Oracle® Solaris 11 Security Guidelines

N. di parte: E25816–03
Marzo 2012

ORACLE

120424@25097

Indice

Prefazione

Questo documento presenta le linee guida di sicurezza per Sistema operativo Oracle Solaris (SO Oracle Solaris). Innanzitutto, la guida descrive i problemi di sicurezza che il sistema operativo di una azienda deve affrontare. Quindi, mostra le funzioni di sicurezza predefinite del SO Oracle Solaris. Infine, la guida indica i passaggi specifici da eseguire per rendere il sistema più sicuro e per usufruire delle funzioni di sicurezza di Oracle Solaris a protezione di dati e applicazioni. È possibile adattare le raccomandazioni riportate in questa guida ai criteri di sicurezza dei singoli siti.

Audience

Il documento *Oracle Solaris 11 Security Guidelines* è destinato agli amministratori della sicurezza e ad altri amministratori incaricati delle seguenti operazioni:

- Analisi dei requisiti di sicurezza
- Implementazione dei criteri di sicurezza all'interno di software
- Installazione e configurazione del SO Oracle Solaris
- Mantenimento della sicurezza di sistema e di rete

Per utilizzare questa guida è necessario disporre di competenze generiche in merito all'amministrazione UNIX, di una buona base in sicurezza dei software e delle conoscenze necessarie relative ai criteri di sicurezza del proprio sito.

Accesso al supporto Oracle

I clienti Oracle hanno accesso al supporto elettronico tramite My Oracle Support. Per ulteriori informazioni, visitare il sito `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oppure l'indirizzo `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` per utenti con problemi di udito.

Convenzioni tipografiche

La tabella seguente descrive le convenzioni tipografiche usate nel manuale.

TABELLA P–1 Convenzioni tipografiche

Carattere tipografico	Descrizione	Esempio
`AaBbCc123`	Nomi di comandi, file e directory; messaggi di sistema sullo schermo	Aprire il file `.login`. Usare `ls -a` per visualizzare l'elenco dei file. `sistema% Nuovi messaggi.`
`AaBbCc123`	Comandi digitati dall'utente, in contrasto con l'output del sistema sullo schermo	`sistema%` **`su`** `Password:`
aabbcc123	Segnaposto: da sostituire con nomi o valori reali	Per rimuovere un file, digitare `rm` *nomefile*.
AaBbCc123	Titoli di manuali, termini citati per la prima volta, parole particolarmente importanti nel contesto	Vedere il Capitolo 6 del *Manuale dell'utente*. La *cache* è una copia memorizzata localmente. *Non* salvare il file. **Nota:** alcuni termini compaiono in grassetto nella visualizzazione in linea

Prompt della shell negli esempi di comando

Nella tabella seguente sono riportati i prompt predefiniti UNIX di sistema e superutente per le shell incluse nel sistema operativo Oracle Solaris. Il prompt di sistema predefinito visualizzato negli esempi di comandi varia a seconda della release di Oracle Solaris.

TABELLA P–2 Prompt della shell

Shell	Prompt
Shell Bash, shell Korn e shell Bourne	`$`
Shell Bash, shell Korn e shell Bourne per superutenti	`#`
C shell	`nome_sistema%`
C shell, superutente	`nome_sistema#`

◆ ◆ ◆ CAPITOLO 1

1 Panoramica della sicurezza di Oracle Solaris 11

Oracle Solaris 11 è un sistema operativo aziendale valido e di qualità, in grado di offrire funzioni di sicurezza affidabili. Grazie al sofisticato sistema di sicurezza a livello di rete che consente di controllare modalità di accesso ai file da parte degli utenti, tipo di protezione dei database di sistema utilizzo delle risorse, Oracle Solaris 11 è in grado di soddisfare esigenze di sicurezza di qualsiasi tipo. Mentre i sistemi operativi tradizionali possono presentare punti deboli nella protezione, la flessibilità di Oracle Solaris 11 consente di soddisfare una grande varietà di requisiti di sicurezza, dai server aziendali ai client per desktop. Oracle Solaris 11 è completamente testato e compatibile con svariati sistemi SPARC e basati su x86, di Oracle nonché su altre piattaforme di fornitori terzi.

Protezioni di sicurezza di Oracle Solaris 11

Oracle Solaris costituisce una solida base per dati e applicazioni aziendali e protegge i dati sia sul disco sia in transito. Oracle Solaris Resource Manager, denominato da qui in seguito *sistema di gestione delle risorse*, e Oracle Solaris Zones offrono funzioni che consentono di separare le applicazioni e proteggerle da un utilizzo improprio. Questo limite, insieme al privilegio minimo implementato tramite i privilegi stessi e la funzione RBAC (role-based access control) di Oracle Solaris, consente di ridurre il rischio di sicurezza per intrusione o operazioni improprie di utenti regolari. Protocolli autenticati e cifrati, quali IP security (IPsec), consentono la creazione di reti virtuali private (VPN) su Internet, nonché di tunnel nella LAN o WAN per la distribuzione sicura dei dati. Inoltre, la funzione di auditing di Oracle Solaris consente la conservazione di record delle attività più importanti.

I servizi di sicurezza di Oracle Solaris 11 offrono livelli di protezione del sistema e della rete avanzati Oracle Solaris protegge il kernel limitando, nell'ambito delle utilità stesse del kernel, le

azioni con privilegi che l'utilità può eseguire. La configurazione di rete predefinita garantisce la protezioni dei dati nel sistema e in tutta la rete. IPsec, la funzione di filtro IP di Oracle Solaris, e Kerberos possono assicurare ulteriore protezione.

I servizi di sicurezza di Oracle Solaris includono:

- La protezione del kernel: daemon e dispositivi del kernel sono protetti da autorizzazioni dei file e privilegi.
- Login protetti: l'esecuzione del login richiede l'inserimento di password. Le password sono caratterizzate da una cifratura complessa. L'esecuzione di login in remoto è inizialmente limitata a un canale cifrato e autenticato tramite la funzione Secure Shell di Oracle Solaris. L'account `root` non può eseguire direttamente il login.
- Protezione dei dati: i dati sul disco vengono protetti dalle autorizzazioni del file. È possibile configurare ulteriori livelli di protezione. Ad esempio, è possibile utilizzare le ACL (access control list), collocare i dati in una zona, cifrare un file, cifrare un set di dati ZFS di Oracle Solaris, creare un set di dati ZFS di sola lettura e attivare file system in modo che i programmi `setuid` e i file eseguibili non possano essere avviati.

Tecnologie di sicurezza di Oracle Solaris 11

Le funzioni di sicurezza di Oracle Solaris possono essere configurate per implementare i criteri di sicurezza del sito.

Le sezioni seguenti forniscono una breve introduzione alle funzioni di sicurezza di Oracle Solaris. Le descrizioni contengono riferimenti a spiegazioni più dettagliate e a procedure riportate nella presente guida e in altre guide di amministrazione del sistema Oracle Solaris che mostrano le funzioni in oggetto.

Servizio di audit

Per auditing si intende la raccolta di dati relativi all'uso delle risorse di sistema. I dati di audit forniscono un record di eventi di sistema relativi alla sicurezza. Questi dati possono essere utilizzati per determinare la responsabilità di azioni registrate in un sistema.

L'auditing è un requisito di base per gli organismi di valutazione, convalida e certificazione della sicurezza. L'auditing può costituire inoltre un deterrente per potenziali intrusioni.

Per maggiori informazioni, vedere:

- Per un elenco di pagine man relative agli audit, vedere Capitolo 29, “Auditing (Reference)” in *Oracle Solaris Administration: Security Services*.
- Per linee guida, vedere “Audit di eventi rilevanti oltre a Login/Logout” a pagina 33 e le pagine man.

- Per una panoramica sull'auditing, vedere Capitolo 26, "Auditing (Overview)" in *Oracle Solaris Administration: Security Services*.
- Per attività di auditing, vedere Capitolo 28, "Managing Auditing (Tasks)" in *Oracle Solaris Administration: Security Services*.

BART (Basic Audit Reporting Tool)

La funzione BART (Basic Audit Reporting Tool) di Oracle Solaris consente di convalidare in modo completo i sistemi eseguendo verifiche a livello del file nel tempo. Creando file manifesto BART, è possibile raccogliere in modo facile e affidabile informazioni sui componenti dello stack del software installato nei sistemi implementati.

BART è uno strumento utile per la gestione dell'integrità su un sistema o su una rete di sistemi.

Per maggiori informazioni, vedere:

- Le pagine man selezionate includono `bart`(1M), `bart_rules`(4) e `bart_manifest`(4).
- Per le linee guida, vedere "Creazione di un'istantanea BART del sistema" a pagina 47, "Utilizzo dello strumento BART (Basic Audit Reporting Tool)" a pagina 51 e le pagine man.
- Per una panoramica di BART, vedere Capitolo 6, "Verifying File Integrity by Using BART" in *Oracle Solaris Administration: Security Services*.
- Per esempi relativi all'utilizzo dei file BART, vedere "Using BART (Tasks)" in *Oracle Solaris Administration: Security Services* e le pagine man.

Servizi di cifratura

La funzione relativa al framework di cifratura di Oracle Solaris e la funzione KMF (Key Management Framework) di Oracle Solaris forniscono repository centrali per servizi di cifratura e gestione delle chiavi. Gli utenti di hardware e software e gli utenti finali hanno accesso diretto ad algoritmi ottimizzati. I meccanismi di archiviazione, utilità amministrative e interfacce di programmazione per le diverse infrastrutture PKI possono utilizzare un'interfaccia unificata quando adottano interfacce KMF.

Il framework di cifratura assicura servizi di cifratura a utenti e applicazioni tramite comandi individuali, un'interfaccia di programmazione a livello dell'utente e un'interfaccia di programmazione del kernel, nonché framework a livello del kernel e dell'utente. Il framework di cifratura fornisce i relativi servizi ad applicazioni e moduli kernel in maniera trasparente all'utente. Inoltre, fornisce all'utente finale servizi di cifratura diretti come la cifratura e la decifratura dei file.

KMF fornisce strumenti e interfacce di programmazione per gestire in modo centralizzato oggetti della chiave pubblica, quali certificati X.509 e coppie di chiavi pubblica/privata. I formati

di archiviazione di questi oggetti possono variare. KMF fornisce inoltre uno strumento di gestione dei criteri che definisce l'utilizzo dei certificati X.509 da parte delle applicazioni. KMF supporta plugin di terze parti.

Per maggiori informazioni, vedere:

- La pagine man selezionate includono `cryptoadm(1M)`, `encrypt(1)`, `mac(1)`, `pktool(1)` e `kmfcfg(1)`.
- Per una panoramica dei servizi di cifratura, vedere Capitolo 11, "Cryptographic Framework (Overview)" in *Oracle Solaris Administration: Security Services* e Capitolo 13, "Key Management Framework" in *Oracle Solaris Administration: Security Services*.
- Per esempi relativi all'utilizzo del framework di cifratura, vedere Capitolo 12, "Cryptographic Framework (Tasks)" in *Oracle Solaris Administration: Security Services* e le pagine man.

Autorizzazioni del file e voci di controllo dell'accesso

La prima linea di difesa per la protezione degli oggetti in un file system è rappresentata dalle autorizzazioni UNIX predefinite assegnate a ogni oggetto del file system. Le autorizzazioni UNIX supportano l'assegnazione dei diritti di accesso univoci al proprietario dell'oggetto, a un gruppo assegnato all'oggetto o a chiunque altro. Inoltre, ZFS supporta le ACL, denominate anche ACE (access control entries) che consentono di controllare in modo più preciso l'accesso a oggetti del file system individuali o di gruppo.

Per maggiori informazioni, vedere:

- Per istruzioni sull'impostazione delle ACL su file ZFS, vedere la pagina man `chmod(1)`.
- Per una panoramica delle autorizzazioni dei file, vedere "Using UNIX Permissions to Protect Files" in *Oracle Solaris Administration: Security Services* .
- Per una panoramica ed esempi di protezione dei file ZFS, vedere Capitolo 8, "Using ACLs and Attributes to Protect Oracle Solaris ZFS Files" in *Oracle Solaris Administration: ZFS File Systems* e le pagine man.

Filtro del pacchetto

Il filtro del pacchetto garantisce una protezione di base dagli attacchi di rete. Oracle Solaris include la funzione di filtraggio IP e wrapper TCP.

Filtro IP

La funzione di filtro IP di Oracle Solaris crea un firewall per respingere gli attacchi di rete.

In particolare, il filtro IP offre funzionalità di filtro del pacchetto con stato e consente di filtrare i pacchetti per indirizzo IP, rete, porta, protocollo, interfaccia di rete e direzione del traffico. Inoltre, presenta un filtro che intercetta i pacchetti senza stato e offre la capacità di creare e gestire pool di indirizzi. Il filtro IP ha poi la capacità di eseguire la traslazione degli indirizzi di rete (NAT) e delle porte (PAT).

Per maggiori informazioni, vedere:

- Le pagine man selezionate includono `ipfilter(5)`, `ipf(1M)`, `ipnat(1M)`, `svc.ipfd(1M)` e `ipf(4)`.
- Per una panoramica sul filtro IP, vedere Capitolo 20, "IP Filter in Oracle Solaris (Overview)" in *Oracle Solaris Administration: IP Services*.
- Per esempi sull'utilizzo del filtro IP, vedere Capitolo 21, "IP Filter (Tasks)" in *Oracle Solaris Administration: IP Services* e le pagine man.
- Per informazioni ed esempi sulla sintassi del linguaggio del criterio del filtro IP, vedere la pagina man `ipnat(4)`.

Wrapper TCP

I wrapper TCP consentono di controllare l'accesso verificando l'indirizzo di un host che richiede un determinato servizio di rete rispetto ad una ACL. Le richieste vengono accettate o respinte in base al risultato del controllo. I wrapper TCP registrano anche nel log le richieste degli host di servizi di rete e rappresentano un'utile funzione di monitoraggio. Le funzioni Secure Shell e `sendmail` di Oracle Solaris sono configurate per utilizzare wrapper TCP. Tra i servizi di rete che possono essere controllati vi sono `ftpd` e `rpcbind`.

I wrapper TCP supportano un linguaggio avanzato per il criterio di configurazione grazie al quale è possibile specificare un criterio di sicurezza non solo a livello globale, ma anche di tipo "per servizio". Un ulteriore accesso ai servizio può essere consentito o limitato in base al nome host, all'indirizzo IPv4 o IPv6, al nome netgroup, alla rete e persino al dominio DNS.

Per maggiori informazioni, vedere:

- Per informazioni sui wrapper TCP, vedere "How to Use TCP Wrappers to Control Access to TCP Services" in *Oracle Solaris Administration: IP Services* .
- Per informazioni ed esempi sulla sintassi relativa al linguaggio di controllo dell'accesso per wrapper TCP, vedere la pagina man `hosts_access`(4).

Password e limiti della password

Password utente sicure aiutano a difendersi da attacchi di tipo brute force o guessing.

Oracle Solaris dispone di un numero di funzioni che possono essere utilizzate per incrementare il livello di sicurezza delle password utente. È possibile impostare lunghezza della password,

contenuto, frequenza e requisiti della modifica. Inoltre, è possibile conservare una cronologia delle password. Viene altresì fornito un dizionario delle password da evitare. Sono disponibili molteplici algoritmi di password.

Per maggiori informazioni, vedere:

- "Maintaining Login Control" in *Oracle Solaris Administration: Security Services*
- "Securing Logins and Passwords (Tasks)" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `passwd(1)` e `crypt.conf(4)`.

Modulo di autenticazione collegabile (PAM, Pluggable Authentication Module)

Il framework relativo al modulo di autenticazione collegabile (PAM) consente di coordinare e configurare i requisiti di autenticazione dell'utente per account, credenziali, sessioni e password.

Il framework PAM consente alle organizzazioni di personalizzare l'esperienza di autenticazione dell'utente e le funzionalità di gestione di account, sessione e password. I servizi di ingresso nel sistema come `login` e `ftp` utilizzano il framework PAM per garantire che tutti i punti di ingresso del sistema siano stati protetti. L'architettura consente la sostituzione o la modifica dei moduli di autenticazione nel campo per proteggere il sistema da ogni nuovo punto debole rilevato senza rendere necessarie modifiche ai servizi di sistema che utilizzano il framework PAM.

Per maggiori informazioni, vedere:

- Capitolo 14, "Using PAM" in *Oracle Solaris Administration: Security Services*
- Pagina man `pam.conf(4)`

I privilegi in Oracle Solaris

I privilegi sono diritti discreti e specifici relativi a processi attivi nel kernel. Oracle Solaris definisce oltre 80 privilegi, da quelli di base come `file_read` a privilegi più specializzati quali `proc_clock_highres`. I privilegi possono essere assegnati a un comando, un utente, un ruolo o un sistema. Molti comandi e daemon di Oracle Solaris vengono eseguiti utilizzando solo i privilegi necessari per completare le rispettive attività. L'utilizzo di privilegi è anche denominato *gestione dei diritti del processo*.

I programmi dotati di privilegi possono evitare le intrusioni ottenendo più privilegi rispetto a quelli comunemente utilizzati. Inoltre, proprio grazie ai privilegi, le organizzazioni possono stabilire quali privilegi sono garantiti a servizi e processi in esecuzione nei sistemi.

Per maggiori informazioni, vedere:

- "Privileges (Overview)" in *Oracle Solaris Administration: Security Services*
- "Using Privileges (Tasks)" in *Oracle Solaris Administration: Security Services*
- Capitolo 2, "Developing Privileged Applications" in *Developer's Guide to Oracle Solaris 11 Security*
- Le pagine man selezionate includono `ppriv(1)` e `privileges(5)`.

Accesso remoto

Gli attacchi di accesso remoto possono danneggiare un sistema e una rete. La protezione dell'accesso di rete è necessaria nell'ambiente Internet moderno ed è utile anche in ambienti WAN e LAN.

IPsec e IKE

La sicurezza IP (IPsec) protegge i pacchetti IP autenticandoli e/o cifrandoli. Oracle Solaris supporta IPsec per IPv4 e IPv6. Poiché IPsec è implementato ben al di sotto del livello applicazione, le applicazioni Internet possono sfruttare IPsec senza richiedere modifiche del codice.

IPsec e il relativo protocollo di scambio della chiave (IKE) utilizza algoritmi dal framework di cifratura. Inoltre, il framework di cifratura fornisce un keystore softtoken alle applicazioni che utilizzano il metaslot. Quando il protocollo IKE è configurato per utilizzare il metaslot, le organizzazioni possono scegliere di memorizzare le chiavi nel disco, nel keystore dell'hardware o nel keystore del softtoken.

Se amministrato correttamente, IPsec è uno strumento utile per la protezione del traffico di rete.

Per maggiori informazioni, vedere:

- Capitolo 14, "IP Security Architecture (Overview)" in *Oracle Solaris Administration: IP Services*
- Capitolo 15, "Configuring IPsec (Tasks)" in *Oracle Solaris Administration: IP Services*
- Capitolo 17, "Internet Key Exchange (Overview)" in *Oracle Solaris Administration: IP Services*
- Capitolo 18, "Configuring IKE (Tasks)" in *Oracle Solaris Administration: IP Services*
- Le pagine man selezionate includono `ipsecconf(1M)` e `in.iked(1M)`.

Secure Shell

La funzione Secure Shell di Oracle Solaris consente a utenti o servizi di accedere o trasferire file tra sistemi remoti su un canale di comunicazione cifrato. In Secure Shell, tutto il traffico di rete è

cifrato. Secure Shell può essere utilizzato come rete privata virtuale (VPN) on-demand che può inoltrare il traffico di sistema X Window oppure connettere numeri di porta individuali tra un sistema locale e sistemi remoti tramite un collegamento di rete cifrato e autenticato.

Pertanto, Secure Shell impedisce a potenziali intrusi di leggere una comunicazione intercettata e previene lo spoofing del sistema da parte di terzi. Per impostazione predefinita, Secure Shell è l'unico meccanismo di accesso remoto attivo su un sistema appena installato.

Per maggiori informazioni, vedere:

- Capitolo 15, "Using Secure Shell" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `ssh(1)`, `sshd(1M)`, `sshd_config(4)`, e `ssh_config(4)`.

Servizio Kerberos

La funzione Kerberos di Oracle Solaris attiva un accesso di tipo SSO (single sign-on) e protegge le transazioni anche su reti eterogenee che eseguono il servizio Kerberos.

Kerberos è basato sul protocollo di autenticazione della rete Kerberos V5 sviluppato dal Massachusetts Institute of Technology (MIT) Il servizio Kerberos è un'architettura client-server che consente di effettuare transazioni di rete sicure. Il servizio offre una solida autenticazione utente nonché integrità e privacy. Utilizzando il servizio Kerberos è possibile eseguire il login una volta sola e accedere ad altri sistemi, eseguire i comandi, scambiare i dati e trasferire i file in modo sicuro. Inoltre, il servizio consente agli amministratori di limitare l'accesso ai servizi e ai sistemi.

Per maggiori informazioni, vedere:

- Parte VI, "Kerberos Service" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `kerberos(5)` e `kinit(1)`.

Controllo dell'accesso basato su ruolo (RBAC, Role-Based Access Control)

RBAC applica il principio di sicurezza del privilegio minimo consentendo alle organizzazioni di garantire in modo selettivo i diritti amministrativi a utenti o ruoli in base alle esigenze e ai requisiti specifici.

La funzione RBAC di Oracle Solaris consente di controllare l'accesso utente per quelle attività che sarebbero normalmente riservate al ruolo `root`. Applicando gli attributi di sicurezza ai processi e agli utenti, la funzione RBAC distribuisce i diritti amministrativi tra più amministratori. La funzione RBAC è denominata anche *gestione dei diritti utente*.

Per maggiori informazioni, vedere:

- Parte III, "Roles, Rights Profiles, and Privileges" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `rbac(5)`, `roleadd(1M)`, `profiles(1)`, e `user_attr(4)`.

Service Management Facility

La funzione Service Management Facility (SMF) di Oracle Solaris viene utilizzata per aggiungere, rimuovere, configurare e gestire i servizi. La funzione SMF utilizza la funzione RBAC per controllare l'accesso alle funzioni di gestione del servizio nel sistema. In particolare, la funzione SMF utilizza le autorizzazioni per determinare chi può gestire un servizio e quali funzioni possono essere eseguite dall'utente.

La funzione SMF consente di controllare l'accesso ai servizi e di verificare in che modo tali servizi vengono avviati, arrestati e aggiornati.

Per maggiori informazioni, vedere:

- Capitolo 6, "Managing Services (Overview)" in *Oracle Solaris Administration: Common Tasks*
- Capitolo 7, "Managing Services (Tasks)" in *Oracle Solaris Administration: Common Tasks*
- Le pagine man selezionate includono `svcadm(1M)`, `svcs(1)` e `smf(5)`.

File system ZFS di Oracle Solaris

ZFS è il file system predefinito per Oracle Solaris 11. Il file system ZFS modifica in modo radicale l'amministrazione dei file system da parte di Oracle Solaris. ZFS è solido, scalabile e facile da amministrare. Poiché la creazione del file system in ZFS è leggera, è possibile stabilire facilmente quote e spazio riservato. Le autorizzazioni UNIX e ACE proteggono i file, mentre RBAC supporta l'amministrazione delegata dei set di dati ZFS.

Per maggiori informazioni, vedere:

- Capitolo 1, "Oracle Solaris ZFS File System (Introduction)" in *Oracle Solaris Administration: ZFS File Systems*
- Capitolo 3, "Oracle Solaris ZFS and Traditional File System Differences" in *Oracle Solaris Administration: ZFS File Systems*
- Capitolo 6, "Managing Oracle Solaris ZFS File Systems" in *Oracle Solaris Administration: ZFS File Systems*
- Le pagine man selezionate includono `zfs(1M)` e `zfs(7FS)`.

Oracle Solaris Zones

La tecnologia di partizionamento software Oracle Solaris Zones consente di mantenere il modello di implementazione "un'applicazione per server" condividendo simultaneamente le risorse hardware.

Zones fornisce ambienti operativi virtualizzati che consentono a più applicazioni di essere eseguite in modo isolato l'una dall'altra sullo stesso hardware fisico. Tale isolamento impedisce ai processi che vengono eseguiti in una zona di monitorare o influenzare i processi in esecuzione in altre zone, visualizzare gli altri dati o manipolare l'hardware sottostante. Zones, inoltre, fornisce un livello di astrazione che separa le applicazioni dagli attributi fisici del sistema su cui vengono implementati, come, ad esempio, percorsi del dispositivo fisico e nome dell'interfaccia di rete.

Per maggiori informazioni, vedere:

- Parte II, "Oracle Solaris Zones" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Le pagine man includono `brands(5)`, `zoneadm(1M)` e `zonecfg(1M)`.

Trusted Extensions

La funzione Trusted Extensions di Oracle Solaris costituisce un livello attivabile in via opzionale con tecnologia di labeling che consente di separare i criteri di sicurezza dei dati dalla proprietà dei dati stessi. Trusted Extensions supporta criteri di controllo dell'accesso di tipo discrezionale (DAC) e tradizionale in base alla proprietà, nonché criteri MAC (Mandatory Access Control) basati sull'etichetta. Se il livello Trusted Extensions non è attivo, tutte le etichette risultano uguali e il kernel non è configurato per applicare i criteri MAC. Quando i criteri MAC basati su etichetta sono attivi, tutti i flussi di dati sono limitati in base al confronto delle etichette associate ai processi (soggetti) che richiedono l'accesso e agli oggetti che contengono i dati. Diversamente dalla maggior parte degli altri sistemi operativi multilivello, Trusted Extensions include un desktop multilivello.

La funzione Trusted Extensions soddisfa i requisiti Common Criteria Labeled Security Protection Profile (LSPP), Role-Based Access Protection Profile (RBACPP) e Controlled Access Protection Profile (CAPP). Tuttavia, l'implementazione della funzione Trusted Extensions si differenzia per la sua capacità di garantire la massima affidabilità ottimizzando la compatibilità e riducendo l'overhead.

Per maggiori informazioni, vedere:

- Per informazioni sulla configurazione e la manutenzione di Trusted Extensions, vedere *Trusted Extensions Configuration and Administration* .
- Per informazioni sull'utilizzo del desktop multilivello, vedere *Trusted Extensions User's Guide* .

- Le pagine man selezionate includono `trusted_extensions(5)` e `labeld(1M)`.

Impostazioni predefinite di sicurezza di Oracle Solaris 11

Dopo l'installazione, Oracle Solaris protegge il sistema dalle intrusioni e, tra le altre funzioni di sicurezza, esegue il monitoraggio dei tentativi di login.

Accesso al sistema limitato e monitorato

Account dell'utente iniziale e del ruolo `root` : l'account dell'utente iniziale può eseguire il login dalla console. L'account viene assegnato al ruolo `root`. La password per i due account è inizialmente identica.

- Dopo aver eseguito il login, l'utente iniziale può assumere il ruolo `root` per configurare ulteriormente il sistema. Dopo aver assunto il ruolo, all'utente viene richiesto di modificare la password `root`. Tenere presente che nessun ruolo può eseguire il login direttamente, incluso il ruolo `root`.
- L'utente iniziale è assegnato per impostazione predefinita dal file `/etc/security/policy.conf`. Le impostazioni predefinite includono il profilo relativo ai diritti di base per l'utente Solaris (Basic Solaris User) e relativo all'utente della console (Console User). Questi profili di diritti consentono agli utenti di leggere e scrivere un CD o DVD, eseguire ogni comando nel sistema senza privilegi e arrestare e riavviare il sistema dalla console.
- Anche all'account dell'utente iniziale è assegnato il profilo dei diritti di amministratore di sistema. Pertanto, senza assumere il ruolo `root` l'utente iniziale dispone di alcuni diritti di amministrazione quali il diritto di installare software e gestire il servizio di denominazione.

Requisiti della password: le password utente devono essere composte da almeno sei caratteri e devono contenere almeno un carattere alfabetico e uno numerico. Viene eseguito l'hashing delle password mediante l'algoritmo `SHA256` . Alla modifica delle password, tutti gli utenti, inclusi quelli con ruolo `root`, dovranno conformarsi ai requisiti richiesti.

Accesso di rete limitato: dopo l'installazione, il sistema è protetto dalle intrusioni di rete. Il login remoto eseguito dall'utente iniziale è consentito su una connessione cifrata e autenticata mediante protocollo `ssh`. Questo è l'unico protocollo di rete che accetta pacchetti in ingresso. Il wrapping della chiave `ssh` viene eseguito mediante l'algoritmo `AES128`. Con cifratura e autenticazione attive, l'utente può raggiungere il sistema senza intercessioni, modifiche o spoofing.

Tentativi di login registrati: il servizio di audit è attivo per tutti gli eventi `login/logout` (login, logout, passaggio di utente, avvio e arresto di una sessione `ssh` e blocco dello schermo) e per tutti i login (non riusciti) non attribuibili. Poiché il ruolo `root` non può eseguire il login, il nome

dell'utente che utilizza il ruolo `root` può essere tracciato nell'audit trail. L'utente iniziale può rivedere i log di audit grazie a un diritto garantito tramite il profilo di diritti di amministratore di sistema (System Administrator).

Attivazione di protezioni per kernel, file, e desktop

Dopo l'esecuzione del login da parte dell'utente iniziale, kernel, file system e applicazioni desktop sono protetti da privilegi, autorizzazioni e controlli dell'accesso basati su ruolo (RBAC) minimi.

Protezioni del kernel: a molti daemon e comandi amministrativi vengono assegnati solo privilegi che ne consentono una corretta esecuzione. Molti daemon vengono eseguiti da account amministrativi speciali che non dispongono di privilegi `root` (`UID=0`), per evitare l'hijack ed eseguire altre attività. Tali account amministrativi speciali non possono effettuare il login. I dispositivi non sono protetti da privilegi.

File system: per impostazione predefinita, tutti i file system sono di tipo ZFS. Il valore `umask` dell'utente è `022`, pertanto quando un utente crea un nuovo file o directory sarà il solo a disporre delle autorizzazioni per modificarli. I membri di un gruppo utente possono leggere e ricercare la directory, nonché leggere il file. I login che avvengono all'esterno di un gruppo utente possono elencare la directory e leggere il file. Le autorizzazioni della directory sono `drwxr-xr-x` (`755`). Le autorizzazioni del file sono `-rw-r--r--` (`644`).

Applet desktop: gli applet desktop sono protetti da RBAC. Ad esempio, solo l'utente iniziale o il ruolo `root` possono utilizzare l'applet del Package Manager per installare nuovi pacchetti. Package Manager non viene visualizzato da utenti regolari che non dispongono dei relativi diritti.

Ulteriori funzioni di sicurezza attive

Oracle Solaris 11 garantisce funzioni di sicurezza che possono essere utilizzate per configurare sistemi e utenti e soddisfare così i requisiti di sicurezza del sito.

- **Role-based access control (RBAC)**: Oracle Solaris fornisce una serie di autorizzazioni, privilegi e profili di diritti. `root` è l'unico ruolo definito. I profili di diritti assicurano una buona base per i ruoli creati. Inoltre, alcuni comandi amministrativi richiedono autorizzazioni RBAC per riuscire correttamente. Gli utenti senza autorizzazioni non possono eseguire i comandi anche se dispongono dei privilegi necessari.
- **Diritti utente**: agli utenti viene assegnato un set di privilegi di base, di profili di diritti e di autorizzazioni definito nel file `/etc/security/policy.conf` proprio come avviene per l'utente iniziale, in base a quanto descritto nella sezione "Accesso al sistema limitato e monitorato" a pagina 19. I tentativi di login dell'utente non sono limitati, ma tutti i login non riusciti vengono registrati dal servizio di audit.

- **Protezione del file di sistema**: i file di sistema sono protetti da autorizzazioni del file. Solo il ruolo `root` ha la possibilità di modificare i file di configurazione del sistema.

Criteri e procedure di sicurezza del sito

Per un sistema sicuro o una rete di sistemi, il sito deve avere un criterio di sicurezza attivo con pratiche di sicurezza a supporto del criterio stesso.

Per maggiori informazioni, vedere:

- Appendice A, "Site Security Policy" in *Trusted Extensions Configuration and Administration*
- "Security Requirements Enforcement" in *Trusted Extensions Configuration and Administration*
- Manutenzione della sicurezza del codice (`http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do`)

◆ ◆ ◆ CAPITOLO 2

Configurazione della sicurezza di Oracle Solaris 11

Questo capitolo descrive la procedura da seguire per configurare la sicurezza del sistema. Il capitolo fa riferimento ai pacchetti di installazione e alla configurazione del sistema stesso, di vari sistemi secondari, nonché di ulteriori applicazioni che potrebbero essere necessarie, come ad esempio IPsec.

Installazione del SO Oracle Solaris

Quando si esegue l'installazione del SO Oracle Solaris, scegliere il supporto che consente di installare il pacchetto *group* appropriato:

- **Oracle Solaris Large Server** – Il file manifesto predefinito in un'installazione di Automated Installer (AI) e il programma di installazione in modalità testo consentono di installare il gruppo `group/system/solaris-large-server`, che fornisce un ambiente idoneo a Oracle Solaris Large Server.
- **Oracle Solaris Desktop**: Live Media consente di installare il gruppo `group/system/solaris-desktop` che offre un ambiente desktop di Oracle Solaris 11.

  Per creare un sistema desktop per l'utilizzo centralizzato, aggiungere il gruppo `group/feature/multi-user-desktop` a un server Oracle Solaris. Per ulteriori informazioni, vedere l'articolo Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment .

Per l'installazione automatica mediante Automated Installer (AI), vedere Parte III, "Installing Using an Install Server" in *Installing Oracle Solaris 11 Systems*.

Per operare la scelta più appropriata, consultare le seguenti linee guida per l'installazione:

- *Installing Oracle Solaris 11 Systems*
- *Creating a Custom Oracle Solaris 11 Installation Image*
- *Adding and Updating Oracle Solaris 11 Software Packages*

Sicurezza del sistema

È consigliabile eseguire le seguenti attività nell'ordine indicato. Al termine della procedura, il sistema operativo Oracle Solaris 11 è installato e solo l'utente iniziale che può assumere il ruolo `root` potrà accedervi.

Attività	Descrizione	Per istruzioni
1. Verificare i pacchetti nel sistema.	Assicurarsi che i pacchetti del supporto di installazione siano identici ai pacchetti installati.	"Verifica dei pacchetti" a pagina 25
2. Salvaguardare le impostazioni dell'hardware nel sistema.	Proteggere l'hardware impostando una password per la modifica delle impostazioni hardware.	"Controlling Access to System Hardware (Tasks)" in *Oracle Solaris Administration: Security Services*
3. Disattivare i servizi non necessari.	Impedire l'esecuzione dei processi che non rientrano tra le funzioni richieste dal sistema.	"Disattivazione dei servizi non necessari" a pagina 25

Attività	Descrizione	Per istruzioni
4. Impostare l'allocazione del dispositivo.	Impedire l'uso di supporti removibili senza esplicita autorizzazione. I dispositivi includono microfoni, unità USB e CD.	"How to Enable Device Allocation" in *Oracle Solaris Administration: Security Services*
5. Impedire al proprietario della workstation di spegnere il sistema.	Impedire all'utente della console di spegnere o sospendere il sistema.	"Disattivazione della gestione dell'alimentazione del sistema da parte degli utenti" a pagina 26
6. Creare un messaggio di avvertenza login che rifletta il criterio di sicurezza del sito.	Inviare notifiche a utenti e potenziali intrusi indicando che il sistema è monitorato.	"Inserire un messaggio di sicurezza nei file banner" a pagina 26 "Inserire un messaggio di sicurezza nella schermata di login del desktop" a pagina 27

▼ Verifica dei pacchetti

Al completamento dell'installazione, convalidarla verificando i pacchetti.

Prima di cominciare È necessario utilizzare il ruolo `root`.

1 Eseguire il comando `pkg verify`.

Per conservare un record, inviare l'output del comando a un file.

```
# pkg verify > /var/pkgverifylog
```

2 Verificare che il log non contenga errori.

3 In caso contrario, ripetere l'installazione dal supporto o correggere gli errori.

Vedere anche Per maggiori informazioni, vedere le pagine man `pkg`(1) e `pkg`(5) che includono esempi sull'utilizzo del comando `pkg verify`.

▼ Disattivazione dei servizi non necessari

Seguire questa procedura per disattivare i servizi non necessari al sistema.

Prima di cominciare È necessario utilizzare il ruolo `root`.

1 Elencare i servizi online.

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **Disattivare i servizi non necessari al sistema.**

   Ad esempio, se il sistema non è un server NFS o un server Web e i servizi sono online, disattivarli.

   ```
   # svcadm disable svc:/network/nfs/server:default
   # svcadm disable svc:/network/http:apache22
   ```

Vedere anche Per ulteriori informazioni, vedere Capitolo 6, "Managing Services (Overview)" in *Oracle Solaris Administration: Common Tasks* e la pagina man `svcs(1)`.

▼ Disattivazione della gestione dell'alimentazione del sistema da parte degli utenti

Seguire questa procedura per impedire agli utenti del sistema di sospenderlo o spegnerlo.

Prima di cominciare È necessario utilizzare il ruolo `root`.

1. **Verificare i contenuti del profilo di diritti relativo all'utente della console (Console User).**

   ```
   % getent prof_attr | grep Console
   Console User:RO::Manage System as the Console User:
   profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
   Brightness,CPU Power Management,Network Autoconf User;
   auths=solaris.system.shutdown;help=RtConsUser.html
   ```

2. **Creare un profilo di diritti che includa, nel profilo utente della console (Console User), i diritti che si desidera attribuire all'utente.**

   Per informazioni, vedere "How to Create or Change a Rights Profile" in *Oracle Solaris Administration: Security Services* .

3. **Aggiungere un commento al profilo di diritti dell'utente della console (Console User) nel file `/etc/security/policy.conf` .**

   ```
   #CONSOLE_USER=Console User
   ```

4. **Assegnare agli utenti il profilo di diritti creato al Punto 2.**

   ```
   # usermod -P +new-profile username
   ```

Vedere anche Per ulteriori informazioni, vedere "policy.conf File" in *Oracle Solaris Administration: Security Services* e le pagine man `policy.conf(4)` e `usermod(1M)`.

▼ Inserire un messaggio di sicurezza nei file banner

Utilizzare questa procedura per creare messaggi di avvertenza che riflettano i criteri di sicurezza del sito. I contenuti di questi file vengono visualizzati al momento del login locale e remoto.

Nota – I messaggi di esempio riportati nella descrizione della procedura non soddisfano i requisiti governativi degli Stati Uniti e potrebbero non soddisfare i criteri di sicurezza.

Prima di cominciare È necessario utilizzare il ruolo `root`. È consigliabile contattare un consulente legale dell'azienda in merito al contenuto del messaggio di sicurezza.

1. **Digitare un messaggio di sicurezza nel file `/etc/issue` .**

```
# vi /etc/issue
      ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

   Per ulteriori informazioni, vedere la pagina man `issue(4)`.

   Il programma `telnet` mostra i contenuti del file `/etc/issue` come il relativo messaggio di login. Per l'utilizzo di questo file da parte di altre applicazioni, vedere "Visualizzare il messaggio di sicurezza per gli utenti `ssh` e `ftp`" a pagina 37 e "Inserire un messaggio di sicurezza nella schermata di login del desktop" a pagina 27.

2. **Aggiungere un messaggio di sicurezza al file `/etc/motd`.**

```
# vi /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

▼ Inserire un messaggio di sicurezza nella schermata di login del desktop

Scegliere tra i diversi metodi per creare un messaggio di sicurezza che gli utenti possano visionare al login.

Per ulteriori informazioni, fare clic sul menu Sistema > Guida sul desktop per utilizzare il browser della guida di GNOME. È possibile utilizzare anche il comando `yelp`. Informazioni sugli script di login al desktop sono disponibili nella sezione `GDM Login Scripts and Session Files` della pagina man `gdm`(1M).

Nota – I messaggi di esempio riportati nella descrizione della procedura non soddisfano i requisiti governativi degli Stati Uniti e potrebbero non soddisfare i criteri di sicurezza.

Prima di cominciare È necessario utilizzare il ruolo `root`. È consigliabile contattare un consulente legale dell'azienda in merito al contenuto del messaggio di sicurezza.

- **Inserire un messaggio di sicurezza nella schermata di login del desktop.**

  Sono disponibili più opzioni. Le opzioni che costituiscono una finestra di dialogo possono utilizzare il file `/etc/issue` da Punto 1 di "Inserire un messaggio di sicurezza nei file banner" a pagina 26.

  - **OPZIONE 1: Creare un file desktop che mostri il messaggio di sicurezza in una finestra di dialogo al login.**

    ```
    # vi /usr/share/gdm/autostart/LoginWindow/banner.desktop
    [Desktop Entry]
    Type=Application
    Name=Banner Dialog
    Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    Dopo l'autenticazione nella finestra di login, l'utente deve chiudere la finestra di dialogo per raggiungere l'area di lavoro. Per le opzioni del comando `zenity`, consultare la pagina man `zenity`(1).

  - **OPZIONE 2: Modificare uno script di inizializzazione GDM che mostri il messaggio di sicurezza in una finestra di dialogo.**

    La directory `/etc/gdm` include tre script di inizializzazione che mostrano il messaggio di sicurezza prima, durante o subito dopo il login al desktop. Tali script sono inoltre disponibili nella release Oracle Solaris 10.

    - **Visualizzare il messaggio di sicurezza prima che venga aperta la schermata di login.**

      ```
      # vi /etc/gdm/Init/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - **Visualizzare il messaggio di sicurezza nella schermata di login dopo l'autenticazione.**

      Questo script viene eseguito prima di visualizzare l'area di lavoro dell'utente. Per creare questo script, modificare lo script `Default.sample`.

      ```
      # vi /etc/gdm/PostLogin/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - **Visualizzare il messaggio di sicurezza nell'area di lavoro iniziale dell'utente dopo l'autenticazione.**

      ```
      # vi /etc/gdm/PreSession/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

Nota – La finestra di dialogo può essere nascosta da finestre nell'area di lavoro dell'utente.

- **OPZIONE 3: Modificare la finestra di login per visualizzare il messaggio di sicurezza sopra il campo di inserimento.**

  La finestra di login viene ingrandita per adattarsi al messaggio. Questo metodo non punta al file `/etc/issue`. È necessario digitare il testo nell'interfaccia utente grafica.

  Nota – La finestra di login, `gdm-greeter-login-window.ui`, viene sovrascritta dai comandi `pkg fix` e `pkg update`. Per conservare le modifiche apportate, copiare il file in una directory di file di configurazione e integrare le modifiche con il nuovo file dopo l'aggiornamento del sistema. Per ulteriori informazioni, consultare la pagina man `pkg`(5).

  a. **Modificare la directory nell'interfaccia utente della finestra di login.**

     ```
     # cd /usr/share/gdm
     ```

  b. **(Opzionale) Salvare una copia dell'interfaccia utente della finestra di login originale.**

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
     ```

  c. **Aggiungere un'etichetta alla finestra di login utilizzando il generatore di interfacce del GNOME Toolkit.**

     Il programma `glade-3` consente di aprire il generatore di interfacce GTK. Digitare il messaggio di sicurezza in un'etichetta che viene visualizzata sopra il campo di immissione dell'utente.

     ```
     # /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
     ```

     Per visualizzare la guida al generatore di interfacce, fare clic su Sviluppo nel browser della guida GNOME. La pagina man `glade-3`(1) è indicata in Applicazioni nelle pagine del manuale.

  d. **(Opzionale) Dopo aver modificato l'interfaccia utente grafica della finestra di login, salvare una copia.**

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
     ```

Esempio 2–1 Creazione di un breve messaggio di avvertenza al login del desktop

In questo esempio, l'amministratore digita un breve messaggio come argomento nel comando `zenity` nel file desktop. L'amministratore utilizza inoltre l'opzione `--warning`, che mostra un'icona di avvertenza con il messaggio.

```
# vi /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
```

```
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Sicurezza degli utenti

Al termine della procedura, solo l'utente iniziale che può assumere il ruolo `root` ha la possibilità di accedere al sistema. È consigliabile eseguire le seguenti attività nell'ordine indicato, prima che gli utenti con ruoli regolari possano eseguire il login.

Attività	Descrizione	Per istruzioni
Impostare password complesse da modificare frequentemente.	Aumentare la complessità della password predefinita in ogni sistema.	"Impostazione di password più complesse" a pagina 31
Configurare autorizzazioni del file restrittive per gli utenti regolari.	Impostare un valore più restrittivo di `022` per le autorizzazioni del file per gli utenti regolari.	"Impostazione di un valore `umask` più restrittivo per gli utenti regolari." a pagina 32.
Impostare un blocco dell'account per gli utenti regolari.	Nei sistemi non utilizzati per l'amministrazione, impostare un blocco dell'account a livello del sistema e ridurre il numero di login che attivano il blocco.	"Impostazione di un blocco dell'account per gli utenti regolari" a pagina 32
Preselezionare ulteriori classi di audit.	Fornire monitoraggio e registrazioni migliori delle potenziali minacce al sistema.	"Audit di eventi rilevanti oltre a Login/Logout" a pagina 33
Inviare riepiloghi in formato testo di eventi audit all'utilità `syslog`.	Fornire informazioni in tempo reale degli eventi di audit rilevanti, quali login e tentativi di login.	"Monitoraggio degli eventi `lo` in tempo reale" a pagina 34
Creare ruoli.	Distribuire attività amministrative discrete a più utenti affidabili affinché nessun utente possa danneggiare il sistema.	"Setting Up User Accounts" in *Oracle Solaris Administration: Common Tasks* "How to Create a Role" in *Oracle Solaris Administration: Security Services* "How to Assign a Role" in *Oracle Solaris Administration: Security Services* .
Mostrare solo applicazioni consentite su un desktop utente.	Impedire agli utenti di vedere o utilizzare applicazioni non autorizzate.	Vedere "How to Limit a User to Desktop Applications" in *Trusted Extensions Configuration and Administration* .
Limitare i privilegi di un utente.	Rimuovere i privilegi di base non necessari all'utente.	"Rimozione di privilegi di base non necessari all'utente" a pagina 35

▼ Impostazione di password più complesse

Utilizzare questa procedura se le impostazioni predefinite non soddisfano i requisiti di sicurezza del sito. I passaggi seguono l'elenco di voci nel file `/etc/deault/passwd` .

Prima di cominciare

Prima di modificare le impostazioni predefinite, verificare che tali modifiche consentano a tutti gli utenti di autenticarsi nelle rispettive applicazioni e negli altri sistemi presenti in rete.

È necessario utilizzare il ruolo `root`.

- **Modificare il file `/etc/default/passwd`.**

  a. **Imporre agli utenti la modifica delle password ogni mese ma con una frequenza non superiore a tre settimane.**

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  MINWEEKS=3
  ```

  b. **Impostare una password di almeno otto caratteri.**

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. **Conservare una cronologia delle password.**

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. **Imporre una differenza minima tra la vecchia e la nuova password.**

  ```
  #MINDIFF=3
  MINDIFF=4
  ```

  e. **Richiedere almeno un carattere maiuscolo.**

  ```
  #MINUPPER=0
  MINUPPER=1
  ```

  f. **Richiedere almeno un carattere numerico.**

  ```
  #MINDIGIT=0
  MINDIGIT=1
  ```

Vedere anche

- Per l'elenco di variabili che costituiscono i limiti di creazione della password, vedere il file `/etc/default/passwd`. Nello stesso file sono indicate anche le impostazioni predefinite.
- Per i criteri della password in uso dopo l'installazione, vedere "Accesso al sistema limitato e monitorato" a pagina 19.
- Pagina man `passwd(1)`

▼ Impostazione di un blocco dell'account per gli utenti regolari

Utilizzare questa procedura per bloccare gli account degli utenti regolari dopo un certo numero di tentativi di login non riusciti.

Nota – Non impostare blocchi dell'account per gli utenti che possono assumere determinati ruoli al fine di non bloccare il ruolo stesso.

Prima di cominciare È necessario utilizzare il ruolo `root`. Non impostare questa protezione a livello di sistema se quest'ultimo viene utilizzato per attività amministrative.

1 **Impostare l'attributo di sicurezza `LOCK_AFTER_RETRIES` su `YES`.**

- **Impostare a livello di sistema.**

```
# vi /etc/security/policy.conf
...
#LOCK_AFTER_RETRIES=NO
LOCK_AFTER_RETRIES=YES
...
```

- **Impostare a livello di utente.**

```
# usermod -K lock_after_retries=yes username
```

2 **Impostare l'attributo di sicurezza `RETRIES` su `3`.**

```
# vi /etc/default/login
...
#RETRIES=5
RETRIES=3
...
```

Vedere anche

- Per informazioni sugli attributi di sicurezza di utente e ruolo, vedere Capitolo 10, "Security Attributes in Oracle Solaris (Reference)" in *Oracle Solaris Administration: Security Services*.
- Le pagine man selezionate includono `policy.conf`(4) e `user_attr`(4).

▼ Impostazione di un valore umask più restrittivo per gli utenti regolari.

Se il valore predefinito `umask`, `022`, non è sufficientemente restrittivo, impostare una maschera più restrittiva come descritto di seguito.

Prima di cominciare È necessario utilizzare il ruolo `root`.

- **Modificare il valore di umask nei profili di login nelle directory skeleton per diverse shell.**

  Oracle Solaris fornisce directory che gli amministratori possono utilizzare per personalizzare le impostazioni predefinite della shell utente. Tali directoy skeleton includono file quali `.profile` , `.bashrc` e `.kshrc`.

  Scegliere uno dei valori seguenti:

  - `umask 027`: fornisce una protezione moderata del file

    (`740`): `w` per gruppo, `rwx` per altri
  - `umask 026`: fornisce una protezione leggermente più rigida del file

    (`741`): `w` per gruppo, `rw` per altri
  - `umask 077`: fornisce una protezione completa del file

    (`700`): nessun accesso per gruppo o altri

Vedere anche Per maggiori informazioni, vedere:

- "Setting Up User Accounts" in *Oracle Solaris Administration: Common Tasks*
- "Default umask Value" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `usermod`(1M) e `umask`(1).

▼ Audit di eventi rilevanti oltre a Login/Logout

Utilizzare questa procedura per l'audit dei comandi amministrativi, per i tentativi di intrusione nel sistema e per altri eventi rilevanti come specificato dai criteri di sicurezza del sito.

Nota – Gli esempi riportati nella procedura potrebbero non essere sufficienti a soddisfare i criteri di sicurezza.

Prima di cominciare È necessario utilizzare il ruolo `root`. Con la seguente procedura è possibile implementare i criteri di sicurezza del sito relativi all'auditing.

1. **Eseguire l'audit di qualsiasi utilizzo di comandi privilegiati da parte di utenti e ruoli.**

   Per tutti gli utenti e i ruoli, aggiungere l'evento di audit `AUE_PFEXEC` nella relativa maschera di preselezione.

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. **Registrare gli argomenti nei comandi sottoposti ad auditing.**

   ```
   # auditconfig -setpolicy +argv
   ```

3 **Registrare l'ambiente in cui vengono eseguiti i comandi sottoposti ad auditing.**

```
# auditconfig -setpolicy +arge
```

Vedere anche

- Per informazioni sul criterio di audit, vedere "Audit Policy" in *Oracle Solaris Administration: Security Services* .
- Per esempi sui flag dell'audit delle impostazioni, vedere "Configuring the Audit Service (Tasks)" in *Oracle Solaris Administration: Security Services* e "Troubleshooting the Audit Service (Tasks)" in *Oracle Solaris Administration: Security Services* .
- Per configurare l'auditing, vedere la pagina man `auditconfig(1M)`.

▼ Monitoraggio degli eventi lo in tempo reale

Utilizzare questa procedura per attivare il plugin `audit__syslog` per eventi che si desidera monitorare sin dalla loro comparsa.

Prima di cominciare

È necessario utilizzare il ruolo `root` per modificare il file `syslog.conf`. Per eseguire ulteriori passaggi è necessario disporre del profilo di diritti di configurazione audit (Audit Configuration).

1 **Invia della classe `lo` al plugin `audit_syslog` e attivazione.**

```
# auditconfig -setplugin audit_syslog active p_flags=lo
```

2 **Aggiungere una voce `audit.notice` al file `syslog.conf`.**

La voce predefinita include la posizione del file di log.

```
# cat /etc/syslog.conf
...
audit.notice       /var/adm/auditlog
```

3 **Creazione del file di log.**

```
# touch /var/adm/auditlog
```

4 **Aggiornamento delle informazioni di configurazione del servizio `syslog`.**

```
# svcadm refresh system/system-log
```

5 **Aggiornare il servizio di audit.**

Il servizio di audit legge le modifiche del plugin di audit dopo l'aggiornamento.

```
# audit -s
```

Vedere anche

- Per inviare riepiloghi di audit a un altro sistema, vedere ad esempio "How to Configure syslog Audit Logs" in *Oracle Solaris Administration: Security Services* .

- Il servizio di audit può generare output di grandi dimensioni. Per gestire i log, vedere la pagina man `logadm`(1M).
- Per controllare l'output, vedere "Monitoraggio dei riepiloghi di audit `audit__syslog`" a pagina 53.

Rimozione di privilegi di base non necessari all'utente

In alcuni casi, almeno uno dei tre privilegi di base può essere rimosso da un set di base di un utente regolare.

- `file_link_any`: consente di eseguire un processo per creare collegamenti hard a file il cui proprietario ha un UID diverso dall'UID effettivo del processo.
- `proc_fork`: consente a un processo di esaminare lo stato di altri processi ai quali non invia segnali. I processi che non possono essere esaminati non vengono visualizzati in `/proc` e risultano inesistenti.
- `proc_session`: consente a un processo di inviare segnali o processi di tracing al di fuori della propria sessione.

Prima di cominciare È necessario utilizzare il ruolo `root`.

1. **Impedire a un utente di utilizzare il collegamento a un file non di sua proprietà.**

   ```
   # usermod -K defaultpriv=basic,!file_link_any user
   ```

2. **Impedire a un utente di esaminare processi non di sua proprietà.**

   ```
   # usermod -K defaultpriv=basic,!proc_info user
   ```

3. **Impedire a un utente di avviare una seconda sessione, ad esempio avviandone una `ssh`, dalla sessione corrente.**

   ```
   # usermod -K defaultpriv=basic,!proc_session user
   ```

4. **Rimuovere tutti e tre i privilegi da un set di base dell'utente.**

   ```
   # usermod -K defaultpriv=basic,!file_link_any,!proc_info,!proc_session user
   ```

Vedere anche Per ulteriori informazioni, vedere Capitolo 8, "Using Roles and Privileges (Overview)" in *Oracle Solaris Administration: Security Services* e la pagina man `privileges`(5).

Sicurezza del kernel

A questo punto, dovrebbero essere stati creati sia utenti in grado di assumere ruoli, sia i ruoli stessi. Solo il ruolo `root` ha la possibilità di modificare i file di sistema.

Attività	Descrizione	Per istruzioni
Impedire ai programmi di eseguire un exploit di uno stack eseguibile.	Impostare una variabile di sistema che impedisce di eseguire l'exploit degli overflow del buffer che eseguono l'exploit dello stack eseguibile.	"Protecting Executable Files From Compromising Security" in *Oracle Solaris Administration: Security Services*
Proteggere i file core che potrebbero contenere informazioni importanti.	Creare una directory con accesso limitato dedicata ai file core.	"How to Enable a Global Core File Path" in *Oracle Solaris Administration: Common Tasks* "Managing Core Files (Task Map)" in *Oracle Solaris Administration: Common Tasks*

Configurazione della rete

A questo punto, dovrebbero essere stati creati sia utenti in grado di assumere ruoli, sia i ruoli stessi. Solo il ruolo `root` ha la possibilità di modificare i file di sistema.

Tra le attività di rete indicate di seguito, eseguire quelle che garantiscono maggiore sicurezza in base ai requisiti del sito. Queste attività di rete consentono di notificare agli utenti che hanno eseguito il login in remoto che il sistema è protetto e permettono di rafforzare i protocolli IP, ARP e TCP.

Attività	Descrizione	Per istruzioni
Visualizzare messaggi di avvertenza che riflettano i criteri di sicurezza del sito.	Inviare notifiche a utenti e potenziali intrusi indicando che il sistema è monitorato.	"Visualizzare il messaggio di sicurezza per gli utenti `ssh` e `ftp`" a pagina 37
Disattivare il daemon di routing di rete.	Limitare l'accesso ai sistemi da parte di potenziali sniffer di rete.	"Disattivazione del daemon di routing di rete." a pagina 38
Impedire la diffusione di informazioni sulla topologia di rete.	Impedire il broadcast di pacchetti.	"Disattivazione dell'inoltro del pacchetto di broadcast" a pagina 39
	Impedire di rispondere a richieste di eco di broadcast e di multicast.	"Disattivazione delle risposte a richieste di eco" a pagina 40

Attività	Descrizione	Per istruzioni
Per i sistemi che sono gateway per altri domini, come firewall o nodi VPN, attivare un rigido livello di multihoming per origine e destinazione.	Impedire ai pacchetti che non hanno l'indirizzo del gateway nell'intestazione di spostarsi oltre il gateway.	"Impostazione di un rigido multihoming" a pagina 40
Impedire attacchi DOS controllando il numero di connessioni di sistema incomplete.	Limitare il numero consentito di connessioni TCP incomplete per un listener TCP.	"Impostazione del numero massimo di connessioni TCP incomplete" a pagina 41
Impedire attacchi DOS controllando il numero di connessioni di ingresso consentite.	Specificare il numero massimo predefinito di connessioni TCP in sospeso per un listener TCP.	"Impostazione del numero massimo di connessioni TCP in sospeso" a pagina 41
Generare numeri casuali interi per le connessioni TCP iniziali.	Uniformarsi al valore di generazione del numero di sequenza specificato da RFC 1948.	"Specificare un numero casuale intero per la connessione TCP iniziale" a pagina 42
Ripristinare i parametri di rete ai valori predefiniti di sicurezza.	Aumentare la sicurezza ridotta da precedenti interventi di amministrazione.	"Ripristino dei parametri di rete su valori protetti" a pagina 42
Aggiungere wrapper TCP ai servizi di rete per limitare l'uso delle applicazioni agli utenti autorizzati.	Specificare i sistemi che possono accedere ai servizi di rete come, ad esempio, FTP. Per impostazione predefinita, l'applicazione `sendmail` viene protetta con wrapper TCP, come descritto in "Support for TCP Wrappers From Version 8.12 of sendmail" in *Oracle Solaris Administration: Network Services* .	Per attivare wrapper TCP per tutti i servizi `inetd`, vedere "How to Use TCP Wrappers to Control Access to TCP Services" in *Oracle Solaris Administration: IP Services* . Per un esempio di wrapper TCP che protegge il servizio di rete FTP, vedere "How to Start an FTP Server Using SMF" in *Oracle Solaris Administration: Network Services* .

▼ Visualizzare il messaggio di sicurezza per gli utenti ssh e ftp

Utilizzare questa procedura per visualizzare le avvertenze al momento del login remoto e del trasferimento file.

Prima di cominciare

È necessario utilizzare il ruolo `root`. È stato creato il file `/etc/issue` in Punto 1 di "Inserire un messaggio di sicurezza nei file banner" a pagina 26.

1. **Per visualizzare un messaggio di sicurezza per gli utenti registrati mediante l'utilizzo di `ssh`, eseguire quanto indicato di seguito:**

   a. **Rimuovere il commento della direttiva Banner nel file `/etc/sshd_config`.**

   ```
   # vi /etc/ssh/sshd_config
   # Banner to be printed before authentication starts.
   Banner /etc/issue
   ```

   b. **Aggiornare il servizio `ssh`.**

   ```
   # svcadm refresh ssh
   ```

   Per ulteriori informazioni, vedere le pagine man `issue(4)` e `sshd_config(4)`.

2. **Per visualizzare un messaggio di sicurezza per gli utenti registrati mediante `ftp`, eseguire quanto indicato di seguito:**

   a. **Aggiungere la direttiva `DisplayConnect` al file `proftpd.conf`.**

   ```
   # vi /etc/proftpd.conf
   # Banner to be printed before authentication starts.
   DisplayConnect /etc/issue
   ```

   b. **Riavviare il servizio `ftp`.**

   ```
   # svcadm restart ftp
   ```

   Per ulteriori informazioni, vedere il sito Web ProFTPD (`http://www.proftpd.org/`).

▼ Disattivazione del daemon di routing di rete.

Utilizzare questa procedura per prevenire il routing di rete dopo l'installazione specificando un router predefinito. In caso contrario, eseguire questa procedura dopo aver eseguito il routing manualmente.

Nota – Molte procedure di configurazione della rete richiedono la disattivazione del daemon di routing. Tuttavia, il daemon potrebbe essere stato disattivato nell'ambito di una procedura di configurazione più ampia.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1. **Verificare che il daemon di routing sia in esecuzione.**

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
```

```
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

Se il servizio non è in esecuzione, la procedura è conclusa.

2 Disattivare il daemon di routing.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 Verificare che il daemon di routing sia disattivato.

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

Vedere anche Pagina man `routeadm(1M)`

▼ Disattivazione dell'inoltro del pacchetto di broadcast

Per impostazione predefinita, Oracle Solaris inoltra pacchetti di broadcast. Se i criteri di sicurezza del sito richiede la riduzione delle possibilità di snellire il broadcast, modificare l'impostazione predefinita utilizzando questa procedura.

Nota – Quando si disattiva la proprietà di rete `_forward_directed_broadcasts` si disattivano anche i ping di broadcast.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1 Impostare la proprietà di inoltro del pacchetto di broadcast su 0 per i pacchetti IP.

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 Verificare il valore corrente.

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                   PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts  rw   0         --           0         0,1
```

Vedere anche Pagina man `ipadm(1M)`

▼ Disattivazione delle risposte a richieste di eco

Utilizzare questa procedura per impedire la diffusione di informazioni sulla topologia di rete.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1 Impostare la risposta per la proprietà delle richieste di eco broadcast su 0 per i pacchetti IP, quindi verificare il valore corrente.

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2 Impostare la risposta per la proprietà delle richieste di eco multicast su 0 per i pacchetti IP, quindi verificare il valore corrente.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

Vedere anche Per ulteriori informazioni, vedere "_respond_to_echo_broadcast and _respond_to_echo_multicast (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual* e la pagina man `ipadm`(1M).

▼ Impostazione di un rigido multihoming

Per i sistemi che sono gateway per altri domini, come firewall o nodi VPN, utilizzare questa procedura per attivare un rigido livello di multihoming.

La release Oracle Solaris 11 introduce una nuova proprietà `hostmodel` per IPv4 e IPv6. Tale proprietà controlla i comportamenti di invio e ricezione dei pacchetti IP in un sistema di multihoming.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1 Impostare la proprietà `hostmodel` su `strong` per i pacchetti IP.

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2 Verificare il valore corrente e annotare i valori possibili.

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

Vedere anche Per ulteriori informazioni, vedere "hostmodel (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual* e la pagina man `ipadm`(1M).

Per ulteriori informazioni sull'utilizzo di un rigido multihoming, vedere "How to Protect a VPN With IPsec in Tunnel Mode" in *Oracle Solaris Administration: IP Services* .

▼ Impostazione del numero massimo di connessioni TCP incomplete

Adottare questa procedura per prevenire attacchi DOS (denial of service) controllando il numero di connessioni in sospeso incomplete.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1 Impostare il numero massimo di connessioni in ingresso.

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2 Verificare il valore corrente.

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0  rw   4096      --           128       1-4294967295
```

Vedere anche Per ulteriori informazioni, vedere "_conn_req_max_q0" in *Oracle Solaris Tunable Parameters Reference Manual* e la pagina man `ipadm`(1M).

▼ Impostazione del numero massimo di connessioni TCP in sospeso

Utilizzare questa procedura per impedire attacchi DOS controllando il numero di connessioni di ingresso consentite.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management).

1. **Impostare il numero massimo di connessioni in ingresso.**

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2. **Verificare il valore corrente.**

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q   rw   1024      --           128       1-4294967295
```

Vedere anche Per ulteriori informazioni, vedere "_conn_req_max_q" in *Oracle Solaris Tunable Parameters Reference Manual* e la pagina man `ipadm`(1M).

▼ Specificare un numero casuale intero per la connessione TCP iniziale

Questa procedura consente di impostare il parametro di generazione del numero di sequenza iniziale TCP affinché sia conforme a RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`).

Prima di cominciare Per modificare un file system, è necessario che sia attivo il ruolo `root`.

- **Modificare il valore predefinito per la variabile `TCP_STRONG_ISS`.**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ Ripristino dei parametri di rete su valori protetti

Molti parametri di rete protetti per impostazione predefinita sono configurabili e possono essere modificati. Se le condizioni del sito lo consentono, ripristinare i seguenti parametri configurabili ai valori predefiniti.

Prima di cominciare È necessario che all'utente venga assegnato un profilo di diritti per la gestione di rete (Network Management). Il valore corrente del parametro è meno sicuro del valore predefinito.

1. **Impostare la proprietà di inoltro del pacchetto di origine su 0 per i pacchetti IP, quindi verificare il valore corrente.**

   Il valore predefinito impedisce attacchi DOS da pacchetti falsificati.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY            PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
```

```
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6  _forward_src_routed   rw   0         --           0         0,1
```

Per ulteriori informazioni, vedere "forwarding (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual* .

2 Impostare la proprietà di risposta della maschera di rete su 0 per i pacchetti IP, quindi verificare il valore corrente.

Il valore predefinito impedisce la diffusione di informazioni sulla topologia di rete.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 Impostare la proprietà di risposta data/ora su 0 per i pacchetti IP, quindi verificare il valore corrente.

Il valore predefinito consente di rimuovere ulteriori richieste di CPU sui sistemi e impedire la diffusione delle informazioni sulla rete.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_timestamp           rw   0         --           0         0,1
```

4 Impostare la proprietà di risposta data/ora di broadcast su 0 per i pacchetti IP, quindi verificare il valore corrente.

Il valore predefinito consente di rimuovere ulteriori richieste di CPU sui sistemi e impedisce la diffusione delle informazioni sulla rete.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_timestamp_broadcast  rw   0         --           0         0,1
```

5 Impostare la proprietà che consente di ignorare i reindirizzamenti su 0 per i pacchetti IP, quindi verificare il valore corrente.

Il valore predefinito impedisce ulteriori richieste di CPU sui sistemi.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4  _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6  _ignore_redirect  rw   0         --           0         0,1
```

6 Impedire il routing di origine IP.

Se è necessario un routing di origine IP per scopi diagnostici, non disattivare questo parametro di rete.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
```

```
PROTO  PROPERTY          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

Per ulteriori informazioni, vedere "_rev_src_routes" in *Oracle Solaris Tunable Parameters Reference Manual* .

7 Impostare la proprietà che consente di ignorare i reindirizzamenti su 0 per i pacchetti IP, quindi verificare il valore corrente.

Il valore predefinito impedisce ulteriori richieste di CPU sui sistemi. Generalmente, se la rete è ben progettata, non sono necessari reindirizzamenti.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

Vedere anche Pagina man `ipadm`(1M)

Protezione di file system e file

I file system ZFS sono leggeri e possono essere cifrati, compressi e configurati con spazio riservato e limiti di spazio su disco.

Le attività seguenti forniscono una panoramica delle protezioni disponibili in ZFS, il file system predefinito di Oracle Solaris. Per ulteriori informazioni, vedere "Setting ZFS Quotas and Reservations" in *Oracle Solaris Administration: ZFS File Systems* e la pagina man `zfs`(1M).

Attività	Descrizione	Per istruzioni
Prevenire attacchi DOS gestendo e riservando spazio su disco.	Specificare l'utilizzo dello spazio su disco da parte di file system, utente, gruppo o progetto.	"Setting ZFS Quotas and Reservations" in *Oracle Solaris Administration: ZFS File Systems*
Garantire una quantità minima di spazio su disco a un set di dati e ai relativi discendenti.	Garantire spazio su disco per file system, utente, gruppo o progetto.	"Setting Reservations on ZFS File Systems" in *Oracle Solaris Administration: ZFS File Systems*
Cifrare i dati in un file system.	Proteggere un set di dati con cifratura e passphrase per accedervi al termine della sua creazione.	"Encrypting ZFS File Systems" in *Oracle Solaris Administration: ZFS File Systems* "Examples of Encrypting ZFS File Systems" in *Oracle Solaris Administration: ZFS File Systems*

Attività	Descrizione	Per istruzioni
Specificare delle ACL per proteggere i file a un livello di granularità più fine rispetto alle autorizzazioni standard del file UNIX.	Gli attributi di sicurezza estesi possono essere utili per la protezione dei file. Per le precauzioni nell'utilizzo delle ACL, vedere Hiding Within the Trees (`http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf`).	ZFS End-to-End Data Integrity (`http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data`)

Protezione e modifica dei file

Solo il ruolo `root` ha la possibilità di modificare i file di sistema.

Attività	Descrizione	Per istruzioni
Configurare autorizzazioni del file restrittive per gli utenti regolari.	Impostare un valore più restrittivo di `022` per le autorizzazioni del file per gli utenti regolari.	"Impostazione di un valore `umask` più restrittivo per gli utenti regolari." a pagina 32
Impedire la sostituzione di file di sistema con file rogueware.	Trovare i file rogueware mediante uno script o utilizzando file BART.	"How to Find Files With Special File Permissions" in *Oracle Solaris Administration: Security Services*

Sicurezza di applicazioni e servizi

È possibile configurare le funzioni di sicurezza di Oracle Solaris per proteggere le applicazioni.

Creazione di zone per contenere applicazioni critiche

Le zone sono contenitori che consentono di isolare i processi. Sono utili per includere applicazioni e parti di applicazioni. Ad esempio, le zone possono essere utilizzate per separare il database di un sito Web dal server Web del sito.

Per maggiori informazioni e procedure, vedere:

- Capitolo 15, "Introduction to Oracle Solaris Zones" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Summary of Zones by Function" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Capabilities Provided by Non-Global Zones" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Setting Up Zones on Your System (Task Map)" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management* .

- Capitolo 16, “Non-Global Zone Configuration (Overview)” in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*.
- *Hardening Oracle Database with Oracle Solaris Security Technologies* (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

Gestione delle risorse in zone

Le zone forniscono strumenti per la gestione delle relative risorse di zona.

Per maggiori informazioni e procedure, vedere:

- Capitolo 14, “Resource Management Configuration Example” in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Parte I, “Oracle Solaris Resource Management” in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*

Configurazione di IPsec e IKE

IPsec e IKE consentono di proteggere le trasmissioni di rete tra nodi e reti configurati insieme a IPsec e IKE.

Per maggiori informazioni e procedure, vedere:

- Capitolo 14, “IP Security Architecture (Overview)” in *Oracle Solaris Administration: IP Services*
- Capitolo 17, “Internet Key Exchange (Overview)” in *Oracle Solaris Administration: IP Services*
- Capitolo 15, “Configuring IPsec (Tasks)” in *Oracle Solaris Administration: IP Services*
- Capitolo 18, “Configuring IKE (Tasks)” in *Oracle Solaris Administration: IP Services*

Configurazione del filtro IP

La funzione di filtro IP fornisce un firewall.

Per maggiori informazioni e procedure, vedere:

- Capitolo 20, “IP Filter in Oracle Solaris (Overview)” in *Oracle Solaris Administration: IP Services*
- Capitolo 21, “IP Filter (Tasks)” in *Oracle Solaris Administration: IP Services*

Configurazione di Kerberos

È possibile proteggere la rete con il servizio Kerberos. Questa architettura client-server garantisce transazioni sicure sulle reti. Il servizio offre una solida autenticazione utente nonché integrità e privacy. Utilizzando il servizio Kerberos è possibile eseguire il login in altri sistemi, eseguire i comandi, scambiare i dati e trasferire i file in modo sicuro. Inoltre, il servizio consente agli amministratori di limitare l'accesso ai servizi e ai sistemi. Gli utenti Kerberos hanno la possibilità di regolare gli accessi di altri utenti al proprio account.

Per maggiori informazioni e procedure, vedere:

- Capitolo 20, "Planning for the Kerberos Service" in *Oracle Solaris Administration: Security Services*
- Capitolo 21, "Configuring the Kerberos Service (Tasks)" in *Oracle Solaris Administration: Security Services*
- Le pagine man selezionate includono `kadmin`(1M), `pam_krb5`(5) e `kclient`(1M).

Aggiunta di SMF a un servizio legacy

È possibile limitare la configurazione dell'applicazione a utenti o ruoli affidabili aggiungendo l'applicazione alla funzione SMF (Service Managemet Facility) di Oracle Solaris.

Per maggiori informazioni e procedure, vedere:

- "How to Add RBAC Properties to Legacy Applications" in *Oracle Solaris Administration: Security Services*
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`).
- Le pagine man selezionate includono `smf`(5), `smf_security`(5), `svcadm`(1M), e `svccfg`(1M).

Creazione di un'istantanea BART del sistema

Al termine della configurazione di sistema, è possibile creare uno o più file manifesto BART. Tali file manifesto forniscono istantanee del sistema. Quindi, è possibile programmare l'esecuzione regolare di istantanee e confronti. Per maggiori informazioni, vedere la sezione "Utilizzo dello strumento BART (Basic Audit Reporting Tool)" a pagina 51.

Aggiunta di sicurezza multilivello (servizi con etichetta)

Trusted Extensions estende la sicurezza di Oracle Solaris applicando un criterio di controllo dell'accesso obbligatorio (MAC, mandatory access control). Le etichette di sensibilità vengono applicate automaticamente a tutte le origini di dati (reti, file system e finestre) e ai fruitori dei dati stessi (utente e processi). L'accesso a tutti i dati è limitato in base alla relazione tra l'etichetta dei dati (oggetto) e il fruitore (soggetto). La funzionalità su livelli consiste in un set di servizi basati su etichette.

L'elenco parziale dei servizi Trusted Extensions include:

- Networking con etichette
- Attivazione e condivisione di file system basati su etichette
- Desktop con etichette
- Configurazione e traduzione delle etichette
- Strumenti di gestione del sistema basati su etichette
- Allocazione dei dispositivi basata su etichette.

I pacchetti `group/feature/trusted-desktop` forniscono l'ambiente desktop Oracle Solaris multilivello e affidabile.

Configurazione di Trusted Extensions

È necessario installare i pacchetti Trusted Extensions quindi configurare il sistema. Dopo l'installazione del pacchetto, il sistema può eseguire un desktop con uno schermo bitmap direttamente connesso (ad esempio, laptop o workstation). La configurazione di rete è necessaria per comunicare con altri sistemi.

Per maggiori informazioni e procedure, vedere:

- Parte I, "Initial Configuration of Trusted Extensions" in *Trusted Extensions Configuration and Administration*
- Parte II, "Administration of Trusted Extensions" in *Trusted Extensions Configuration and Administration*

Configurazione di IPsec con etichette

È possibile proteggere i pacchetti con etichette tramite IPsec.

Per maggiori informazioni e procedure, vedere:

- Capitolo 14, "IP Security Architecture (Overview)" in *Oracle Solaris Administration: IP Services*
- "Administration of Labeled IPsec" in *Trusted Extensions Configuration and Administration*

- "Configuring Labeled IPsec (Task Map)" in *Trusted Extensions Configuration and Administration*

◆ ◆ ◆ CAPITOLO 3

Monitoraggio e manutenzione della sicurezza di Oracle Solaris 11

Oracle Solaris fornisce due strumenti di sistema per monitorare la sicurezza: la funzione BART (Basic Audit Reporting Tool) e il servizio di audit. I programmi individuali e le applicazioni possono creare inoltre log di accesso e utilizzo.

Utilizzo dello strumento BART (Basic Audit Reporting Tool)

I file manifesto BART assicurano un record statico di ciò che è installato nel sistema. I file manifesto BART possono essere confrontati a distanza di tempo e tra sistemi diversi per tenere traccia delle modifiche apportate ai sistemi installati e delle relative differenze.

Per maggiori informazioni e procedure, vedere:

- "BART (Overview)" in *Oracle Solaris Administration: Security Services*
- "Using BART (Tasks)" in *Oracle Solaris Administration: Security Services*
- "BART Manifests, Rules Files, and Reports (Reference)" in *Oracle Solaris Administration: Security Services*

Per istruzioni specifiche su come tracciare le modifiche nei sistemi installati, vedere "How to Compare Manifests for the Same System Over Time" in *Oracle Solaris Administration: Security Services* .

Utilizzo del servizio di audit

La funzione di auditing consente di conservare un record relativo all'utilizzo del sistema. Il servizio di audit include strumenti di supporto per le analisi dei dati di auditing.

Il servizio di audit è descritto in Parte VII, "Auditing in Oracle Solaris" in *Oracle Solaris Administration: Security Services*.

- Capitolo 26, "Auditing (Overview)" in *Oracle Solaris Administration: Security Services*
- Capitolo 27, "Planning for Auditing" in *Oracle Solaris Administration: Security Services*
- Capitolo 28, "Managing Auditing (Tasks)" in *Oracle Solaris Administration: Security Services*
- Capitolo 29, "Auditing (Reference)" in *Oracle Solaris Administration: Security Services*

  Per un elenco delle pagine man e i relativi collegamenti, vedere "Audit Service Man Pages" in *Oracle Solaris Administration: Security Services* .

Per soddisfare i requisiti del sito, si consiglia di utilizzare le seguenti procedure del servizio di audit:

- Creare ruoli separati per configurare e verificare l'auditing e avviare e arrestare il servizio di audit.

  Utilizzare i profili dei diritti di configurazione, revisione e controllo di audit (Audit Configuration, Audit Review e Audit Control) come base per i ruoli.

  Per creare un ruolo, vedere "How to Create a Role" in *Oracle Solaris Administration: Security Services* .
- Monitorare i riepiloghi in formato testo relativi agli eventi audit nell'utilità `syslog`.

  Attivare il plugin `audit_syslog`, quindi monitorare gli eventi rilevati.

  Vedere "How to Configure syslog Audit Logs" in *Oracle Solaris Administration: Security Services* .
- Limitare le dimensioni dei file di audit.

  Impostare l'attributo `p_fsize` per il plugin `audit_binfile` scegliendo una dimensione utile. Tra gli altri fattori, considerare la pianificazione di revisione, lo spazio su disco e la frequenza del processo `cron`.

  Alcuni esempi sono disponibili in "How to Assign Audit Space for the Audit Trail" in *Oracle Solaris Administration: Security Services* .
- Pianificare il trasferimento sicuro di file di audit completi verso un file system di revisione dell'audit in un pool ZFS separato.
- Rivedere i file di audit completi nel file system di revisione audit.

Monitoraggio dei riepiloghi di audit audit__syslog

Il plugin `audit__syslog` consente di registrare riepiloghi di eventi audit preselezionati.

Dopo averli generati, è possibile visualizzarli in una finestra del terminale eseguendo un comando simile al seguente:

```
# tail -0f /var/adm/auditlog
```

Revisione e archiviazione dei log di audit

I record di audit possono essere visualizzati in formato testo o in un browser in formato XML.

Per maggiori informazioni e procedure, vedere:

- "Audit Logs" in *Oracle Solaris Administration: Security Services*
- "How to Prevent Audit Trail Overflow" in *Oracle Solaris Administration: Security Services*
- "Managing Audit Records on Local Systems (Tasks)" in *Oracle Solaris Administration: Security Services*

Rilevamento di file rogueware

È possibile rilevare l'utilizzo potenzialmente non consentito delle autorizzazioni `setuid` e `setgid` nei programmi. Un file eseguibile sospetto attribuisce la proprietà a un utente e non a un account di sistema quale `root` o `bin`.

Per conoscere la procedura e accedere a un esempio, vedere "How to Find Files With Special File Permissions" in *Oracle Solaris Administration: Security Services* .

◆ ◆ ◆ APPENDICE A

Bibliografia per il documento sulla sicurezza in Oracle Solaris

I seguenti riferimenti includono informazioni di sicurezza importanti per i sistemi Oracle Solaris. Le informazioni di sicurezza delle release precedenti del SO Oracle Solaris includono informazioni utili e altre obsolete.

Riferimenti per Oracle Solaris 11

I manuali e gli articoli seguenti includono descrizioni relative alla sicurezza dei sistemi Oracle Solaris 11:

- *Oracle Solaris Administration: Security Services*

  Questa guida per la sicurezza è stata pubblicata da Oracle per gli amministratori di Oracle Solaris 11 e descrive le funzioni di sicurezza di Oracle Solaris nonché il loro utilizzo per la configurazione dei sistemi. La prefazione include collegamenti ad altre guide di amministrazione del sistema Oracle Solaris che possono contenere informazioni sulla sicurezza.

- *Oracle Solaris Security: Oracle Solaris Express (*`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`*)*

  Questo articolo fornisce un'istantanea delle funzioni di sicurezza di Oracle Solaris per la versione di novembre 2010 di questa release.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  Questo articolo fornisce un'istantanea delle funzioni di Oracle Solaris per la versione di novembre 2010 di questa release.

Per riferimenti utili su Oracle Solaris 10, vedere *Oracle Solaris 10 Security Guidelines*.