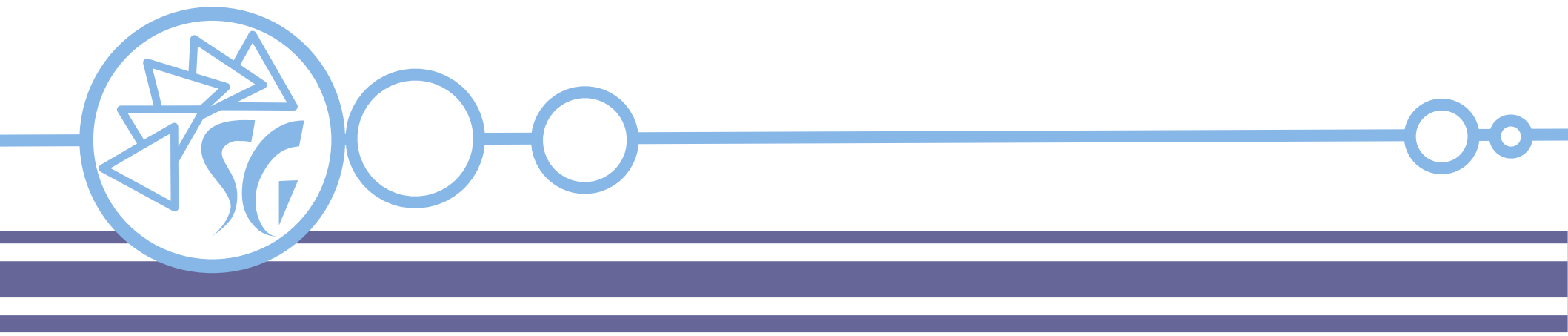
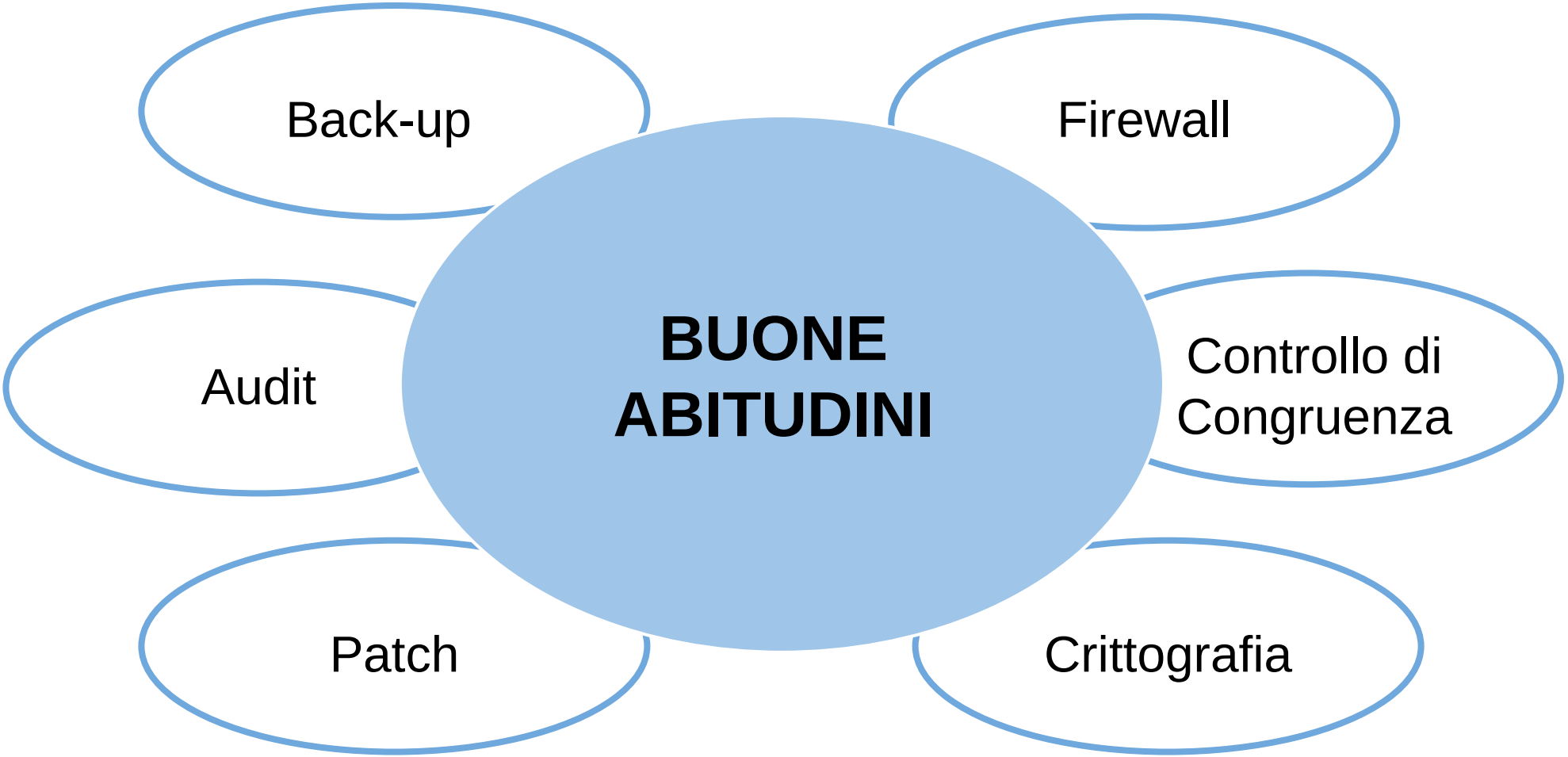


Linux
Introduzione a SELinux

Ing. Simone Giustetti

www.giustetti.net

Cosa è la Sicurezza Informatica



Cosa è SELinux

SELinux è l'acronimo di **S**ecurity **E**nhanced **Linux**.

Un sistema di controllo degli accessi implementato a basso livello tramite **patch** per il kernel.

Segue una filosofia dei minori privilegi possibili:

- Nega automaticamente l'accesso alle risorse;
- Applica alcune eccezioni basandosi su politiche centralizzate.

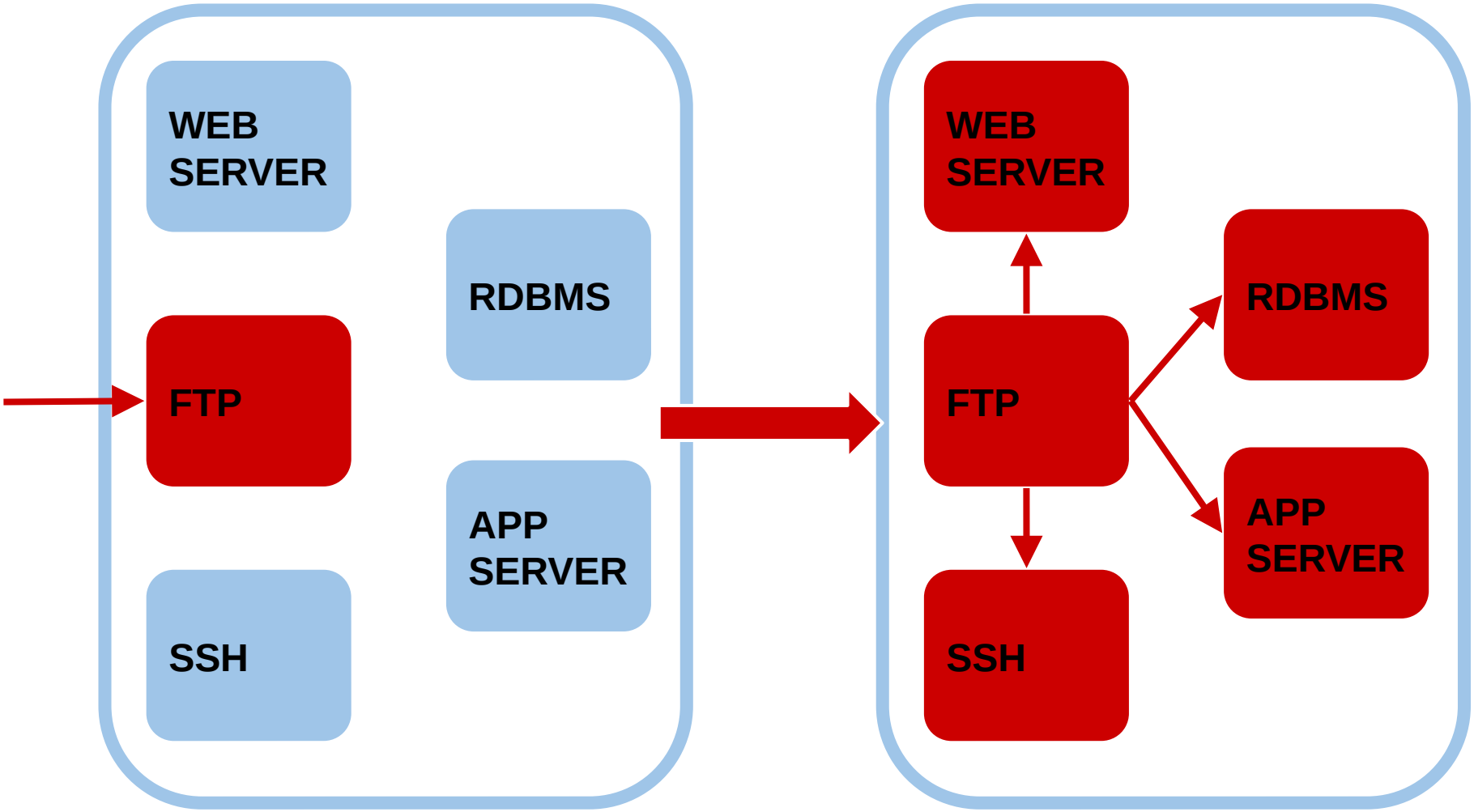
Controllo degli Accessi

SELinux non è un sistema di autenticazione.

SELinux non interviene direttamente sui permessi di file e risorse.

Il fine di SELinux è evitare che un processo o un utente compromesso infettino l'intero sistema.

Escalation dei Privilegi



Conseguenze di un Attacco Riuscito

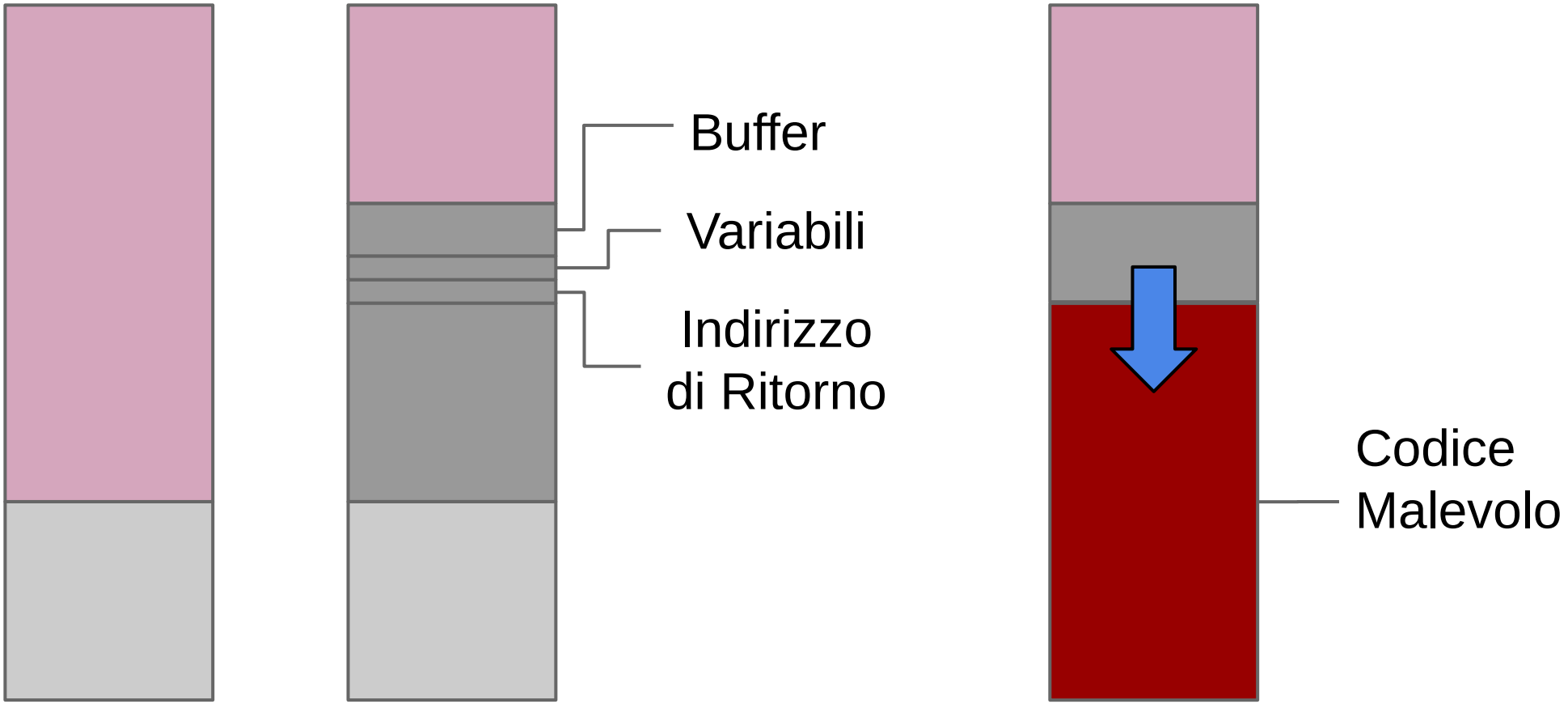
Un sistema compromesso può essere impiegato per arrecare danni o commettere attività illegali:

- Attacchi DOS o DDOS;
- Furto di dati;
- Furto di identità;
- Pirateria informatica;
- Invio di Spam.
- ...

Problemi Difficilmente Arginabili

Stack

Buffer Overflow Remoto



Soluzioni Potenziali

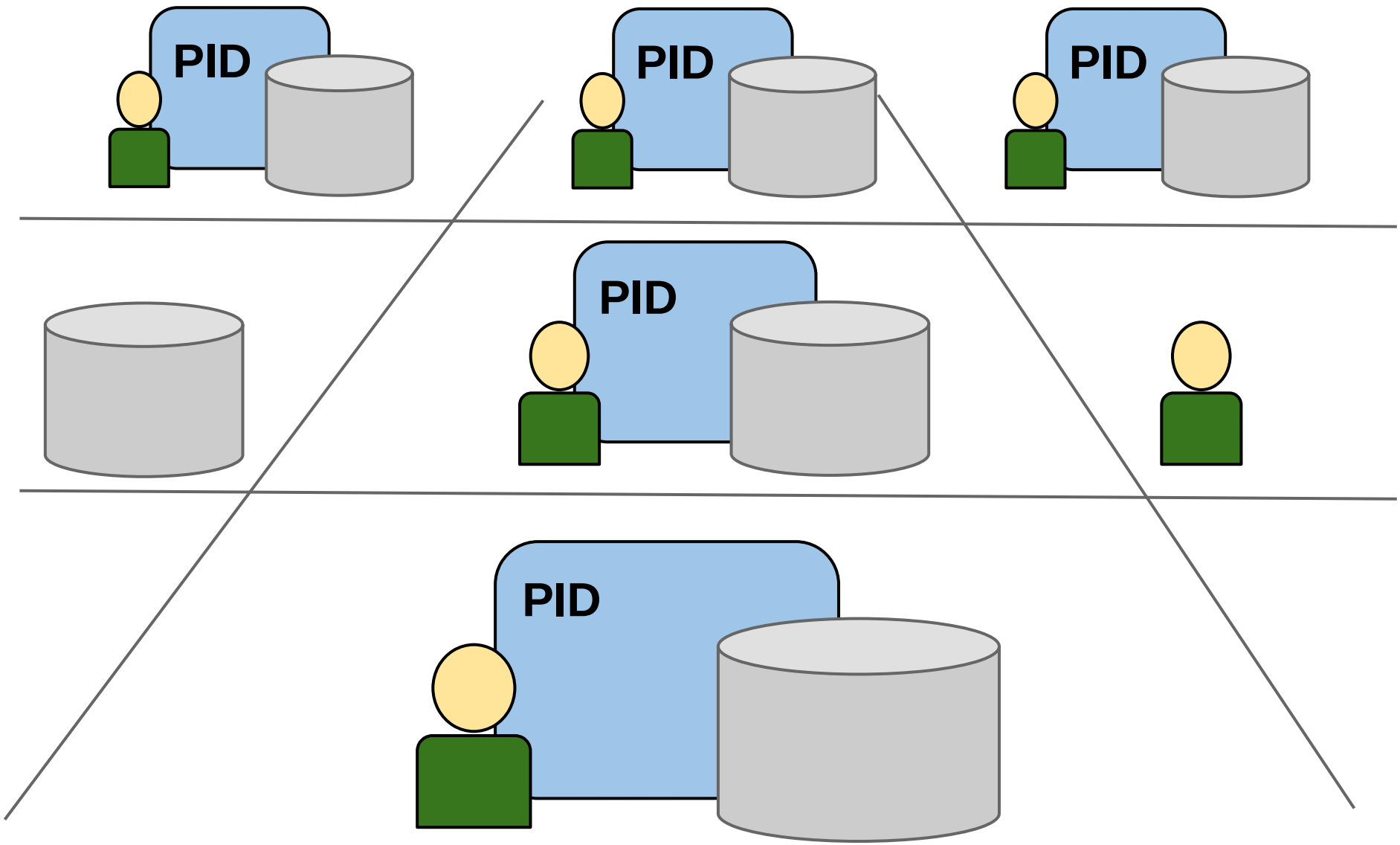
Soluzioni a posteriori

- Documentazione;
- Applicazione di Patch.

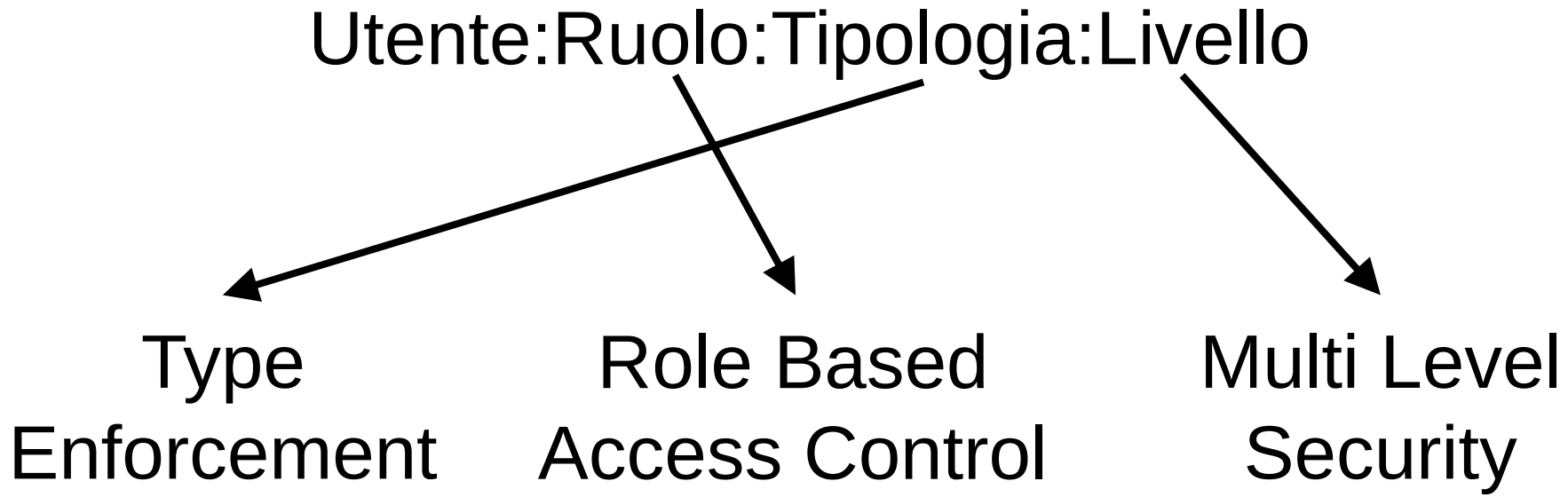
Soluzioni proattive

- Rimuovere tutto il software non utilizzato;
- Riscrivere il software utilizzando apposite librerie orientate alla sicurezza;
- Patch exec-shield per il Kernel Linux;
- SELinux => Contestualizzare processi e risorse.

Confinamento

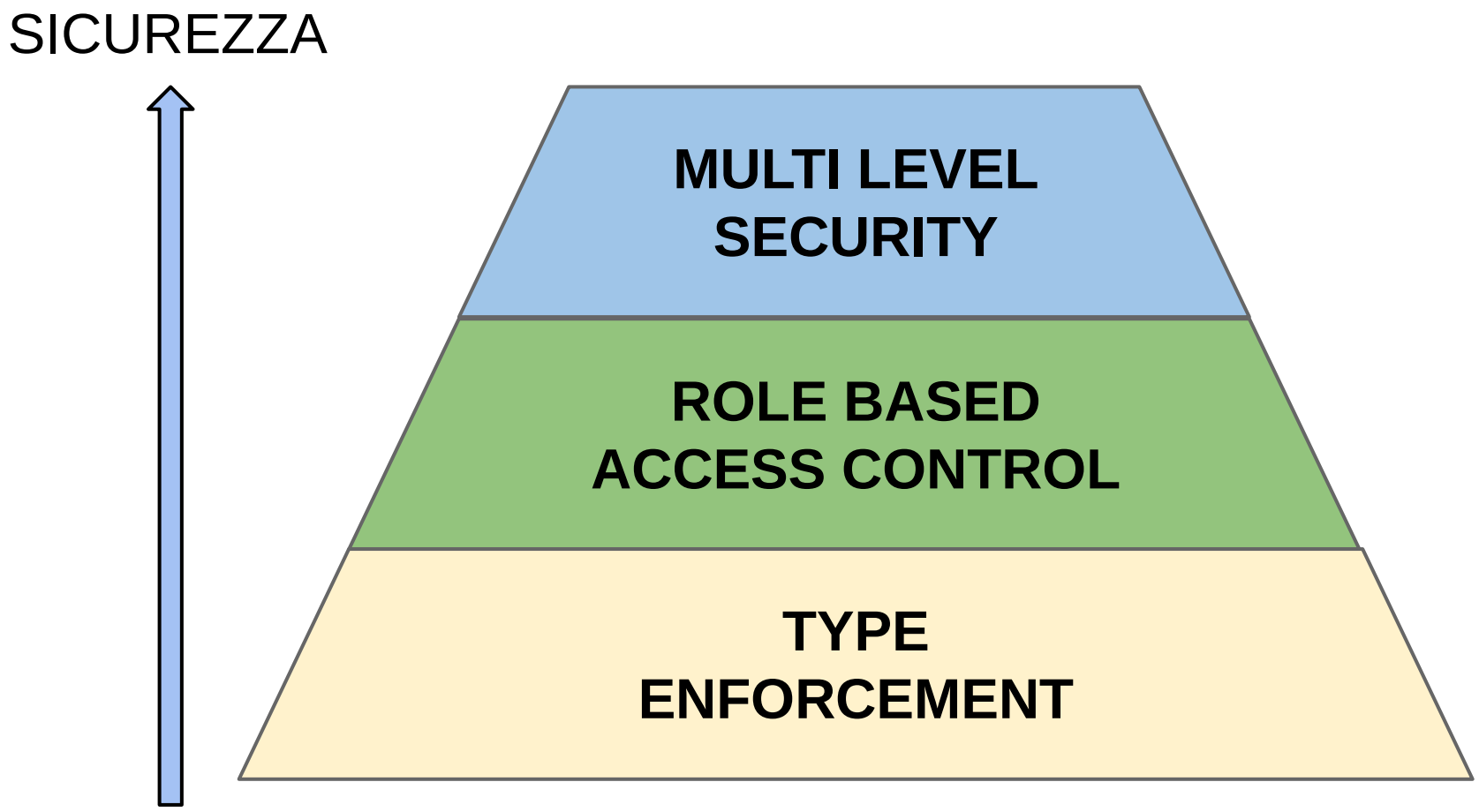


SELinux: Contesto



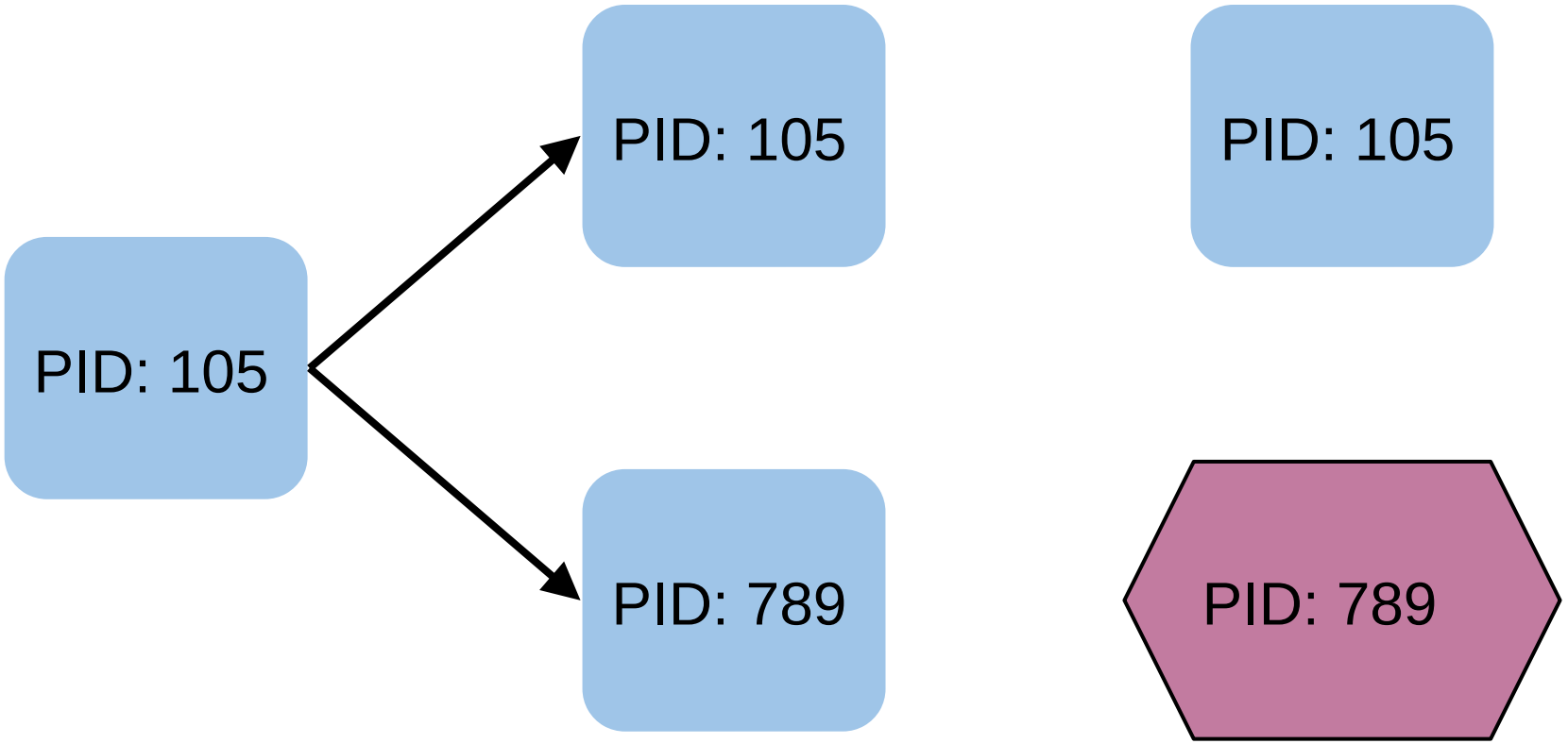
- Risorsa: **ls** *-Z*
- Processo: **ps** *-Z*
- Assegnazione: **chcon**

SELinux: Forme di Accesso alle Risorse



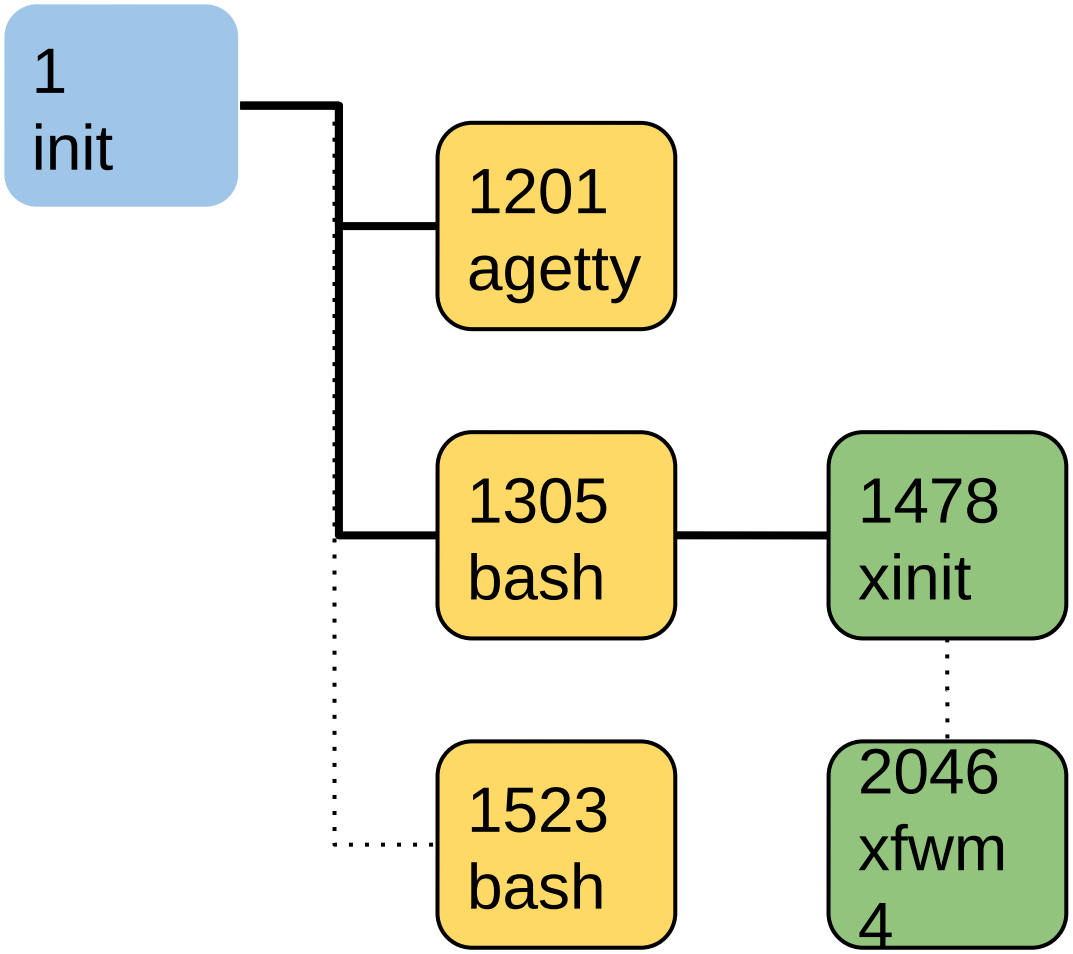
Assegnazione Automatica del Contesto

I processi nascono per scissione (Fork)



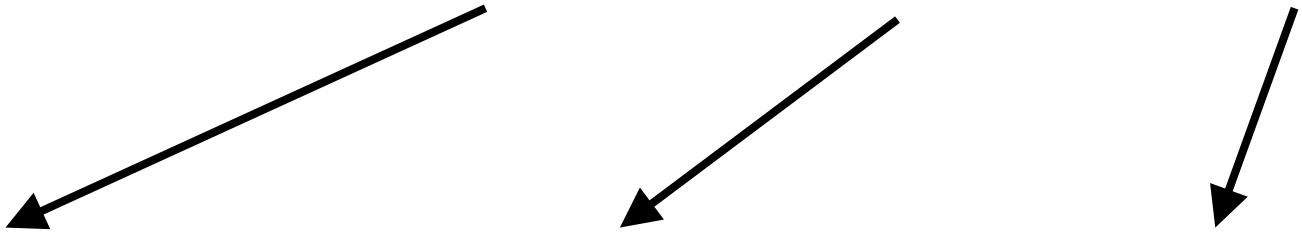
Assegnazione Automatica del Contesto

Il contesto dei processi è applicato alla nascita



Regole di Transizione

domain_auto_trans(initrc_t, named_exec, namedrc_t)



Contesto del processo padre

Chiamata di sistema

Contesto del processo figlio

SELinux: Politiche Predefinite

- **Targeted**: Solo alcuni demoni / servizi sono soggetti al controllo;
- **Strict**: Tutti i demoni / servizi hanno un proprio contesto delimitato (Non supportata);
- **MLS**: Un novero scelto di demoni / servizi forniti di un proprio cotesto delimitato.

SELinux: Modalità d’Uso

- **Disabled**: Nessuna limitazione;
- **Permissive**: Tiene traccia di tutti gli eventi nei file di registro (log), ma non impone limitazioni (Utile per configurare un sistema);
- **Enforcing**: Attivo.

Impostare la Modalità d'Uso

La modalità predefinita deve essere impostata nel file */etc/selinux/config*.

La modalità attiva può essere visualizzata mediante il comando **sestatus**.

Il comando **setenforce** attiva la modalià **enforcing**.

Abilitare i Servizi

La configurazione dei servizi può essere interrogata mediante il comando **getsebool**.

I singoli servizi e le rispettive funzionalità possono essere abilitati / disabilitati mediante il comando **setsebool**.

Integrazione con i Comandi Standard

cp: Assegna il contesto della directory di destinazione.
cp -Z <contesto>: Impone un nuovo contesto alla copia.

mv: Mantiene il contesto di origine.

tar: Non mantiene traccia dei contesti.
star: Versione modificata di tar in grado di memorizzare le informazioni inerenti i contesti.

Pacchetti Relativi a SELinux

Produzione	Sviluppo	Opzionali
selinux-policy	policycoreutils	mcstrans
selinux-policy-targeted	policycoreutils-gui	
libselinux	selinux-policy-mls	
libselinux-python	setools-lib	
libselinux-utils	setools-console	
	setools-gui	
	setroubleshoot-server	

Informazioni & Licenze