

Manuale di Installazione e Gestione (MIG)

*Sistema di gestione delle segnalazioni di condotte illecite
(c.d. Whistleblowing 2 Livello)*

Release 1.1.0



1.1

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	1 di 20

Indice

1	DEFINIZIONI, ACRONIMI E RIFERIMENTI	4
1.1	DATI DEL DOCUMENTO	4
1.2	DEFINIZIONI E ACRONIMI	5
1.3	CONVENZIONI DI CARATTERE GENERALE	6
1.4	RIFERIMENTI INTERNI	6
1.5	RIFERIMENTI ESTERNI	7
1.6	INDICE DELLE FIGURE	7
2	OBIETTIVO E CONTENUTI DEL DOCUMENTO	8
2.1	OBIETTIVO DEL DOCUMENTO	8
2.2	CONTENUTI DEL DOCUMENTO	8
3	DESCRIZIONE DEL SERVIZIO	9
4	ARCHITETTURA, CONFIGURAZIONE E DEPLOYMENT	9
4.1	ARCHITETTURA	9
4.2	DISTRIBUZIONE DEGLI ITEM SULLE RISORSE FISICHE	10
5	CONTENUTI DEL SET UP	10
5.1	SOFTWARE	10
6	SOFTWARE TERZE PARTI, PIATTAFORME E FRAMEWORK UTILIZZATI	11
7	PROCEDURE DI INSTALLAZIONE, AGGIORNAMENTO E DISINSTALLAZIONE	11
7.1	PREREQUISITI	11
7.2	PREDISPOSIZIONE DEL SISTEMA	12
7.2.1	GLOBALEAKS	12

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	2 di 20

7.2.2	TOR2WEB.....	14
7.2.3	POSTGRESQL SERVER	15
7.2.4	BASE DATI.....	16
7.3	CONFIGURAZIONI PROPEDEUTICHE ALL'INSTALLAZIONE.....	17
7.3.1	UTENTI NECESSARI ALL'INSTALLAZIONE	17
7.4	AGGIORNAMENTI SUCCESSIVI	17
7.5	POST INSTALLAZIONE	17
7.5.1	TEST DELL'INSTALLAZIONE.....	17
7.5.2	PATCHING	18
8	DISINSTALLAZIONE	18
9	PROCEDURE DI MANUTENZIONE E GESTIONE	18
10	LOG FILE	18
11	UTENTI E POLICY.....	19
12	SLA HELPDESK.....	19

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	3 di 20

1 Definizioni, acronimi e riferimenti

1.1 Dati del documento

Codice del Progetto/Servizio	Specificare il codice del Progetto/Servizio		
Versione documento	1.0	Versione template	1.2
Ufficio Committente	UVIF	Referente/i committente	Dott.ssa Maria Grassini
Data creazione documento	23 ottobre 2017	Data ultimo aggiornamento	23 ottobre 2017

ANAC		FORNITORE	
Ufficio responsabile del Progetto	Dott. Michele Pizziconi	Società	Laser Romae S.r.l.
		Referente/i	Ing. Emiliano Fedeli

Ver.	Elabora	Verifica	Approva	Data emissione	Descrizione delle modifiche
1.0	Fabio D'Andria	Emiliano Fedeli	Michele Pizziconi	23/10/2017	Prima emissione del documento
1.1	Fabio D'Andria	Emiliano Fedeli	Michele Pizziconi	15/12/2017	Migrazione S.O. RHEL 7.x Revisione generale

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	4 di 20

1.2 Definizioni e acronimi

La presenza nel documento dell'abbreviazione **[tbd]** (to be defined) indica una parte per la quale non si hanno elementi sufficienti per procedere ad una completa definizione; come tale sarà subordinata ad un'ulteriore definizione in una successiva versione del documento.

La presenza nel documento dell'abbreviazione **[tbc]** (to be confirmed) indica una parte per la quale sono stati assunti elementi che debbono essere confermati; come tale sarà subordinata ad una conferma in fase successiva.

La presenza nel documento dell'abbreviazione **[na]** (non applicabile) indica che un argomento previsto nello standard di struttura di questo documento, risulta privo di significato nel contesto di questo sistema.

AVCP	<i>Autorità per la Vigilanza Contratti Pubblici</i> <i>Organo collegiale che vigila sul rispetto delle regole che disciplinano la materia dei contratti pubblici, dotata di indipendenza funzionale, di giudizio, di valutazione e di autonomia organizzativa.</i>
ANAC	<i>Autorità Nazionale Anticorruzione</i>
Autorità	<i>Si riferisce all'ANAC</i>
UAFI	<i>Ufficio Analisi Flussi Informativi</i>
UPSI	<i>Ufficio Progettazione e sviluppo, Servizi Informatici e Gestione del Portale dell'ANAC.</i>
UESI	<i>Ufficio Esercizio Sistemi</i>
BDNCP	<i>Banca Dati Nazionale dei Contratti Pubblici</i> <i>Anagrafe unica dei contratti pubblici. È la banca dati di riferimento di ANAC per utenze e soggetti rappresentati.</i>

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	5 di 20

Portale Internet	<i>Portale Internet</i> <i>Punto di erogazione dei servizi web per gli utenti esterni ANAC</i>
Servizi ANAC	<i>Servizi ANAC</i> <i>Nucleo centralizzato di servizi che contengono la logica di Business dell'Autorità.</i>

Tabella 1 - Definizioni e acronimi

1.3 Convenzioni di carattere generale

Di seguito sono elencate le convenzioni per l'identificazione degli elementi presenti all'interno del documento e dove:

- **nnn** è un progressivo numerico.
- **{short_desc}** è una descrizione breve

Identificativo	Descrizione
RIF. {short_desc}.nnn	<i>Identificativo univoco di un riferimento dove {short_desc} è una descrizione breve e nnn è un progressivo numerico</i>
REQ.{short_desc}.nnn	<i>Identificativo univoco di un requisito dove {short_desc} è una descrizione breve e nnn è un progressivo numerico</i>

Tabella 2 – Convenzioni di carattere generale

1.4 Riferimenti interni

Codice riferimento	Descrizione del documento	Versione	Codice del documento
--------------------	---------------------------	----------	----------------------

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	6 di 20

RIF.DOCINT.001	<i>Linee guida tecniche per lo sviluppo dei Servizi dell'ANAC</i>	2.0	<i>Servizi-A.N.A.C.-LGT</i>
RIF.DOCINT.002	<i>Stack Tecnologico – Sistema di gestione delle segnalazioni di condotte illecite</i>	1.0	<i>OpenWB-stackTecnologico</i>
RIF.DOCINT.003	<i>Requisiti Utente – Sistema di gestione delle segnalazioni di condotte illecite</i>	1.0	

Tabella 3 - Riferimenti interni

1.5 Riferimenti esterni

Codice riferimento	Codice	Descrizione
RIF.EXT.001		

Tabella 4 - Riferimenti esterni

1.6 Indice delle figure

<i>Figura 1 – Architettura Logica.....</i>	<i>9</i>
<i>Figura 2 – Architettura Fisica.....</i>	<i>10</i>
<i>Figura 3 – Diagramma di Deployment.....</i>	<i>10</i>
<i>Figura 4 - Prerequisiti fisici.....</i>	<i>12</i>

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	7 di 20

2 Obiettivo e contenuti del documento

2.1 Obiettivo del documento

Questo documento si pone l'obiettivo di descrivere dettagliatamente le procedure di installazione e gestione necessarie a fornire tutte le informazioni necessarie all'esercizio del sistema di gestione delle segnalazioni di condotte illecite (c.d. Whistleblowing 2 Livello)

2.2 Contenuti del documento

Il presente documento è suddiviso essenzialmente nelle seguenti sezioni:

- Definizioni, acronimi e riferimenti (capitolo 1)
- Obiettivo e contenuti del documento (capitolo 2): in cui è riportata una descrizione dell'ambito del documento, dei suoi contenuti e di eventuali acronimi utilizzati
- Descrizione del servizio (capitolo 3)
- Architettura: sezione contenente i diagrammi relativi all'architettura logica e al le componenti coinvolte nel deployment dell'applicazione in termini di item e di risorse interessate e delle loro configurazioni (capitolo 4)
- Contenuti del set up: le risorse necessarie per l'installazione del servizio (capitolo 5)
- Software di terze parti, piattaforme e framework utilizzati (capitolo 6)
- Procedure di Installazione: in questa sezione vengono descritte le procedure di installazione per i diversi ambienti (capitolo 7)
- Procedura di Disinstallazione (capitolo 8)
- Procedure di manutenzione e gestione: in questa sezione vengono descritte le procedure di gestione dell'applicativo/servizio (capitolo 9)
- Vengono descritti i file di log, la loro configurazione e i messaggi di errore o di informazioni in essi presenti (capitolo 10)
- Vengono descritti utenti e policy necessari alla gestione dell'applicazione (capitolo 11)
- Vengono descritti gli SLA dell'applicazione (capitolo 12)

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	8 di 20

3 Descrizione del Servizio

Il Sistema di gestione delle segnalazioni di condotte illecite di 2 livello dell'Autorità Nazionale Anticorruzione è un'applicazione Software che consente ad un dipendente di una Pubblica Amministrazione di redigere ed inviare una segnalazione di condotta illecita avvenuta all'interno del proprio Ente/Amministrazione/Società a partecipazione pubblica all'Autorità Nazionale Anticorruzione (c.d. Whistleblowing 2 livello).

4 Architettura, configurazione e deployment

<Indicare l'architettura logica a componenti e il diagramma della stessa e relativa descrizione. Individuare tutte le componenti, anche esterne all'applicazione stessa, coinvolte nell'installazione, configurazione e quindi deployment dell'applicazione in termini di item e di risorse interessate.>

4.1 Architettura

L'architettura del sistema di gestione delle segnalazioni di condotte illecite (c.d. Whistleblowing) è di tipo **multi-tier**, un'architettura software in cui le varie funzionalità del Software sono logicamente separate ovvero suddivise su più strati o livelli differenti in comunicazione tra loro (presentazione, elaborazione e persistenza).

Ciascuno strato è in comunicazione diretta con quelli adiacenti ovvero richiede ed offre servizi allo strato adiacente (Client-Server).

In figura 1 è riportata la rappresentazione dell'architettura logica:

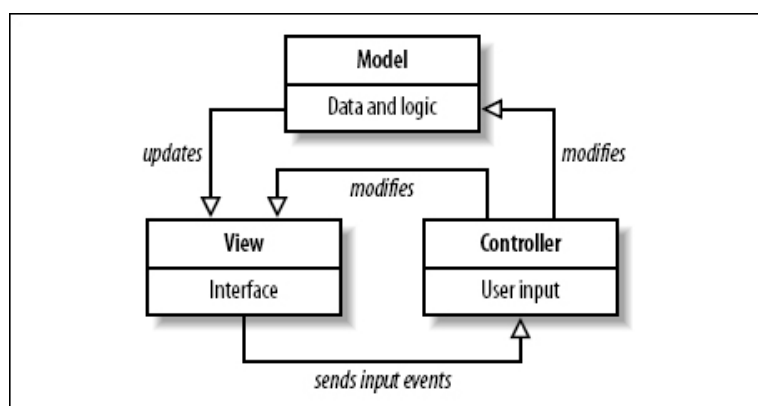


Figura 1 – Architettura Logica

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	9 di 20

In figura 2 è riportata la rappresentazione dell'architettura fisica:

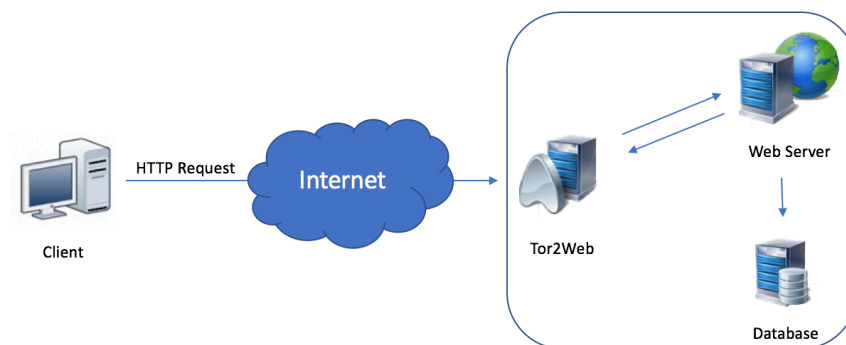


Figura 2 – Architettura Fisica

4.2 Distribuzione degli item sulle risorse fisiche

In figura 3 è riportato il diagramma di distribuzione delle componenti dell'applicazione sulle risorse fisiche coinvolte.

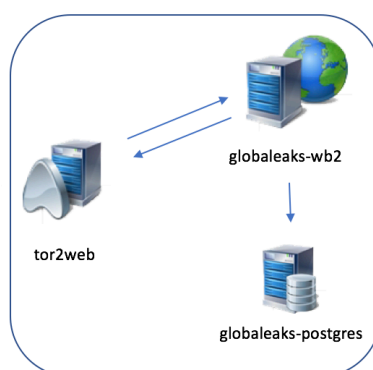


Figura 3 – Diagramma di Deployment

5 Contenuti del set up

5.1 Software

In questa sezione viene riportata la lista degli oggetti software facenti parte della distribuzione software fornita per il Sistema di Whistleblowing di 2 livello:

- globaleaks-wb2-1.0.0-1.x86_64.rpm
- globaleaks-postgres-1.0.30-1.x86_64.rpm

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	10 di 20

- tor2web-1.0.0-1.x86_64.rpm

6 Software terze parti, piattaforme e framework UTILIZZATI

In questa sezione vengono elencate tutti i Software di terze parti, piattaforme software e framework, ivi compresi quelli di sviluppo, impiegati nello sviluppo e nella realizzazione dell'applicazione:

- Linguaggi di sviluppo Front End: Javascript, Angular JS, Bootstrap;
- Linguaggi di sviluppo Back End: Python
- Framework applicativi: Tor2web;
- Framework di accesso a DB: Twisted;
- Application server: Apache
- DBMS: PostgreSQL

7 Procedure di installazione, aggiornamento e disinstallazione

In questa sezione vengono descritte le procedure di installazione del Sistema di Whistleblowing di 2 Livello.

7.1 Prerequisiti

I seguenti prerequisiti Hardware e Software sono preliminari all'installazione del Sistema di Whistleblowing di 2 Livello su piattaforma RedHat 7.x. Per ognuno dei ruoli specifici di ogni server (globaleaks-wb2, tor2web e postgresql server) verrà specificata la lista di prerequisiti software.

Fisici:

In Tabella sono riportate i requisiti fisici in termini di RAM, n. e caratteristiche CPU, numero di dischi con spazio disco disponibile su ciascun disco ivi compresi mount point esterni, n. e caratteristiche schede di rete di ciascun nodo elaborativo previsto:

Nome macchina	Descrizione macchina	CPU	RAM	Dischi	Schede Rete
Globaleaks	Web Server	4 Core	32 GB	200 GB con lvm	1

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	11 di 20

Tor2web	Tor2Web Server	2 Core	8 GB	100 GB con lvm	1
Globaleaks-Postgres	DBMS Server	4 Core	32 GB	200 GB con lvm	1

Figura 4 - Prerequisiti fisici

SO: Sono riportate di seguito le caratteristiche del sistema operativo comprensivo di versione e patch per ciascun nodo elaborativo:

- **Globaleaks:** Red Hat Enterprise Linux Server 7.x
- **Tor2web:** Red Hat Enterprise Linux Server 7.x
- **Globaleaks-Postgres:** Red Hat Enterprise Linux Server 7.x

Middleware: [na]

Data base: Sono riportate di seguito le caratteristiche del DBMS, versione, comprensiva di patch, per ogni DB previsto:

- **Globaleaks-Postgres:** PostgreSQL 9.6.5

7.2 Predisposizione del sistema

In questa sezione sono elencate le operazioni necessarie all'installazione e configurazione delle componenti della pila software utilizzata dal Sistema di Whistleblowing di 2 Livello.

Ogni sistema dovrà essere già predisposto nella configurazione di rete necessaria, con le regole del firewall e di sicurezza già attive (sottosistemi sshd, iptables).

7.2.1 Globaleaks

SO - versione

Red Hat Enterprise Linux Server 7.x

SO - installazione

installazione tipica

SO – configurazione

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	12 di 20

La configurazione necessaria per il sistema operativo prevede la disabilitazione di SELinux e l'installazione dei prerequisiti.

Per disabilitare SELinux modificare il file `/etc/selinux.config` in questo modo:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Installare quindi i prerequisiti con i seguenti comandi:

```
yum -y clean all && yum -y update
yum -y install https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-
11.noarch.rpm
curl -O https://download.postgresql.org/pub/repos/yum/9.6/redhat/rhel-7-x86\_64/pgdg-
redhat96-9.6-3.noarch.rpm
yum -y install ./pgdg-redhat96-9.6-3.noarch.rpm
yum -y install postgresql96-devel
yum -y remove redhat-lsb-*
yum -y install gcc-c++
```

Componente SW 1 – versione

`globaleaks-wb2-1.0.0-1.x86_64.rpm`

Componente SW 1 – installazione

`yum -y install <globaleaks package location>`

Componente SW 1 – configurazione

La configurazione del pacchetto è subordinata alla corretta installazione e configurazione del Server 3 (database PostgreSQL). I passi da eseguire saranno relativi alla configurazione del server di posta in uscita (se presente), degli indirizzi IP autorizzati per il server globaleaks e dall'indirizzo IP del server database:

- modificare il file `/etc/default/globaleaks` per i seguenti parametri (in nero sono evidenziati gli IP e hostname utilizzati sulla piattaforma di sviluppo):

```
HOSTS_LIST=127.0.0.1,localhost,192.168.0.59,84.253.188.101,gleaks-portal-dev.laserromae.it
ALLOWED_SRC_IP=( 127.0.0.1 0.0.0.0 )
ALLOWED_DST_IP=( 127.0.0.1 192.168.0.59 )
```

- se necessario disabilitare l'invio della mail:

```
DISABLE_MAIL_NOTIFICATION=1
```

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	13 di 20

- oppure configurare i parametri del server di posta dalla pagina <base_url>/#/admin/mail
- modificare la linea relativa al tipo di database
(/usr/local/globaleaks/usr/lib/python2.7/dist-packages/globaleaks/settings.py riga 83 (di seguito la configurazione utilizzata nella piattaforma di sviluppo):

```
self.db_type = 'postgres'
```

- modificare la linea relativa alla stringa di connessione al database
(/usr/local/globaleaks/usr/lib/python2.7/dist-packages/globaleaks/settings.py 249 (di seguito la configurazione utilizzata nella piattaforma di sviluppo):

```
self.db_uri = 'postgres://gleaks:gl811ks!@192.168.0.61/gleaks'
```

- far partire il servizio con il comando
service globaleaks start

7.2.2 tor2web

SO - versione

Red Hat Enterprise Linux Server 7.x

SO - installazione

installazione tipica

SO – configurazione

La configurazione necessaria per il sistema operativo comprende la disabilitazione di SELinux e l'installazione dei prerequisiti.

Per disabilitare SELinux modificare il file /etc/selinux.config in questo modo:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Installare quindi i prerequisiti con i seguenti comandi:

```
yum -y clean all && yum -y update
yum -y install https://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	14 di 20

```
subscription-manager repos --enable rhel-6-server-optional-rpms  
yum-config-manager --enable rhui-REGION-rhel-server-rhscs  
yum -y install gcc-c++
```

Componente SW 1 – versione

tor2web-1.0.0-1.x86_64.rpm

Componente SW 1 – installazione

```
yum -y install <tor2web package location>
```

Componente SW 1 – configurazione

La configurazione del pacchetto è subordinata alla corretta installazione e configurazione del Server 1 (server globaleaks). I passi da eseguire saranno relativi alla configurazione dell'IP del server 1 e dell'eventuale proxy HTTP/s:

- modificare l'ultima riga del file /etc/tor2web.conf indicando l'indirizzo IP del server 1

```
# This allows Tor2web to make use a simple TCP proxies  
dummyproxy = http://192.168.0.59:80
```

- modificare il file /etc/tor/torrc (se necessario), per indicare l'indirizzo del web proxy:

```
HTTPProxy 192.168.3.254:8080  
HTTPSProxy 192.168.3.254:8080
```

- copiare il certificato server, chiave e file intermedi nella directory /home/tor2web/certs
- in alternativa, creare dei certificati self-signed, con i seguenti comandi:

```
cd /home/tor2web/certs/  
openssl genrsa -out tor2web-key.pem 4096  
openssl req -new -key tor2web-key.pem -out tor2web-csr.pem
```

- modificare il file /etc/tor2web.conf aggiungendo le seguenti righe:

```
ssl_key = <percorso del file certificate>  
ssl_cert = <percorso del file chiave>  
ssl_intermediate = <percorso del file intermedio>
```

- riavviare il servizio

```
service tor2web restart
```

7.2.3 PostgreSQL server

SO - versione

Red Hat Enterprise Linux Server 7.x

SO - installazione

installazione tipica

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	15 di 20

SO – configurazione

La configurazione necessaria per il sistema operativo comprende la disabilitazione di SELinux e l'installazione dei prerequisiti.

Per disabilitare SELinux modificare il file `/etc/selinux.config` in questo modo:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#   targeted - Targeted processes are protected,
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Installare quindi i prerequisiti con i seguenti comandi:

```
yum -y clean all && yum -y update
yum -y install https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-
11.noarch.rpm
curl -O https://download.postgresql.org/pub/repos/yum/9.6/redhat/rhel-7-x86\_64/pgdg-
redhat96-9.6-3.noarch.rpm
yum -y install ./pgdg-redhat96-9.6-3.noarch.rpm
```

Componente SW 1 – installazione

```
yum -y install <globaleaks-postgres> location
```

Componente SW 1 – configurazione

La configurazione del pacchetto è relativa alla configurazione dell'IP del server 1 fra gli host autorizzati nel database PostgreSQL:

- modificare il file `/var/lib/pgsql/9.6/data/pg_hba.conf` nella riga del database `gleaks`, inserendo l'IP del server1 (in nero l'IP utilizzato sulla piattaforma di sviluppo):

```
host      all                                gleaks      192.168.0.59/32      md5
```

- riavviare il servizio

```
service postgresql-9.6 restart
```

7.2.4 Base Dati

Le basi di dati presenti nel sistema differiscono a seconda che si tratti di WB di 1 livello (che utilizza un database sqlite3) o WB di 2 livello (Postgresql server 9.6.5.). La creazione degli schema e

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	16 di 20

delle tabelle é la medesima ed è completamente automatizzata nei rispettivi pacchetti di installazione.

7.3 Configurazioni propedeutiche all'installazione

7.3.1 Utenti necessari all'installazione

L'installazione dei pacchetti rpm deve essere eseguita dall'utente root, ovvero da un utente della macchina che abbia la possibilità di lanciare i comandi descritti nei paragrafi precedenti utilizzando i privilegi di sudo.

7.4 Aggiornamenti successivi

I successivi rilasci verranno effettuati sempre con pacchetti rpm. Gli stessi internamente prevederanno differenti azioni a seconda si tratti di prima installazione o upgrade. Nessuna ulteriore azione sarà necessaria lato utente per l'installazione, se non l'utilizzo del package manager yum.

7.5 Post installazione

La post installazione non prevede nessuna azione particolare, la procedura prevista per ogni pacchetto contiene già gli step necessari alla configurazione e all'avvio del servizio.

7.5.1 Test dell'installazione

Riportare la procedura idonea fornire a un sistemista senza conoscenze specifiche del prodotto di verificarne la corretta installazione.

La verifica dell'installazione consiste nel controllo che l'rpm sia installato correttamente e che il servizio sia presente tra i processi attivi. Ad esempio per il pacchetto globaleaks-wb2:

```
# rpm -qa | grep globaleaks-wb2
globaleaks-wb2-1.0.0-1.x86_64

# ps -aux | grep globaleaks
501      63  0.2  2.9 270192 60976 ?        Sl    00:53   0:00 /usr/bin/python
/usr/bin/globaleaks --ip=127.0.0.1,172.17.0.2 --port=80 --accept-
host=127.0.0.1,localhost,172.17.0.2 --user=globaleaks --group=globaleaks --working-
path=/var/globaleaks/ --ramdisk=/dev/shm/globaleaks/ --tor-dir=/var/globaleaks/torhs/ --
loglevel=CRITICAL --disable-mail-notification
```

Inoltre é possibile verificare la versione installata, controllando il valore presente nella homepage in basso (e.g. OpenWhistleBlowing v1.0.0)

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	17 di 20

7.5.2 Patching

L'aggiornamento delle componenti per nuove release, migrazioni, patching, scalabilità e procedure di gestione devono essere progettate in modo da minimizzare il disservizio agli utenti nella fruizione del servizio ed effettuabili, per quanto più possibile, anche in orario lavorativo.

Ogni MEV, Hotfix, Bug riscontrato che neccisiti di immediato rilascio verrà gestito con rilascio di release minore e relativa nota.

8 Disinstallazione

La procedura di disinstallazione prevede essenzialmente lo shutdown del servizio e la successiva rimozione del pacchetto. Ad esempio per il pacchetto globaleaks-wb2:

```
# service globaleaks stop
# mv /usr/bin/python.old /usr/bin/python
# yum remove globaleaks-wb2
```

9 Procedure di manutenzione e gestione

Tutti i servizi vengono gestiti tramite init-scripts di sistema. Per questo è possibile gestire ogni componente mediante il paradigma:

service <nome servizio> <azione>

dove nome servizio rappresenta uno di:

- globaleaks-wb1
- globaleaks-wb2
- postgresql-9.5
- tor2web

mentre l'azione è rappresentata da

- start
- stop

I servizi sono stati configurati per partire automaticamente al boot del sistema (runlevel 2, 3, 4, 5).

10 Log file

I file di log sono presenti nella directory /var/globaleaks/log e nella directory dell'utente postgres

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	18 di 20

per il relativo pacchetto. Sono log gestiti con rotazione. Di seguito si riporta come esempio, il listato della directory per il pacchetto globaleaks-wb2:

```
# ll /var/globaleaks/log/
total 10236
-rwx----- 1 globaleaks globaleaks 445483 Dec 7 00:58 globaleaks.log
-rwx----- 1 globaleaks globaleaks 1000069 Oct 19 2016 globaleaks.log.1
-rwx----- 1 globaleaks globaleaks 1000138 Dec 23 2015 globaleaks.log.10
-rwx----- 1 globaleaks globaleaks 1000053 Apr 7 2016 globaleaks.log.2
-rwx----- 1 globaleaks globaleaks 1000059 Jan 5 2016 globaleaks.log.3
-rwx----- 1 globaleaks globaleaks 1000019 Jan 5 2016 globaleaks.log.4
-rwx----- 1 globaleaks globaleaks 1000028 Jan 5 2016 globaleaks.log.5
-rwx----- 1 globaleaks globaleaks 1000131 Jan 5 2016 globaleaks.log.6
-rwx----- 1 globaleaks globaleaks 1000088 Jan 5 2016 globaleaks.log.7
-rwx----- 1 globaleaks globaleaks 1000064 Jan 5 2016 globaleaks.log.8
-rwx----- 1 globaleaks globaleaks 1000096 Jan 4 2016 globaleaks.log.9
```

11 Utenti e Policy

Durante il processo di installazione, ogni pacchetto crea gli utenti necessari per l'esecuzione del servizio. Di seguito l'elenco degli utenti creati e relative caratteristiche:

Pacchetto	Utente	Gruppo	Home directory
globaleaks-wb1	debian-tor	debian-tor	/var/lib/tor
globaleaks-wb1	globaleaks	debian-tor	/var/globaleaks
globaleaks-wb2	debian-tor	debian-tor	/var/lib/tor
globaleaks-wb2	globaleaks	debian-tor	/var/globaleaks
tor2web	tor2web	tor2web	/home/tor2web
globaleaks-postgres	postgres	postgres	/var/lib/pgsql

12 SLA Helpdesk

In tabella sono riportati i valori dei livelli di qualità e di servizio.

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	19 di 20

Tipologia	Indicatore	Livello di Servizio
Disponibilità del Servizio di Whistleblowing di 1 e 2 livello agli Utenti	% Uptime servizio	> 99 %
Tempestività di assegnazione e notifica all'utente di ricezione della richiesta di intervento (tempo massimo di notifica) (SUP)	Ricezione richiesta/chiamata	< 1 H lavorativa nel 97% dei casi < 2 H lavorativa nel restante 3% dei casi
Efficacia nella risoluzione degli Incident alla prima linea (SUP)	% Incident chiusi dalla prima linea	> 30% dei casi risolti senza fare ricorso ai servizi di secondo livello
Tempestività di analisi dei Problem (MAC)	Inizio chiamata / chiusura intervento	4 ore lavorative nel 90% dei casi
Tempestività di completamento dei Change Standard/Predefiniti (MEV)	Inizio chiamata / chiusura intervento	8 ore lavorative nel 90% dei casi

Codice documento	Versione documento	Stato	Classificazione	Pagina
[ANAC_MIG_A01.S04.I01]	1.1 del 15.12.2017	Finale	Uso Interno	20 di 20