Tomcat*

**Per poter effettuare il deploy della WEBUI, il business layer deve essere in running. Pertanto:**

- Assicurarsi che il Business Layer sia online prima di avviare Tomcat con il WAR della WEBUI;
- Scaricare il war del portale (oppure fare l'export del war da Eclipse) ed andare ad inserirlo nella specifica folder di Tomcat

## 2. DATABASE PaaS

**Nome macchina (suggerito):** pr01dbs01

**Descrizione servizio:** contiene i dati della piattaforma PaaS

**Flavor:** 4 CPU - 8 RAM - 50 GB disk

**O.S + tool base:** Ubuntu 14.04 - Pacchetto LAMP- MySQL 5.6.21

(La versione di MySQL richiesta per il Business Layer è di almeno 5.6.20)

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM

http-trusted

```
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
```

zabbix\_agent

```
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
```

mysqldb-secgroup

```
ALLOW IPv4 3306/tcp from Orchestrator/subnet
ALLOW IPv4 3306/tcp from Orchestrator/subnet
ALLOW IPv4 3306/tcp from Orchestrator/subnet
```

#### Osservazioni:

La VM è stata installata con la versione di MySQL 5.6.21, settato anche un diverso session timeout per i server con phpmyadmin (ma non è detto che lo si debba installare).

Sulla base delle policy interne dell'Ente/Azienda che installa la PaaS, è possibile limitare l'accesso a MySQL ad un IP specifico (es. solo al business layer) oppure a qualsiasi IP o ai due BL.

**Guida all'installazione dei servizi:** il manuale di installazione del Database si trova in

*CONFIGURAZIONI* → *Database* → doc: [INSTALLAZ\\_DB\\_MYSQL](#)

Creare i vari schema usando per convenzione gli stessi nomi: \_paas, prisma\_jbpm\_pr01biz01, prisma\_jbpm\_pr01biz02 di tipo latin1\_swedish\_ci. (sono InnoDB). Questo viene selezionato da interfaccia web di phpmyadmin durante la creazione dei vari schema

Mettere i dump sql relativi alla specifica release che si vuole caricare:

- *prisma\_paas*
- *prisma\_jbpm\_pr01biz01* Prendere i dump già puliti vedi file elencati nel paragrafo più avanti
- *prisma\_jbpm\_pr01biz02* Prendere i dump già puliti vedi file elencati nel paragrafo più avanti

ed importarli. (Es. con phpmyadmin se troppo pesanti i file sql, è consigliabile prima zipparli e poi caricare il file, vedi screenshot sottostante).

Importazione nel database "

**File da importare:**

Il file può essere compresso (gzip, bzip2, zip) o non compresso.  
 Il nome di un file compresso deve terminare in **[formato].[compressione]**. Ad esempio: **.sql.zip**

Cerca sul tuo computer:  Nessun file selezionato. (Dimensione massima: 2,048KiB)

Set di caratteri del file:

**Importazione parziale:**

☒ Allow the interruption of an import in case the script detects it is close to the PHP timeout limit. (This might be a good way to import large files, however it can break transactions.)

Numero di righe da saltare dall'inizio:

**Formato:**

**Opzioni specifiche al formato:**

Modalità di compatibilità SQL:

☒ Non usare AUTO\_INCREMENT per il valori zero

Per jBPM (Orchestrator/Business Layer) usare i dump già puliti. Essi si trovano in:

**CONFIGURAZIONI → Database → JBPMdump**

[mysql-innodb-jbpm-schema.sql](#)

[quartz\\_tables\\_mysql\\_innodb.sql](#)

Per ogni schema `prisma_jbpm_pr01biz__`, importarli entrambi.

Ricordarsi poi di aggiungere il database come endpoint nel file di configurazione di jboss dei Business Layer. (vedi paragrafo successivo per i dettagli di configurazione)

Apertura porta 3306 (default mysql, a meno di problemi di blocking sul firewall).

Una volta caricati i dump, ricordarsi di modificare alcune impostazioni nel database come ad esempio le image nella tabella configuration di `prisma_paas` in base alle immagini di openstack su cui si va ad operare (che rispettivamente saranno poi anche in un file di properties del business layer), la tabella Organization, Workgroup e la tabella IDP. Inoltre nella tabella `laaSNetwork` bisogna mettere i dati di openstack:

```
INSERT INTO `laaSNetwork` (`laaSNetworkID`, `adminStateUp`, `name`, `openstackId`, `routerExternal`, `shared`, `status`, `tenantId`, `workgroupId`) VALUES
```

Prendere tipo `prismaDemo` (`prismaDemo`), mettere come name il nome della network a cui sono attaccate le vm, cliccare su quella rete, prendere il suo ID che è l'`openstackID`, prendere inoltre il suo `projectID` che è il suo `tenantID`.

### 3. BUSINESS LAYER

**Descrizione servizio:** Si occupa di orchestrare i flussi tra i diversi componenti della piattaforma PaaS.

**Nome macchina (suggerito):** `pr01biz01` (la seconda si chiamerà `pr01biz02`)

**Flavor:** 4 CPU - 8 RAM - 20 GB disk (Suggerita almeno questa)

**O.S + tool base:** Ubuntu Server 12.04, JDK 7. (Si può usare anche 14.04..)

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM

#### http-trusted

```
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
```

#### JVM-development

```
ALLOW IPv4 8787/udp from 0.0.0.0/0
ALLOW IPv4 8787/tcp from Orchestrator/subnet
```

#### appaas-srcfile-repo

```
ALLOW IPv4 8080/tcp from Orchestrator/subnet
ALLOW IPv6 to ::/0
ALLOW IPv4 to 0.0.0.0/0
ALLOW IPv4 8080/tcp from Orchestrator/subnet
```

#### zabbix\_agent

```
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
```

#### JMX-monitoring

```
ALLOW IPv4 9990/tcp from 0.0.0.0/0
ALLOW IPv4 to 0.0.0.0/0
ALLOW IPv4 8000/tcp from 0.0.0.0/0
ALLOW IPv6 to ::/0
ALLOW IPv4 9999/tcp from 0.0.0.0/0
```

#### Osservazioni:

Installare due business layer per averne uno di appoggio in caso di rottura del primo.

Per quanto riguarda invece i file di JBOSS 7.1.1 final, prendere quello che è già configurato per JBPM che si trova su SVN e poi configurarlo opportunamente (vedi doc sotto). Ricordarsi di modificare il file di configurazione con tutti gli endpoint corretti (Database, etc...) in **standalone\_full.xml**

**Guida all'installazione dei servizi:** il manuale di installazione per il business Layer si trova in

*CONFIGURAZIONI → Application Server → JBOSS → doc:*

- *Config\_JBOSS\_orchestrator*
- *Business Layer configuration per EJBCA*
- *BUSINESS LAYER configuration per MailaaS*

Una volta messo l'application server ed importato il war, andare a modificare i files di properties:

opt/jboss-as-7.1.1.Final/standalone/deployments/business-layer.war/WEB-INF/classes#

more configuration.README

e leggere quali sono i files da aggiornare con tutti gli endpoint, pwd etc..

#### 4. PROXY APACHE

**Descrizione servizio:** Si occupa di orchestrare i flussi tra i diversi componenti della piattaforma PaaS.

**Nome macchina (suggerito):** pr01apiproxy01

**Flavor:** 2 CPU - 4 RAM - 20 GB disk

**O.S + tool base:** Ubuntu 14.0

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

http-public

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv6 to ::/0

ALLOW IPv4 8443/tcp from 0.0.0.0/0  
ALLOW IPv4 8080/tcp from 0.0.0.0/0  
ALLOW IPv4 80/tcp from 0.0.0.0/0  
ALLOW IPv4 443/tcp from 0.0.0.0/0

**Osservazioni:** Valutare l'utilizzo del proxy per le chiamate API/REST.

**Guida all'installazione dei servizi:** il manuale è sotto:

*CONFIGURAZIONI → Reverse Proxy → doc: N/A for now*

Configurare opportunamente con gli endpoint del Business Layer corretto.

## 5. CLOUDIFY SERVERS

**Descrizione servizio: PaaS Deployment Layer (Cloudify):** ha in carico il deploy delle applicazioni e il loro ciclo di vita. Per ciascun servizio, viene creata una ricetta contenente gli elementi di cui si compone il servizio, la quale viene eseguita per il provisioning del servizio stesso.

**Il servizio Cloudify si compone di due tipologie di VMs:**

- 1 Macchina shell per il tenant Orchestrator, nota come Cloudify Shell
- 1 Macchina Manager per ciascun project (associato ad un workgroup o azienda)

### Cloudify SHELL

**Descrizione:** contiene il Servizio che consente di eseguire il bootstrap della VM Manager in un opportuno project di OpenStack.

**Nome macchina (suggerito):** pr01cloudifysh01

**Flavor:** 2 CPU - 4 RAM - 20GB disk

**O.S + tool base:** Ubuntu 12.04 – JDK 6

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM

zabbix\_agent

- ALLOW IPv4 10050/tcp from Orchestrator/subnet
- ALLOW IPv4 10050/tcp from Orchestrator/subnet
- ALLOW IPv4 10050/tcp from Orchestrator/subnet

**Guida all'installazione dei servizi:** il manuale di installazione della Cloudify Shell ed i passi per il bootstrap delle Vm di Management si trovano sul NAS alla seguente folder:

*CONFIGURAZIONI → Cloudify → doc: [Installazione Cloudify shell](#)*



In particolare, l'applicazione Cloudify si trova nella cartella:

*CONFIGURAZIONI → cloudify-2.7.2reply.zip*

### **Cloudify Manager**

**Descrizione:** si tratta di una VM che fornisce il servizio di PaaS deployment per il project nel quale sono installate. Vengono installate e configurate mediante processo di Bootstrap lanciato dalla Cloudify Shell

**Nome macchina:** viene configurato nella Cloudify Shell. Tipicamente è **cfy-mngt-1**

**Flavor:** viene configurato nella Cloudify Shell. Tipicamente è **4 CPU - 8 RAM - 20GB disk**

**O.S + tool base:** Ubuntu 12.04 – JDK 6 – Cloudify agent

**Security Group:** vengono configurati nella Cloudify Shell. Tipicamente sono:

cfy-mngt-management

```
ALLOW IPv6 to ::/0
ALLOW IPv4 8099/tcp from 0.0.0.0/0
ALLOW IPv4 7010-7110/tcp from cfy-mngt-cluster
ALLOW IPv4 7003/tcp from cfy-mngt-cluster
ALLOW IPv4 7001/tcp from cfy-mngt-cluster
ALLOW IPv4 7000/tcp from cfy-mngt-cluster
ALLOW IPv4 7002/tcp from cfy-mngt-cluster
ALLOW IPv4 22/tcp from 0.0.0.0/0
ALLOW IPv4 4174/tcp from cfy-mngt-cluster
ALLOW IPv4 6666/tcp from cfy-mngt-cluster
ALLOW IPv4 8100/tcp from 0.0.0.0/0
ALLOW IPv4 to 0.0.0.0/0
```

cfy-mngt-cluster

```
ALLOW IPv4 to 0.0.0.0/0
ALLOW IPv6 to ::/0
```

## **6. MONITORING SERVER**

**Descrizione servizio: Monitor Aggregator Platform:** si tratta di un modulo per il monitoraggio dei componenti PaaS e dei servizi “as a Service” allocati agli utenti. Tale modulo si basa sui servizi di Zabbix. Componenti e servizi godono di un agent di monitoraggio che invia le metriche.

Il servizio si compone di 4 VMs:

- **1 Macchina di Monitoring (Pillar)**, avente le seguenti caratteristiche:
  - Nome macchina (suggerito):** pr01monit01
  - Flavor:** 2 CPU - 4 RAM - 20 GB disk
  - O.S + tool base:** Ubuntu 12.04
  - Security Group:** di seguito l'elenco dei Security Group da associare alla VM

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

JVM-development

ALLOW IPv4 8787/udp from 0.0.0.0/0  
ALLOW IPv4 8787/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

JMX-monitoring

ALLOW IPv4 9990/tcp from 0.0.0.0/0  
ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 8000/tcp from 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 9999/tcp from 0.0.0.0/0

ssh-reply-only

ALLOW IPv4 22/tcp from Orchestrator/subnet  
ALLOW IPv4 22/tcp from Orchestrator/subnet  
ALLOW IPv4 22/tcp from Orchestrator/subnet

**Guida all'installazione dei servizi:** Il tutorial di installazione si trova alla seguente folder:  
*CONFIGURAZIONI* → *Monitoring* → *Guida monitoring pillar* → doc: Monitoring.docx

### - 3 Macchine Zabbix

- Nome macchina: zabbix-iaas
  - **Flavor:** 2 CPU - 4 RAM - 20 GB disk
  - **O.S + tool base:** Ubuntu 14.04
  - **Security Group:**

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

#### zabbix\_server

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 10051/tcp from 0.0.0.0/0  
ALLOW IPv6 to ::/0

#### http-public

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 8443/tcp from 0.0.0.0/0  
ALLOW IPv4 8080/tcp from 0.0.0.0/0  
ALLOW IPv4 80/tcp from 0.0.0.0/0  
ALLOW IPv4 443/tcp from 0.0.0.0/0

- **Nome macchina:** zabbix-metrics
  - **Flavor:** 2 CPU - 4 RAM - 20 GB disk
  - **O.S + tool base:** Ubuntu 14.04
  - **Security Group:**

#### http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

#### zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

#### zabbix\_server

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 10051/tcp from 0.0.0.0/0

ALLOW IPv6 to ::/0

http-public

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 8443/tcp from 0.0.0.0/0  
ALLOW IPv4 8080/tcp from 0.0.0.0/0  
ALLOW IPv4 80/tcp from 0.0.0.0/0  
ALLOW IPv4 443/tcp from 0.0.0.0/0

- **Nome macchina:** zabbix-watcher
  - **Flavor:** 2 CPU - 4 RAM - 20 GB disk
  - **O.S + tool base:** Ubuntu 14.04
  - **Security Group:**

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

zabbix\_server

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 10051/tcp from 0.0.0.0/0  
ALLOW IPv6 to ::/0

http-public

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 8443/tcp from 0.0.0.0/0  
ALLOW IPv4 8080/tcp from 0.0.0.0/0  
ALLOW IPv4 80/tcp from 0.0.0.0/0  
ALLOW IPv4 443/tcp from 0.0.0.0/0

**Guida all'installazione dei servizi:** Il tutorial di installazione si trova alla seguente folder:

[CONFIGURAZIONI](#) → [Monitoring](#) → [Guida Zabbix Server](#) → doc: Monitoring Zabbix 2.2 - Installazione e Configurazione.docx

**Osservazioni:** Per l'infrastruttura di rete da utilizzare per le macchine di monitoring, fare riferimento alla guida presente nella cartella:

[CONFIGURAZIONI](#) → Rete

## 7. DNS SERVER

**Descrizione servizio:** server DNS per la gestione dei sottodomini di infrastruttura.

**Nome macchina (suggerito):** pr01dns01

**Flavor:** 1 CPU - 1 RAM - 10GB disk

**O.S + tool base:** Ubuntu 14.04 + bind9

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

dns-secgroup

ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv6 to ::/0  
ALLOW IPv4 10000/tcp from Orchestrator/subnet  
ALLOW IPv4 53/udp from 0.0.0.0/0  
ALLOW IPv4 4567/tcp from 0.0.0.0/0  
ALLOW IPv4 icmp from 0.0.0.0/0  
ALLOW IPv4 53/tcp from 0.0.0.0/0

**Guida all'installazione dei servizi:** il file di configurazione si trova alla seguente folder:

[CONFIGURAZIONI](#) → [DNS](#) → doc: [Server DNS](#)

## 8. EJBCA SERVER

**Descrizione servizio:** servizio che implementa una CA

**DNS name:** La macchina per convenzione avrà sul dns il seguente nome: ca01.dominio.mio

(la seconda avrà ca02.dominio.mio). Configurare il dns prima di fare ant deploy ed ant install.

**Nome macchina (suggerito):** pr01servejbca01

**Flavor:** 4 CPU - 4 RAM - 20 GB disk

**O.S + tool base:** Ubuntu server 12.04

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

ejbca-secgroup

ALLOW IPv6 to ::/0  
ALLOW IPv4 9990/tcp from 0.0.0.0/0  
ALLOW IPv4 4447/tcp from 0.0.0.0/0  
ALLOW IPv4 9999/tcp from 0.0.0.0/0  
ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 8443/tcp from 0.0.0.0/0

**Guida all'installazione dei servizi:** il file di configurazione si trova alla seguente folder:

*CONFIGURAZIONI → CaaS-Ejbca → doc:*

- *Installazione EJBCA 6.2.0 su Ubuntu*
- *Configurazioni necessarie per l'utilizzo dei WS di EJBCA*

Download del codice EJBCA (versione 6\_2\_0) dal seguente link:  
<http://sourceforge.net/projects/ejbca/files/ejbca6/>

All'interno della folder *CONFIGURAZIONI → CaaS-Ejbca*, è presente un file **it.zip** che serve per la macchina Maven per importare le jar library che servono per lo sviluppo relativamente ad ejbca. Per questo vedi paragrafo dedicato all'installazione della vm per Maven/Nexus.

## 9. Mail server

**Prerequisiti:**

- sapere quale dominio usare per le mail es. @miodominio.it
- configurare il DNS, record MX ed SPF (vedere file di configurazione ed installazione)
- Per configurare il TLS alla fine della installazione, si consiglia di utilizzare un certificato generato dalla macchina di ejbca installata per la piattaforma PaaS.

**Descrizione servizio:** servizio che implementa un mail server

**DNS name:** La macchina per convenzione avrà sul dns il seguente nome: mail01.dominio.mio (mentre la seconda avrà come convenzione mail02.dominio.mio).

**Nome macchina (suggerito):** pr01mail01

**Flavor:** 2 CPU - 2 RAM - 50 GB disk

**O.S + tool base:** Ubuntu server 14.04

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

http-trusted

ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

mysql-trusted

ALLOW IPv6 to ::/0  
ALLOW IPv4 3306/tcp from Orchestrator/subnet  
ALLOW IPv4 3306/tcp from Orchestrator/subnet  
ALLOW IPv4 to 0.0.0.0/0  
ALLOW IPv4 3306/tcp from Orchestrator/subnet

**Guida all'installazione dei servizi:** il file di configurazione si trova alla seguente folder:

**CONFIGURAZIONI** → **MailaaS-Postfix** → doc:

- [INSTALL\\_SERVER\\_POSTFIX](#)
- [Configurazione TLS](#)

*Installazione di Postfix, pacchetto MYSQL, SASL e configurazione (creazione account mail per i servizi della piattaforma PaaS, account per BL, per Monitoring, per SMS alert..).*

*Postfix-tls non va installato perchè già integrato in Postfix, ma è da configurare con i certificati, come spiegato nel file: Configurazione TLS*

## 10. Repository

**Descrizione servizio:** servizio per lo storage dei template

**Nome macchina (suggerito):** pr01repo01

**Flavor:** 2 CPU - 4 RAM - 20 GB disk

**O.S + tool base:** Ubuntu server 14.04

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

http-trusted

```
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 443/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8080/tcp from Orchestrator/subnet
```

zabbix\_agent

```
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
ALLOW IPv4 10050/tcp from Orchestrator/subnet
```

http-public

```
ALLOW IPv4 to 0.0.0.0/0
ALLOW IPv6 to ::/0
ALLOW IPv4 8443/tcp from 0.0.0.0/0
ALLOW IPv4 8080/tcp from 0.0.0.0/0
ALLOW IPv4 80/tcp from 0.0.0.0/0
ALLOW IPv4 443/tcp from 0.0.0.0/0
```

Attualmente ogni IaaS Environment (installazione IaaS) deve avere un proprio repository, speculare nei template/ricette, ma diverso nei file d'environment per i template Heat.

**Guida all'installazione dei servizi:** il file di configurazione si trova alla seguente folder:

*CONFIGURAZIONI* → *RepositoryTemplate* → doc: *INSTALL\_Repo\_server*

Dovranno essere poi caricati gli opportuni template.

## 11. Playsms and SMS Gateway

**Descrizione servizio:** Macchina dedicata al servizio SMSaaS, collegata ad un SMS Gateway (attualmente in utilizzo solo un SMSgateway a Bari)

**Nome macchina (suggerito):** pr01servplaysms01

**Flavor:** 2 CPU - 4 RAM - 20 GB disk

**O.S + tool base:** Ubuntu server 14.04

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

http-trusted

```
ALLOW IPv4 80/tcp from Orchestrator/subnet
ALLOW IPv4 8443/tcp from Orchestrator/subnet
```



ALLOW IPv4 8080/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 443/tcp from Orchestrator/subnet  
ALLOW IPv4 8443/tcp from Orchestrator/subnet  
ALLOW IPv4 80/tcp from Orchestrator/subnet  
ALLOW IPv4 8080/tcp from Orchestrator/subnet

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

mysqldb-secgroup

ALLOW IPv4 3306/tcp from Orchestrator/subnet  
ALLOW IPv4 3306/tcp from Orchestrator/subnet  
ALLOW IPv4 3306/tcp from Orchestrator/subnet

La relase da utilizzare è la V3: [playSMS-1.0-rc2\\_Modified\\_V3](#)

con relativo file doc abbinato: [README\\_playSMS\\_modified](#)

Installare phpmyadmin per accedere alle tabelle di MySQL di playSMS, se si vuole avere una interfaccia web per il db MySQL.

In alcuni casi per maintainance potrebbe essere utile pulire la tabella degli SMS già inviati.

**Guida all'installazione dei servizi:** il file di configurazione si trova alla seguente folder:

*CONFIGURAZIONI → SMSaaS-Playsms-SMSmachine → doc:*

- [Installazione PLAYSMS-VersioneModificata](#)
- [Configurazione SMSmachine](#)
- [playSMS-1.0-rc2\\_Modified\\_V3](#)
- [README\\_playSMS\\_modified](#)

Ricordarsi di dare credito all'utente amministratore, settare Timezone giusto, di abilitare sms gateway da interfaccia grafica, mentre da ubuntu andare sul file di configurazione e settare l'endpoint e pwd corretti per l'SMS Gateway. Per tutte queste configurazioni vedere i file doc appena citati. Se invece si vuole installare un SMS Gateway, nella stessa folder è presente la guida all'utilizzo e configurazione:

- Manuale SMS Machine HTTP-email.pdf

## 12. Maven Nexus (opzionale – solo per lo sviluppo)

**Descrizione servizio:** Macchina dedicata SOLO per lo sviluppo – Caricamento jar library

**Nome macchina (suggerito):** pr01maven01

**Flavor:** 2 CPU - 4 RAM - 40 GB disk

**O.S + tool base:** Ubuntu server 14.04

**Security Group:** di seguito l'elenco dei Security Group da associare alla VM:

zabbix\_agent

ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet  
ALLOW IPv4 10050/tcp from Orchestrator/subnet

nexus-maven-secgroup

ALLOW IPv6 to ::/0  
ALLOW IPv4 8081/tcp from 0.0.0.0/0  
ALLOW IPv4 22/tcp from 0.0.0.0/0  
ALLOW IPv4 to 0.0.0.0/0

Aggiungere http secgroup, e la porta 8081 per i servizi di nexus

**Guida all'installazione dei servizi:** per installare un repository Sonatype Nexus seguire il manuale di installazione che si trova nella seguente folder:

*CONFIGURAZIONI → Nexus-Maven → doc: Tutorial installing Nexus on Ubuntu*

I jar file da inserire per ejbca sono nella folder

*CONFIGURAZIONI → CaaS-Ejbca → file it.zip*

Da caricare sul repository come Artifact con la seguente nomenclatura come definito in tabella

### **EJBCA jar file per la PaaS**

| Path to jar file - Artifact  | Versione | Jar file             |
|------------------------------|----------|----------------------|
| it.prisma.ejbca.cert-cvc     | 1.0      | cert-cvc-1.0.jar     |
| it.prisma.ejbca.ejbca-util   | 1.0      | ejbca-util-1.0.jar   |
| it.prisma.ejbca.ejbca-ws     | 1.0      | ejbca-ws-1.0.jar     |
| it.prisma.ejbca.ejbca-ws-cli | 3.0      | ejbca-ws-cli-3.0.jar |

<https://books.sonatype.com/nexus-book/reference/using-sect-uploading.html>