Linee guida sulla sicurezza di Oracle® Solaris 11

N. di parte: E53927-02
Settembre 2014

Indice

Indice delle tabelle

Uso della presente documentazione

- **Panoramica**: questo manuale fornisce una panoramica delle funzioni di sicurezza di Oracle Solaris e delle linee guida per il relativo utilizzo volto alla protezione del sistema installato e delle applicazioni.
- **Destinatari**: amministratori di sistema, amministratori della sicurezza, sviluppatori di applicazioni e auditor che sviluppano, distribuiscono o valutano la sicurezza nei sistemi Oracle Solaris 11.
- **Conoscenze richieste**: requisiti di sicurezza del sito.

Libreria della documentazione sul prodotto

Le informazioni più aggiornate e i problemi noti per questo prodotto sono disponibili nella libreria della documentazione all'indirizzo http://www.oracle.com/pls/topic/lookup?ctx=E56341.

Accesso al supporto Oracle

I clienti Oracle possono accedere al supporto elettronico tramite My Oracle Support. Per informazioni, visitare http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs (per non udenti).

Feedback

Inviare feedback su questa documentazione all'indirizzo http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPITOLO 1

Informazioni sulla sicurezza di Oracle Solaris

Oracle Solaris 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 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 hardware di fornitori terzi.

Novità nelle funzioni di sicurezza di Oracle Solaris 11.2

In questa sezione sono evidenziate le informazioni per i clienti esistenti sulle importanti nuove funzioni di sicurezza della presente release.

- È possibile valutare la conformità del sistema agli standard di sicurezza utilizzando il nuovo comando `compliance`. Tale comando consente di valutare e segnalare la conformità del sistema ai benchmark di sicurezza standard del settore, incluso PCI-DSS. Per informazioni dettagliate, vedere «Guida alla verifica della conformità in tema di sicurezza di Oracle Solaris 11.2 » e la pagina man `compliance`(1M).

- La funzione relativa alla struttura di cifratura di Oracle Solaris è conforme allo standard FIPS 140-2, Livello 1 per le funzioni userland e kernel nelle release Oracle Solaris 11.1 SRU 5.5 e Oracle Solaris 11.1 SRU 3.
  - Per un elenco dei prodotti Oracle conformi allo standard FIPS 140, vedere Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html).
  - Per informazioni su come abilitare Modalità FIPS 140 nel sistema, vedere «Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ».
- Oracle Solaris 11.1 ha ottenuto la certificazione Canadian Common Criteria Scheme. Vedere sezione chiamata «Certificazione Common Criteria EAL4+ di Oracle Solaris 11» [28].
- Il servizio di audit può utilizzare Oracle Audit Vault per memorizzare, visionare e analizzare i record di audit. Vedere «Using Oracle Audit Vault and Database Firewall for Storage and Analysis of Audit Records» in «Managing Auditing in Oracle Solaris 11.2 ».
- Il boot verificato protegge il processo di boot dalle minacce sui server Oracle SPARC T5 Series e Oracle SPARC T7 Series. Per ulteriori informazioni, vedere «Using Verified Boot» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 ».
- È possibile proteggere le installazioni AI (Automatic Installation) con certificati e chiavi per il server di installazione, per sistemi client specificati, per tutti i client di un servizio di installazione specificato e per tutti gli altri client AI. Le installazioni AI sicure proteggono la trasmissione dei pacchetti Oracle Solaris ai sistemi degli utenti. Vedere «Increasing Security for Automated Installations» in «Installing Oracle Solaris 11.2 Systems ».
- È disponibile un nuovo pacchetto di installazione di gruppo: `pkg:/group/system/solaris-minimal-server`. Per una descrizione e un confronto dei contenuti del pacchetto di gruppo, vedere «Oracle Solaris 11.2 Package Group Lists ».
- È possibile installare client Kerberos utilizzando AI, per rendere il client un sistema con Kerberos al primo boot. Vedere «How to Configure Kerberos Clients Using AI» in «Installing Oracle Solaris 11.2 Systems ».
- In questa release le zone globali fisiche, denominate zone globali immutabili, e le zone globali virtuali, denominate zone kernel Oracle Solaris, possono essere in sola lettura. Le zone globali immutabili sono leggermente più potenti delle zone kernel, ma nessuno dei due tipi è in grado di modificare in modo permanente l'hardware o la configurazione del sistema. Le zone in sola lettura possono essere avviate in modo più rapido e sono più sicure delle zone che consentono la scrittura.

  Per quanto riguarda la manutenzione, le zone globali immutabili definiscono un set di processi speciale, denominato TCB (Trusted Computing Base) che è possibile configurare tramite un login protetto denominato percorso sicuro. Per ulteriori informazioni, vedere Capitolo 12, «Configuring and Administering Immutable Zones» in «Creating and Using Oracle Solaris Zones ». Per informazioni sulle risorse di configurazione delle zone, vedere «Introduction to Oracle Solaris Zones ». Vedere anche le pagine man `mwac`(5) e `tpd`(5).

  Le zone kernel Oracle Solaris sono utili per la distribuzione di un sistema conforme. È possibile, ad esempio, configurare un sistema conforme e creare un archivio unificato, quindi distribuire l'immagine come zona kernel. Per ulteriori informazioni, consultare la pagina man `solaris-kz`(5) «Creating and Using Oracle Solaris Kernel Zones »,

«Oracle Solaris Zones Overview» in «Introduction to Oracle Solaris 11.2 Virtualization Environments » e «Using Unified Archives for System Recovery and Cloning in Oracle Solaris 11.2 ».

- Di seguito sono riportate alcune nuove funzioni dei diritti di utente e processo.
  - Controllo dell'accesso ai servizi PAM basato sull'orario e sulla posizione
  - Ruoli predefiniti ARMOR (Authorization Roles Managed on RBAC)
  - Profili dei diritti che forzano gli utenti a specificare una password prima di eseguire un'azione privilegiata
  - Profili dei diritti per osservabilità della rete e del sistema per eseguire i comandi di diagnostica `ipstat`, `tcpstat`, `snoop` e `intrstat` con privilegi e senza essere l'utente `root`.

  Per informazioni dettagliate, vedere «What’s New in Rights in Oracle Solaris 11.2» in «Securing Users and Processes in Oracle Solaris 11.2 ».
- IKE Versione 2 (IKEv2) fornisce il protocollo IKE più aggiornato per la gestione automatica delle chiavi dei pacchetti di rete protetti tramite IPsec. Per informazioni dettagliate, vedere «What’s New in Network Security in Oracle Solaris 11.2» in «Securing the Network in Oracle Solaris 11.2 ».
- Oracle Hardware Management Pack (HMP) fornisce strumenti da riga di comando per la configurazione e l'aggiornamento del firmware. Per informazioni su come utilizzare HMP in sicurezza con altri prodotti hardware Oracle come i commutatori e le schede di interfaccia di rete, vedere «Guida per la sicurezza di Oracle Hardware Management Pack per Oracle Solaris ».

Sicurezza di Oracle Solaris 11 dopo l'installazione

L'installazione di Oracle Solaris è di tipo SBD (Secure By Default, sicura per impostazione predefinita). Queste impostazioni di sicurezza proteggono il sistema dalle intrusioni e, tra le altre funzioni di sicurezza, eseguono 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`. Al momento dell'installazione, la password per l'utente iniziale e gli account `root` è 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`.

- All'utente iniziale vengono assegnati i valori predefiniti contenuti nel 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 due caratteri alfabetici e uno non alfabetico. 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 remoto 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` viene registrato 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 autorizzazioni di file, privilegi e diritti dell'utente. I diritti dell'utente sono anche denominati *controllo dell'accesso basato su ruoli* (RBAC, Role-Based Access Control).

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 predefinite sono `drwxr-xr-x` (`755`). Le autorizzazioni del file sono `-rw-r--r--` (`644`).

File di sistema: i file di configurazione del sistema sono protetti da autorizzazioni di file. Un file di sistema può essere modificato solo da un utente con ruolo `root` o a cui sia stato assegnato il diritto di modifica di un determinato file di sistema.

Applet desktop: gli applet desktop sono protetti dalla gestione dei diritti. Le azioni amministrative, come l'aggiunta di stampanti remote in Gestione stampa, sono pertanto limitate agli utenti e ai ruoli che dispongono di diritti amministrativi per la stampa.

Pacchetto di gestione dell'hardware Oracle

Pacchetto di gestione dell'hardware Oracle offre un set di utility per la configurazione, la gestione e il monitoraggio dei server Oracle. Questo set di strumenti a valore aggiunto per l'hardware Oracle è sempre disponibile. Esso può trasmettere automaticamente a ILOM determinate informazioni correlate all'hardware per completarne la visione dell'hardware di sistema. Per informazioni sulle utility e sulla sicurezza, consultare Systems Management and Diagnostics Documentation"> (http://www.oracle.com/goto/ohmp/docs).

Sicurezza configurabile di Oracle Solaris

Oltre alla solida base offerta dalle impostazioni predefinite per la sicurezza di Oracle Solaris, le impostazioni di sicurezza di un sistema Oracle Solaris sono altamente configurabili al fine di soddisfare diversi requisiti di sicurezza.

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.

Protezione dei dati

Oracle Solaris protegge i dati dal boot durante l'installazione, l'uso e l'archiviazione.

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. Il file system predefinito (ZFS) supporta inoltre le liste di controllo dell'accesso (ACL, Access Control List) che consentono di controllare in modo più preciso l'accesso a oggetti del file system individuali o di gruppo.

Per maggiori informazioni, vedere:

- Per una panoramica delle autorizzazioni dei file, vedere «Using UNIX Permissions to Protect Files» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 ».
- Per una panoramica ed alcuni esempi di protezione dei file ZFS, vedere Capitolo 7, «Using ACLs and Attributes to Protect Oracle Solaris ZFS Files» in «Managing ZFS File Systems in Oracle Solaris 11.2 » e le pagine man.
- Per istruzioni sull'impostazione delle ACL su file ZFS, consultare la pagina man `chmod`(1).

Servizi di cifratura

La funzione relativa alla struttura 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. KMF fornisce un'interfaccia unificata per meccanismi di archiviazione, utilità amministrative e interfacce di programmazione altrimenti diverse per varie infrastrutture PKI (Public Key Infrastructure).

La struttura di cifratura fornisce una memoria comune di algoritmi e librerie PKCS 11 per la gestione dei requisiti di cifratura. Le librerie The PKCS 11 vengono implementate in base allo standard PKCS #11 Cryptographic Token Interface (Cryptoki) di RSA Security Inc. I servizi di cifratura, come la cifratura e la decifratura dei file, sono disponibili per gli utenti regolari.

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:

- Le pagine man selezionate includono `cryptoadm`(1M), `encrypt`(1), `mac`(1), `pktool`(1) e `kmfcfg`(1).

- Per una panoramica dei servizi di cifratura, vedere Capitolo 1, «Cryptographic Framework» in «Managing Encryption and Certificates in Oracle Solaris 11.2 » e Capitolo 4, «Key Management Framework» in «Managing Encryption and Certificates in Oracle Solaris 11.2 ».
- Per esempi dell'uso della struttura di cifratura, vedere Capitolo 3, «Cryptographic Framework» in «Managing Encryption and Certificates in Oracle Solaris 11.2 » e le pagine man.
- Per abilitare il provider FIPS 140 della struttura di cifratura, vedere «How to Create a Boot Environment with FIPS 140 Enabled» in «Managing Encryption and Certificates in Oracle Solaris 11.2 ».

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 le ACL proteggono i file ed è possibile cifrare l'intero set di dati al momento della creazione. La gestione dei diritti di Oracle Solaris supporta l'amministrazione delegata dei set di dati ZFS. In altre parole, gli utenti a cui è assegnato un set di privilegi limitato possono amministrare i set di dati ZFS.

Per maggiori informazioni, vedere:

- «User Rights Management» in «Securing Users and Processes in Oracle Solaris 11.2 »
- Capitolo 1, «Oracle Solaris ZFS File System (Introduction)» in «Managing ZFS File Systems in Oracle Solaris 11.2 »
- «Oracle Solaris ZFS and Traditional File System Differences» in «Managing ZFS File Systems in Oracle Solaris 11.2 »
- Capitolo 5, «Managing Oracle Solaris ZFS File Systems» in «Managing ZFS File Systems in Oracle Solaris 11.2 »
- «How to Remotely Administer ZFS With Secure Shell» in «Managing Secure Shell Access in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `zfs`(1M) e `zfs`(7FS).

Java Cryptography Extension (JCE)

Java offre JCE (Java Cryptography Extension) per gli sviluppatori di applicazioni Java. Per ulteriori informazioni, vedere Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

Protezione e isolamento delle applicazioni

Le applicazioni possono essere punti di accesso per malware e utenti malintenzionati. In Oracle Solaris queste minacce sono mitigate dall'uso dei privilegi e dal contenimento delle applicazioni in zone. È possibile eseguire le applicazioni utilizzando solo i privilegi ad esse necessari, in modo che un utente malintenzionato non disponga dei privilegi root per accedere al resto del sistema. Le zone possono limitare l'estensione di un attacco. Gli attacchi alle applicazioni in una zona non globale possono incidere solo sui processi in tale zona e non sul sistema host della zona.

Le funzioni ASLR (Address Space Layout Randomization) e SMF (Service Management Facility) sono funzioni aggiuntive per la protezione delle applicazioni. ASLR rende difficile agli intrusi di controllare un eseguibile e le funzioni SMF consentono agli amministratori di limitare l'avvio, l'arresto e l'uso di un'applicazione.

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 concessi a un processo, un utente o un ruolo. Molti comandi e daemon di Oracle Solaris vengono eseguiti utilizzando solo i privilegi necessari per completare le rispettive attività. I programmi dotati di privilegi possono evitare le intrusioni ottenendo più privilegi rispetto a quelli comunemente utilizzati.

L'utilizzo di privilegi è anche denominato *gestione dei diritti del processo*. I privilegi consentono alle organizzazioni di specificare, e di conseguenza limitare, i privilegi concessi a servizi e processi in esecuzione nei sistemi.

Per maggiori informazioni, vedere:

- «Process Rights Management» in «Securing Users and Processes in Oracle Solaris 11.2 »
- Capitolo 2, «Developing Privileged Applications» in «Developer’s Guide to Oracle Solaris 11 Security »
- Le pagine man selezionate includono `ppriv`(1) e `privileges`(5).

Zone di Oracle Solaris

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.

In Oracle Solaris 11.2 è possibile configurare i file system root immutabili.

Per maggiori informazioni, vedere:

- «Configuring Read-Only Zones» in «Creating and Using Oracle Solaris Zones »
- «Introduction to Oracle Solaris Zones »
- Le pagine man selezionate includono `brands`(5), `zoneadm`(1M) e `zonecfg`(1M).

ASLR (Address Space Layout Randomization)

La funzionalità ASLR (Address Space Layout Randomization) dispone in ordine casuale gli indirizzi utilizzati da un determinato programma. La funzionalità ASLR può prevenire determinati tipi di attacchi basati sulla conoscenza della posizione esatta di determinati intervalli di memoria e rilevare il tentativo quando questo sta per arrestare il programma. Per ulteriori informazioni, vedere «Address Space Layout Randomization» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 » e Come verificare se ASLR è abilitato [33].

Service Management Facility

I *servizi* sono applicazioni continuamente in esecuzione. Un servizio può rappresentare un'applicazione in esecuzione, lo stato del software di un dispositivo o un set di altri servizi. La funzione Service Management Facility (SMF) di Oracle Solaris viene utilizzata per aggiungere, rimuovere, configurare e gestire i servizi. La funzione SMF utilizza la gestione dei diritti 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:

- «Managing System Services in Oracle Solaris 11.2 »
- «How to Assign Specific Privileges to the Apache Web Server» in «Securing Users and Processes in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `svcadm`(1M), `svcs`(1) e `smf`(5).

Protezione degli utenti e assegnazione di diritti aggiuntivi

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 sezione chiamata «Accesso al sistema limitato e monitorato» [13]. Tali diritti sono configurabili. È possibile negare i diritti di base e aumentare i diritti per un utente.

Oracle Solaris protegge gli utenti utilizzando requisiti di complessità flessibili per le password, autenticazione configurabile per diversi requisiti del sito e gestione dei diritti degli utenti tramite profili dei diritti, autorizzazioni e privilegi per la limitazione e la distribuzione dei diritti amministrativi agli utenti sicuri. Inoltre, alcuni account condivisi speciali, denominati *ruoli* assegnano all'utente tali diritti amministrativi solo quando l'utente assume il ruolo. Il pacchetto ARMOR (Authorization Rules Managed On RBAC) fornisce ruoli predefiniti.

Password e limiti della password

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

Oracle Solaris include diverse funzionalità che possono essere utilizzate per configurare le password degli utenti in base ai requisiti del sito. È possibile specificare lunghezza della password, contenuto, frequenza e requisiti di modifica. È inoltre possibile conservare una cronologia delle password. Viene altresì fornito un dizionario delle password da evitare. Sono disponibili diversi algoritmi hash per le password. L'impostazione predefinita è SHA256.

Per maggiori informazioni, vedere:

- «Maintaining Login Control» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 »
- «Securing Logins and Passwords» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `passwd`(1) e `crypt.conf`(4).

Moduli di autenticazione collegabili (PAM, Pluggable Authentication Module)

La struttura del modulo di autenticazione collegabile (PAM) consente agli amministratori di coordinare e configurare i requisiti di autenticazione dell'utente per account, credenziali, sessioni e password senza modificare i servizi che richiedono autenticazione.

La struttura 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 `ssh` utilizzano la struttura PAM per proteggere tutti i punti di accesso al

sistema appena installato. Il modulo PAM 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 la struttura PAM.

Oracle Solaris offre una vasta gamma di moduli PAM e configurazioni volti a soddisfare i criteri della maggior parte dei siti. Per maggiori informazioni, vedere:

- Capitolo 1, «Using Pluggable Authentication Modules» in «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- «Writing Applications That Use PAM Services» in «Developer's Guide to Oracle Solaris 11 Security »
- Pagina man `pam.conf`(4)

Gestione dei diritti degli utenti

I diritti degli utenti in Oracle Solaris sono governati dal principio di sicurezza del privilegio minimo. Le organizzazioni possono garantire in modo selettivo i diritti amministrativi a utenti o ruoli in base a esigenze e requisiti specifici dell'organizzazione. Inoltre, possono negare diritti agli utenti quando necessario. I diritti vengono implementati come privilegi su processi e autorizzazioni per gli utenti o i metodi SMF. I profili dei diritti offrono un modo conveniente per raccogliere privilegi e autorizzazioni in un pacchetto di diritti correlati.

Per maggiori informazioni, vedere:

- «Securing Users and Processes in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `auths`(1), `privileges`(5). `profiles`(1), `rbac`(5), `roleadd`(1M), `roles`(1) e `user_attr`(4).

Sicurezza delle comunicazioni di rete

Le comunicazioni di rete possono essere protette con funzioni quali firewall, wrapper TCP su applicazioni di rete e connessioni remote cifrate e autenticate.

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.

Firewall

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:

- Per una panoramica del filtro IP; vedere Capitolo 4, «About IP Filter in Oracle Solaris» in «Securing the Network in Oracle Solaris 11.2 ».
- Per esempi relativi all'utilizzo del filtro IP, vedere Capitolo 5, «Configuring IP Filter» in «Securing the Network in Oracle Solaris 11.2 » e le pagine man.
- Per informazioni ed esempi sulla sintassi del linguaggio del criterio del filtro IP, consultare la pagina man `ipnat`(4).
- Le pagine man selezionate includono `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) e `ipf`(4).

Wrapper TCP

I wrapper TCP forniscono il controllo dell'accesso per i servizi Internet. Quando diversi servizi Internet (`inetd`) sono abilitati, il daemon `tcpd` controlla l'indirizzo di un host che richiede un determinato servizio di rete in una ACL. Le richieste vengono accettate o respinte in base al risultato del controllo. I wrapper TCP registrano anche le richieste degli host di servizi di rete in `syslog` e rappresentano un'utile funzione di monitoraggio.

Le funzioni Secure Shell (`ssh`) e `sendmail` di Oracle Solaris sono configurate per utilizzare wrapper TCP. I servizi di rete dotati di mapping one-to-one ai file eseguibili, come `proftpd` e `rpcbind`, sono candidati per i wrapper TCP.

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 informazioni sui wrapper TCP, vedere:

- Come utilizzare i wrapper TCP [48]
- Per informazioni ed esempi sulla sintassi relativa al linguaggio di controllo dell'accesso per wrapper TCP, vedere la pagina man `hosts_access`(4).
- Le pagine man selezionate includono `tcpd`(1M) e `inetd`(1M).

Accesso remoto

Gli attacchi di accesso remoto possono danneggiare un sistema e una rete. Oracle Solaris fornisce una difesa avanzata delle trasmissioni di rete. Le funzioni di difesa includono la cifratura e i controlli dell'autenticazione per la trasmissione dei dati, l'autenticazione del login e la disabilitazione di servizi remoti non necessari.

IPsec e IKE

La sicurezza IP (IPsec) protegge le trasmissioni di rete autenticando i pacchetti IP, cifrandoli o effettuando entrambe le operazioni. 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) automatico utilizza algoritmi dalla struttura di cifratura. Inoltre, la struttura di cifratura fornisce un keystore centrale. 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 in un keystore software denominato *softtoken*.

Poiché IPsec e IKE richiedono configurazione, non vengono abilitati per impostazione predefinita. Se amministrato correttamente, IPsec è uno strumento utile per la protezione del traffico di rete.

Per maggiori informazioni, vedere:

- Capitolo 6, «About IP Security Architecture» in «Securing the Network in Oracle Solaris 11.2 »
- Capitolo 7, «Configuring IPsec» in «Securing the Network in Oracle Solaris 11.2 »
- «IPsec and FIPS 140» in «Securing the Network in Oracle Solaris 11.2 »
- Capitolo 8, «About Internet Key Exchange» in «Securing the Network in Oracle Solaris 11.2 »
- Capitolo 9, «Configuring IKEv2» in «Securing the Network in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `ipsecconf`(1M) e `in.iked`(1M).

Secure Shell

Per impostazione predefinita, la funzione Secure Shell di Oracle Solaris è l'unico meccanismo di accesso remoto attivo su un sistema appena installato. Tutti gli altri servizi di rete sono disabilitati o in modalità di solo ascolto.

Secure Shell crea un canale di comunicazione cifrata tra i sistemi. 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 maggiori informazioni, vedere:

- Capitolo 1, «Using Secure Shell (Tasks)» in «Managing Secure Shell Access in Oracle Solaris 11.2 »
- «Secure Shell and FIPS 140» in «Managing Secure Shell Access in Oracle Solaris 11.2 »
- 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 in cui i sistemi eseguono diversi sistemi operativi e il servizio Kerberos.

Kerberos è basato sul protocollo di autenticazione della rete Kerberos V5 sviluppato dal Massachusetts Institute of Technology (MIT) Il servizio Kerberos 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:

- «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- «FIPS 140 Algorithms and Kerberos Encryption Types» in «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `kadmin`(1M), `kdcmgr`(1M), `kerberos`(5), `kinit`(1) e `krb5.conf`(4).

Manutenzione della sicurezza del sistema

Oracle Solaris fornisce le funzionalità indicate di seguito per mantenere la sicurezza di un sistema.

- Boot verificato: protegge il processo di boot. Il boot verificato viene disabilitato per impostazione predefinita.
- Verifica del pacchetto: verifica che i pacchetti installati siano identici a quelli nel repository di origine.

- Servizio di audit: esegue l'audit dell'accesso al sistema e del relativo utilizzo. L'audit è abilitato per impostazione predefinita.
- Verifica dell'integrità dei file: nei file manifesto BART possono essere elencati tutti i file nel sistema. I confronti dei file manifesto vengono utilizzati per verificare che venga manutenuta l'integrità dei file.
- File di log: SMF fornisce file di log per ogni servizio. La utility `syslog` fornisce un file centrale per denominare e configurare i log per i servizi di sistema e può inviare una notifica agli amministratori in caso di eventi critici. Anche altre funzioni, come l'auditing, creano i propri log.
- Report di conformità: Oracle Solaris fornisce diversi benchmark di sicurezza in base ai quali è possibile valutare il sistema. Queste valutazioni producono i report che consentono di valutare le impostazioni di sicurezza del sistema.

Boot verificato

Il boot verificato è una funzione di Oracle Solaris che protegge il processo di boot di un sistema. Questa funzione protegge il sistema da minacce quali l'installazione dei moduli kernel e applicazioni Trojan non autorizzati. Per impostazione predefinita, il boot verificato è disabilitato.

Per ulteriori informazioni, vedere Capitolo 2, «Protecting Oracle Solaris Systems Integrity» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 ».

Verifica dell'integrità del pacchetto

Dopo avere installato o aggiornato i pacchetti, è possibile eseguire il comando `pkg verify` per garantire che i pacchetti nel sistema siano identici a quelli nel repository di origine.

Per ulteriori informazioni, consultare la pagina man `pkg`(1) e Come verificare i pacchetti [33].

Servizio di audit

Oracle Solaris fornisce un servizio di audit che raccoglie dati sull'accesso al sistema e il relativo utilizzo. I dati di audit forniscono un log affidabile con indicatore di data e ora degli eventi di sistema correlati 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, conformità e certificazione della sicurezza. L'auditing può costituire inoltre un deterrente per potenziali intrusioni.

Per maggiori informazioni, vedere:

- Per un elenco di pagine man correlate all'audit, vedere Capitolo 7, «Auditing Reference» in «Managing Auditing in Oracle Solaris 11.2 ».
- Per linee guida, vedere Come eseguire l'audit di eventi rilevanti oltre a Login/Logout [44] e le pagine man.
- Per una panoramica dell'auditing, vedere Capitolo 1, «About Auditing in Oracle Solaris» in «Managing Auditing in Oracle Solaris 11.2 ».
- Per le attività di auditing, vedere Capitolo 3, «Managing the Audit Service» in «Managing Auditing in Oracle Solaris 11.2 ».

Verifica dell'integrità dei file

La funzione BART di Oracle Solaris consente di convalidare in modo completo i sistemi eseguendo verifiche del sistema, a livello di file, nel tempo. Dopo l'installazione, il comando `pkg verify` verifica se il contenuto del pacchetto di origine è identico a quello di destinazione. Dopo la verifica dei pacchetti, i file manifesto BART possono raccogliere in modo facile e affidabile informazioni sui file in un sistema.

BART è uno strumento utile per la gestione dell'integrità su un sistema o su una rete di sistemi. È possibile confrontare i file di un sistema con i file originali del sistema e con altri file del sistema. I report possono indicare che a un sistema non è stata applicata una patch, che un intruso ha installato file non approvati o che un intruso ha modificato le autorizzazioni o il contenuto di file riservati, come i file di proprietà dell'utente `root`.

Per maggiori informazioni, vedere:

- Per le linee guida, vedere sezione chiamata «Verifica dell'integrità del file utilizzando BART» [56], sezione chiamata «Verifica dell'integrità del file utilizzando BART» [56] e le pagine man.
- Per una panoramica su BART, vedere Capitolo 2, «Verifying File Integrity by Using BART» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 ».
- Per alcuni esempio sull'uso di BART, vedere «About Using BART» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 » e le pagine man.
- Le pagine man selezionate includono `bart`(1M), `bart_rules`(4) e `bart_manifest`(4).

File di log

La funzione Service Management Facility (SMF) di Oracle Solaris registra lo stato di ciascun servizio. Molti servizi, come l'auditing e Secure Shell, scrivono i propri log. Il daemon `syslog` o `rsyslog` scrive un log centralizzato che può informare e avvisare gli amministratori in caso di condizioni critiche in molti servizi. È possibile, ad esempio, configurare l'auditing in

modo che vengano scritti record di auditing di riepilogo in `syslog`. Consultare le pagine man `syslogd`(1M) e `syslog.conf`(4).

Conformità agli standard di sicurezza

Il comando `compliance assess` fornisce un'istantanea delle impostazioni di sicurezza del sistema. I report delle assegnazioni suggeriscono modifiche specifiche al sistema per soddisfare i benchmark di sicurezza del settore. Per ulteriori informazioni, vedere «Guida alla verifica della conformità in tema di sicurezza di Oracle Solaris 11.2 » e la pagina man `compliance`(1M).

Sicurezza con etichette

In Oracle Solaris la sicurezza con etichette viene fornita dalla funzione Trusted Extensions.

Funzione Trusted Extensions in Oracle Solaris

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.

L'implementazione della funzione Trusted Extensions si differenzia per la sua capacità di garantire la massima affidabilità ottimizzando la compatibilità e riducendo l'overhead. Trusted Extensions fa parte della certificazione sezione chiamata «Certificazione Common Criteria EAL4+ di Oracle Solaris 11» [28].

Trusted Extensions soddisfa i requisiti del pacchetto Common Criteria Labeled Security Package (LSP). Vedere sezione chiamata «Certificazione Common Criteria EAL4+ di Oracle Solaris 11» [28].

Per maggiori informazioni, vedere:

- Per informazioni sulla configurazione e la manutenzione di Trusted Extensions, vedere «Trusted Extensions Configuration and Administration ».
- Le pagine man selezionate includono `trusted_extensions`(5), `labeladm`(1M) e `labeld`(1M).

File system con etichette

Per impostazione predefinita, ai file system viene assegnata una singola etichetta in una zona con la stessa etichetta. È possibile creare un set di dati ZFS su più livelli, installarlo su un sistema Trusted Extensions e, con le autorizzazioni appropriate, eseguire l'upgrade e il downgrade dei file in tale set di dati. Per ulteriori informazioni, vedere «Multilevel Datasets for Relabeling Files» in «Trusted Extensions Configuration and Administration ».

Comunicazioni di rete con etichetta

Trusted Extensions assegna etichette alle comunicazioni di rete. I flussi di dati vengono limitati in base a un confronto delle etichette associate agli endpoint di rete di origine e agli endpoint di rete riceventi. È necessario che siano state assegnate etichette anche ai gateway e agli hop intermedi per consentire il passaggio di informazioni all'etichetta della comunicazione. Il file system di rete e i set di dati ZFS su più livelli forniscono ulteriori funzioni in una rete.

Per maggiori informazioni, vedere:

- «Configuring the Network Interfaces in Trusted Extensions» in «Trusted Extensions Configuration and Administration »
- Capitolo 15, «Trusted Networking» in «Trusted Extensions Configuration and Administration »
- Capitolo 16, «Managing Networks in Trusted Extensions» in «Trusted Extensions Configuration and Administration »

Desktop multilivello di Trusted Extensions

Diversamente dalla maggior parte degli altri sistemi operativi multilivello, Trusted Extensions include un desktop multilivello. È possibile configurare gli utenti in modo da visualizzare solo le etichette consentite. Ciascuna etichetta può essere configurata in modo da richiedere una password separata.

Per ulteriori informazioni, vedere «Trusted Extensions User’s Guide ». Per configurare gli utenti, vedere Capitolo 11, «Managing Users, Rights, and Roles in Trusted Extensions» in «Trusted Extensions Configuration and Administration ».

Certificazione Common Criteria EAL4+ di Oracle Solaris 11

Oracle Solaris 11 ha ottenuto la certificazione Canadian Common Criteria Scheme al livello Evaluation Assurance Level 4 (EAL4), aumentato grazie alla risoluzione dei difetti (EAL4+).

EAL4 è il livello di valutazione più elevato mutualmente riconosciuto da 26 paesi nell'ambito del CCRA (Common Criteria Recognition Arrangement).

La certificazione riguarda l'OSPP (Operating System Protection Profile) e include i pacchetti estesi riportati di seguito.

- Gestione avanzata
- Autenticazione e identificazione estesa
- Sicurezza con etichette
- Virtualizzazione

Per informazioni sulla certificazione, vedere:

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

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. Se si stanno sviluppando programmi o installando programmi di fornitori terzi, è necessario sviluppare e installare tali programmi in modo sicuro.

Per maggiori informazioni, vedere:

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- Appendice A, «Secure Coding Guidelines for Developers» in «Developer’s Guide to Oracle Solaris 11 Security »
- 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

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 Sistema operativo Oracle Solaris

Per installare il Sistema operativo Oracle Solaris, selezionare una serie di pacchetti denominata *group* da un repository di pacchetti. Gruppi diversi forniscono pacchetti per usi diversi, come server multiuso, sistemi a installazione minima e sistemi desktop. I pacchetti sono contrassegnati ed è possibile verificarne il trasferimento sicuro.

Quando si esegue l'installazione del Sistema operativo 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 Oracle Solaris Large Server.
- **Oracle Solaris Small Server –** l'esecuzione di Automated Installer (AI) ed, eventualmente, del programma di installazione in modalità testo, determina l'installazione del gruppo `group/system/solaris-small-server`, che offre un utile ambiente a riga di comando a cui è possibile aggiungere pacchetti.
- **Oracle Solaris Minimal Server –** l'esecuzione di Automated Installer (AI) ed, eventualmente, del programma di installazione in modalità testo, determina l'installazione

del gruppo `group/system/solaris-minimal-server`, che offre un ambiente a riga di comando ridotto a cui è possibile aggiungere solo i pacchetti desiderati.

- **Oracle Solaris Desktop –** l'esecuzione di Live Media determina l'installazione del 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` al server desktop. Per maggiori 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 11.2 Systems ».

Consultare le seguenti guide dei contenuti su installazione e pacchetti per la scelta del supporto:

- «Installing Oracle Solaris 11.2 Systems »
- «Creating a Custom Oracle Solaris 11.2 Installation Image »
- «Adding and Updating Software in Oracle Solaris 11.2 »
- «Oracle Solaris 11.2 Package Group Lists »

Sicurezza iniziale del sistema

È consigliabile eseguire le seguenti attività nell'ordine indicato. In questa fase il sistema operativo Oracle Solaris è installato e solo l'utente iniziale che può assumere il ruolo `root` potrà accedervi.

TABELLA 2-1 Mappa delle attività per la sicurezza del sistema

Attività	Descrizione	Per istruzioni
1. Verificare i pacchetti nel sistema.	Assicurarsi che i pacchetti di installazione di origine siano identici ai pacchetti installati.	Come verificare i pacchetti [33]
2. Assicurarsi che i file eseguibili siano protetti.	Consente di verificare se ASLR è abilitato.	Come verificare se ASLR è abilitato [33]
3. Salvaguardare le impostazioni dell'hardware nel sistema.	Proteggere l'hardware impostando una password per la modifica delle impostazioni hardware. Su una piattaforma x86 l'accesso al menu GRUB è controllato. Su una piattaforma SPARC il comando `eeprom` protegge l'hardware.	«Controlling Access to System Hardware» in «Securing Systems and Attached Devices in Oracle Solaris 11.2 »
3. Disabilitare i servizi non necessari.	Impedire l'esecuzione dei processi che non rientrano tra le funzioni richieste dal sistema.	Come disattivare i servizi non necessari [34]
5. Impedire al proprietario della workstation di spegnere il sistema.	Impedire all'utente della console di spegnere o sospendere il sistema.	Come disattivare la gestione dell'alimentazione del sistema da parte degli utenti [34]
6. Creare un messaggio di avvertenza login che rifletta il criterio di sicurezza del sito.	Consente di inviare notifiche prima e dopo l'autenticazione indicando che il sistema è monitorato.	Come inserire un messaggio di sicurezza nei file banner [35]

Attività	Descrizione	Per istruzioni
		Come inserire un messaggio di sicurezza nella schermata di login del desktop [36]

▼ Come verificare i pacchetti

Al completamento dell'installazione, convalidarla verificando i pacchetti.

Prima di cominciare È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Esaminare il log di installazione.**
2. **Eseguire il comando `pkg verify`.**

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

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

3. **Verificare che il log non contenga errori.**
4. **In caso contrario, ripetere l'installazione dal supporto o correggere gli errori.**

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

▼ Come verificare se ASLR è abilitato

Per impostazione predefinita, le istruzioni eseguibili contrassegnate vengono scritte su spazi con indirizzi non connessi per ridurre la possibilità che eventuali intrusi inseriscano istruzioni nello stack eseguibile.

Prima di cominciare È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Verificare se ASLR è abilitato.**

   ```
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (all)           enabled (all)
   ```

   Il valore `all` è più complesso del valore predefinito e potrebbe generare errori in applicazioni che si basano su uno stack consecutivo in memoria. Ad esempio, i database potrebbero basarsi su uno stack consecutivo in memoria.

2. **Se ASLR è disabilitato, abilitare il valore predefinito e verificare che sia operativo.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (tagged-files)  system default (default)
```

Vedere anche A scopo di debug, è possibile disattivare ASLR richiamando il comando `sxadm` su un determinato binario. Per alcuni esempi, consultare la pagina man `sxadm`(1M).

▼ Come disattivare i servizi non necessari

Seguire questa procedura per disattivare i servizi non necessari in questo sistema.

Prima di cominciare È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Elencare i servizi di rete online.**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server: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 1, «Introduction to the Service Management Facility» in «Managing System Services in Oracle Solaris 11.2 » e consultare la pagina man `svcs`(1).

▼ Come disattivare la gestione dell'alimentazione del sistema da parte degli utenti

Seguire questa procedura per impedire agli utenti alla console di un sistema di sospenderlo o spegnerlo. Questa soluzione software non è efficace se l'hardware del sistema può essere scollegato dall'utente della console.

Prima di cominciare È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

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

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 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 le istruzioni, vedere «How to Create a Rights Profile» in «Securing Users and Processes in Oracle Solaris 11.2 ».

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 il profilo di diritti creato al Passo 2.**

   - In caso di più utenti che condividono un profilo di diritti, l'impostazione di questo valore in un profilo può rappresentare una soluzione scalabile.

     ```
     # usermod -P shared-profile username
     ```

   - È anche possibile assegnare il profilo in base al sistema nel file `policy.conf`.

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

Vedere anche Per ulteriori informazioni, vedere «policy.conf File» in «Securing Users and Processes in Oracle Solaris 11.2 » e consultare le pagine man `policy.conf`(4) e `usermod`(1M).

▼ Come inserire un messaggio di sicurezza nei file banner

Utilizzare questa procedura per creare messaggi di sicurezza in due file banner che riflettano i criteri di sicurezza del sito. Il file `/etc/issue` viene visualizzato prima dell'autenticazione, mentre il file `/etc/motd` viene visualizzato dopo l'autenticazione.

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. Contattare un consulente legale dell'azienda in merito al contenuto del messaggio di sicurezza.

Prima di cominciare

È necessario diventare un amministratore con profilo dotato di diritti di amministratore per la modifica dei messaggi. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Creare il file `/etc/issue` e aggiungere un messaggio di sicurezza.**

```
# pfedit /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.
```

Il comando `login` consente di visualizzare il contenuto del file `/etc/issue` prima dell'autenticazione, allo stesso modo dei servizi `ssh`, `telnet` e FTP. Per visualizzare il contenuto del file `/etc/issue` nella schermata di login al desktop, vedere Come inserire un messaggio di sicurezza nella schermata di login del desktop [36].

Per ulteriori informazioni, consultare le pagine man `issue`(4) e `pfedit`(1M).

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

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

In Oracle Solaris la shell iniziale dell'utente mostra il contenuto del file `/etc/motd`.

▼ Come 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 prima dell'autenticazione, dopo l'autenticazione o in entrambi i momenti. Il file `/etc/issue` viene visualizzato prima dell'autenticazione, mentre il file `/etc/motd` viene visualizzato dopo l'autenticazione.

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. Contattare un consulente legale dell'azienda in merito al contenuto del messaggio di sicurezza.

Prima di cominciare

Per creare un file, è necessario utilizzare il ruolo `root`. Per modificare un file esistente, è necessario diventare amministratore con autorizzazione `solaris.admin.edit/`*path-to-existing-file*.

1. **Inserire un messaggio di sicurezza nella schermata di login del desktop prima dell'autenticazione utilizzando una delle tre opzioni riportate di seguito.**

   Le opzioni che consentono di creare una finestra di dialogo prima dell'autenticazione utilizzano il messaggio di sicurezza del file `/etc/issue` riportato al Passo 1 della sezione Come inserire un messaggio di sicurezza nei file banner [35].

   - **OPZIONE 1: Modificare uno script di inizializzazione GDM che mostri il messaggio di sicurezza in una finestra di dialogo.**

     La directory `/etc/gdm` contiene tre script di inizializzazione che mostrano il messaggio di sicurezza prima e dopo l'autenticazione.

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

     Per informazioni sulla modifica dei file di sistema in qualità di utente non-`root`, consultare la pagina man `pfedit`(1M).

   - **OPZIONE 2: 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 rivedere la guida per individuare il designer dell'interfaccia, fare clic su Development (Sviluppo) nel browser della guida di GNOME. La pagina man `glade-3`(1) è indicata in Applicazioni nelle pagine del manuale.

d. (Opzionale) Salvare una copia dell'interfaccia utente della finestra di login modificata.

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

2. Inserire un messaggio di sicurezza nella schermata di login del desktop dopo l'autenticazione utilizzando una delle tre opzioni riportate di seguito.

Il file che consente di creare una finestra di dialogo dopo l'autenticazione utilizza il messaggio di sicurezza del file `/etc/motd` riportato al Passo 2 della sezione Come inserire un messaggio di sicurezza nei file banner [35].

- **OPZIONE 1: inserire un messaggio di sicurezza sul desktop dopo l'autenticazione.**

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

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

- **OPZIONE 2: creare un desktop file che mostri il messaggio di sicurezza in una finestra aggiuntiva dopo l'autenticazione.**

```
# pfedit /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/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Per raggiungere l'area di lavoro dopo l'autenticazione nella finestra di login, è necessario che l'utente chiuda la finestra del messaggio di sicurezza. Per le opzioni del comando `zenity`, consultare la pagina man `zenity`(1).

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.

```
# pfedit /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.

TABELLA 2-2 Mappa delle attività per la sicurezza degli utenti

Attività	Descrizione	Per istruzioni
Impostare password complesse da modificare regolarmente.	Aumentare la complessità della password predefinita in ogni sistema.	Come impostare password più complesse [40]
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.	Come impostare un valore `umask` più restrittivo per gli utenti regolari [43].
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.	Come impostare un blocco dell'account per gli utenti regolari [41]
Preselezionare la classe di audit `cusa` per tutti gli utenti.	Fornire monitoraggio e registrazioni migliori delle potenziali minacce al sistema.	Come eseguire l'audit di eventi rilevanti oltre a Login/Logout [44]
Creare ruoli.	Distribuire attività amministrative discrete a più utenti affidabili affinché nessun utente possa danneggiare il sistema. È possibile utilizzare ruoli ARMOR predefiniti, creare ruoli personalizzati o estendere ARMOR con ruoli personalizzati.	«Managing User Accounts by Using the CLI» in «Managing User Accounts and User Environments in Oracle Solaris 11.2 » «Assigning Rights to Users» in «Securing Users and Processes in Oracle Solaris 11.2 »
Ridurre il numero di applicazioni desktop GNOME visibili.	Impedire agli utenti di utilizzare applicazioni desktop che possono influire sulla sicurezza.	Vedere Capitolo 11, «Disabling Features in the Oracle Solaris Desktop System»

Attività	Descrizione	Per istruzioni
		in «Oracle Solaris 11.2 Desktop Administrator's Guide ».
Limitare i privilegi di un utente.	Rimuovere i privilegi di base non necessari all'utente.	Come rimuovere privilegi di base non necessari all'utente [45]

▼ Come impostare password più complesse

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

Prima di cominciare È necessario diventare amministratore con autorizzazione `solaris.admin.edit/etc/default/passwd` assegnata. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

- **Utilizzare il comando `pfedit` per apportare le modifiche elencate di seguito nel file `/etc/default/passwd`.**

  a. **Imporre agli utenti la modifica delle password ogni quattro mesi, ma con una frequenza non superiore alle tre settimane.**

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  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 delle variabili che vincolano la creazione della password, consultare la pagina man `passwd`(1).
- Per i criteri della password in uso dopo l'installazione, vedere sezione chiamata «Accesso al sistema limitato e monitorato» [13].

▼ Come impostare 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 - I ruoli sono account condivisi. Non impostare blocchi dell'account per gli utenti che possono assumere determinati ruoli in quanto un utente bloccato può bloccare il ruolo stesso.

Prima di cominciare

Non impostare questa protezione a livello di sistema se quest'ultimo viene utilizzato per attività amministrative. Monitorare piuttosto il sistema amministrativo per rilevare eventuali utilizzi inusuali e garantirne la disponibilità per gli amministratori.

È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

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

Scegliere l'ambito del valore dell'attributo.

- **Impostare a livello di sistema.**

  Questa protezione si applica a qualsiasi utente che tenta di utilizzare il sistema.

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

- **Impostare a livello di utente.**

  Questa protezione si applica solo all'utente per il quale si esegue il comando. In presenza di più utenti, questa soluzione non è scalabile.

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

- **Creare e assegnare un profilo di diritti.**

  Questa protezione si applica a qualsiasi utente o sistema in cui si assegna questo profilo di diritti.

  a. **Creare il profilo di diritti.**

  ```
  # profiles -p shared-profile -S ldap
  shared-profile: set lock_after_retries=yes
  ...
  ```

  Per ulteriori informazioni sulla creazione dei profili di diritti, vedere «Creating Rights Profiles and Authorizations» in «Securing Users and Processes in Oracle Solaris 11.2 ».

  b. **Assegnare il profilo di diritti agli utenti o a livello di sistema.**

  In caso di più utenti che condividono un profilo di diritti, l'impostazione di questo valore in un profilo può rappresentare una soluzione scalabile.

  ```
  # usermod -P shared-profile username
  ```

  È anche possibile assegnare il profilo in base al sistema nel file `policy.conf`.

  ```
  # pfedit /etc/security/policy.conf
  ...
  #PROFS_GRANTED=Basic Solaris User
  PROFS_GRANTED=shared-profile,Basic Solaris User
  ```

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

   Scegliere l'ambito del valore dell'attributo.

   - **Impostare a livello di sistema.**

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

   - **Impostare a livello di utente.**

   ```
   # usermod -K lock_after_retries=3 username
   ```

   - **Creare e assegnare un profilo di diritti.**

     Eseguire le operazioni indicate al Passo 1.3 e creare un profilo di diritti che includa `lock_after_retries=3`.

Vedere anche

- Per informazioni sugli attributi di sicurezza di utente e ruolo, vedere Capitolo 8, «Reference for Oracle Solaris Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».
- Le pagine man selezionate includono `policy.conf`(4), `profiles`(1), `user_attr`(4) e `usermod`(1M).

▼ Come impostare un valore `umask` più restrittivo per gli utenti regolari

La utility `umask` i bit di autorizzazione dei file creati dall'utente. Se il valore predefinito `umask`, `022`, non è sufficientemente restrittivo, impostare una maschera più restrittiva come descritto di seguito.

Prima di cominciare

È necessario diventare amministratore autorizzato alla modifica dei file skeleton. Queste autorizzazioni vengono assegnate al ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Visualizzare i file di esempio forniti da Oracle Solaris per le impostazioni predefinite della shell utente.**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **Impostare il valore `umask` nei file `/etc/skel` che si intende assegnare agli utenti.**

   Scegliere uno dei valori seguenti:

   - `umask 026`: fornisce una protezione moderata del file

     (`751`) – `r` per i gruppi, `x` per altri
   - `umask 027` – Fornisce una protezione rigida

     (`750`) – `r` per i gruppi, nessun accesso per altri
   - `umask 077`: fornisce una protezione completa del file

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

Vedere anche

Per maggiori informazioni, vedere:

- «Managing User Accounts by Using the CLI» in «Managing User Accounts and User Environments in Oracle Solaris 11.2 »
- «Default umask Value» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »

- Le pagine man selezionate includono useradd(1M) e umask(1).

▼ Come eseguire l'audit di eventi rilevanti oltre a Login/Logout

Seguire questa procedura per effettuare l'audit dei comandi amministrativi, dell'accesso al sistema e di 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. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Eseguire l'audit di qualsiasi utilizzo di comandi privilegiati da parte di utenti a cui sono assegnati profili e ruoli con diritti amministrativi.**

   Aggiungere la classe di audit cusa alla maschera di preselezione.

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   Le classi di audit incluse nella metaclasse cusa sono elencate nel file /etc/security/audit_class.

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

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

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

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

   Nota - Questa opzione correlata ai criteri può risultare utile durante la risoluzione dei problemi.

Vedere anche

- Per informazioni sui criteri di audit, vedere «Audit Policy» in «Managing Auditing in Oracle Solaris 11.2 ».
- Per esempi sui flag di audit delle impostazioni, vedere «Configuring the Audit Service» in «Managing Auditing in Oracle Solaris 11.2 » e «Troubleshooting the Audit Service» in «Managing Auditing in Oracle Solaris 11.2 ».
- Pagina man auditconfig(1M)

Come rimuovere privilegi di base non necessari all'utente

In alcuni casi, alcuni privilegi di base possono essere rimossi da un set di base di un utente regolare o ospite. Ad esempio, è possibile che agli utenti di Sun Ray venga impedito di esaminare lo stato dei processi non di loro proprietà.

Prima di cominciare

È necessario utilizzare il ruolo `root`. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Elencare una definizione completa del set di privilegi di base.**

   I tre privilegi di base riportati di seguito sono probabili candidati per la rimozione.

```
% ppriv -lv basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
...
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. **Scegliere l'ambito della rimozione del privilegio.**

   - **Impostare a livello di sistema.**

     Questi privilegi vengono negati a tutti gli utenti che tentano di utilizzare il sistema. Questo metodo di rimozione dei privilegi può essere appropriato per un computer disponibile pubblicamente.

```
# pfedit /etc/security/policy.conf
...
#PRIV_DEFAULT=basic
PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
```

   - **Rimuovere i privilegi dai singoli utenti.**

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

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

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

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

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

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

- **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
  ```

- **Creare e assegnare un profilo di diritti.**

  Questa protezione si applica a qualsiasi utente o sistema in cui si assegna questo profilo di diritti.

  a. **Creare il profilo di diritti.**

  ```
  # profiles -p shared-profile -S ldap
  shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
  ...
  ```

  Per ulteriori informazioni sulla creazione dei profili di diritti, vedere «Creating Rights Profiles and Authorizations» in «Securing Users and Processes in Oracle Solaris 11.2 ».

  b. **Assegnare il profilo di diritti agli utenti o a livello di sistema.**

  In caso di più utenti che condividono un profilo di diritti, ad esempio Sun Ray o utenti remoti, l'impostazione di questo valore in un profilo può rappresentare una soluzione scalabile.

  ```
  # usermod -P shared-profile username
  ```

  È anche possibile assegnare il profilo in base al sistema nel file `policy.conf`.

  ```
  # pfedit /etc/security/policy.conf
  ...
  #PROFS_GRANTED=Basic Solaris User
  PROFS_GRANTED=shared-profile,Basic Solaris User
  ```

Vedere anche Per ulteriori informazioni, vedere Capitolo 1, «About Using Rights to Control Users and Processes» in «Securing Users and Processes in Oracle Solaris 11.2 » e consultare la pagina man `privileges`(5).

Protezione della rete

A questo punto, dovrebbero essere stati creati sia utenti in grado di assumere ruoli, sia i ruoli stessi.

Tra le attività di rete indicate di seguito, eseguire quelle che garantiscono maggiore sicurezza in base ai requisiti del sito. Queste attività di rete rafforzano i protocolli IP, ARP e TCP.

TABELLA 2-3 Mappa delle attività per la configurazione di rete

Attività	Descrizione	Per istruzioni
Disattivare il daemon di routing di rete.	Limitare l'accesso ai sistemi da parte di potenziali sniffer di rete.	«How to Disable the Network Routing Daemon» in «Securing the Network in Oracle Solaris 11.2 »
Impedire la diffusione di informazioni sulla topologia di rete.	Impedire il broadcast di pacchetti.	«How to Disable Broadcast Packet Forwarding» in «Securing the Network in Oracle Solaris 11.2 »
	Impedire di rispondere a richieste di eco di broadcast e di multicast.	«How to Disable Responses to Echo Requests» in «Securing the Network in Oracle Solaris 11.2 »
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.	«How to Set Strict Multihoming» in «Securing the Network in Oracle Solaris 11.2 »
Impedire attacchi Denial of Service (DoS) controllando il numero di connessioni di sistema incomplete.	Limitare il numero consentito di connessioni TCP incomplete per un listener TCP.	«How to Set Maximum Number of Incomplete TCP Connections» in «Securing the Network in Oracle Solaris 11.2 »
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.	«How to Set Maximum Number of Pending TCP Connections» in «Securing the Network in Oracle Solaris 11.2 »
Ripristinare i parametri di rete ai valori predefiniti di sicurezza.	Aumentare la sicurezza ridotta da precedenti interventi di amministrazione.	«How to Reset Network Parameters to Secure Values» in «Securing the Network in Oracle Solaris 11.2 »
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.	Come utilizzare i wrapper TCP
Configurare un firewall.	Utilizza la funzione di filtro IP per fornire un firewall.	Capitolo 4, «About IP Filter in Oracle Solaris» in «Securing the Network in Oracle Solaris 11.2 » Capitolo 5, «Configuring IP Filter» in «Securing the Network in Oracle Solaris 11.2 »
Configurare le connessioni di rete cifrate e autenticate.	Utilizza IPsec e IKE per proteggere le trasmissioni di rete tra nodi e reti configurati insieme a IPsec e IKE.	Capitolo 7, «Configuring IPsec» in «Securing the Network in Oracle Solaris 11.2 » Capitolo 9, «Configuring IKEv2» in «Securing the Network in Oracle Solaris 11.2 »

▼ Come utilizzare i wrapper TCP

I passaggi seguenti illustrano tre modi in cui vengono utilizzati o possono essere utilizzati i wrapper TCP in Oracle Solaris.

Prima di cominciare È necessario utilizzare il ruolo `root` per modificare un programma in modo che vengano utilizzati wrapper TCP.

1. **Non è necessario proteggere l'applicazione `sendmail` con wrapper TCP.**

   Per impostazione predefinita, tale applicazione viene protetta con wrapper TCP, come descritto in «Support for TCP Wrappers From Version 8.12 of sendmail» in «Managing sendmail Services in Oracle Solaris 11.2 ».

2. **Per abilitare i wrapper TCP per tutti i servizi `inetd`, vedere «How to Use TCP Wrappers to Control Access to TCP Services» in «Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2 ».**

3. **Proteggere il servizio di rete FTP con wrapper TCP.**

   a. **Seguire le istruzioni riportate nel modulo `/usr/share/doc/proftpd/modules/mod_wrap.html`.**

      Poiché questo modulo è dinamico, è necessario caricarlo per utilizzare wrapper TCP con FTP.

   b. **Caricare il modulo aggiungendo al file `proftpd.conf` le seguenti istruzioni:**

      ```
      # pfedit /etc/proftpd.conf
      <IfModule mod_dso.c>
          LoadModule mod_wrap.c
      </IfModule>
      ```

   c. **Riavviare il servizio FTP.**

      ```
      # svcadm restart svc:/network/ftp
      ```

Protezione dei file system

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

Le dimensioni del file system `tmpfs` possono aumentare senza alcun limite. Per impedire un attacco denial of service (DoS), vedere Come limitare le dimensioni del file system `tmpfs` [49].

Le attività seguenti consentono di configurare un limite delle dimensioni di tmpfs e forniscono una panoramica delle protezioni disponibili in ZFS, il file system predefinito in Oracle Solaris. Per ulteriori informazioni, vedere «Setting ZFS Quotas and Reservations» in «Managing ZFS File Systems in Oracle Solaris 11.2 » e la pagina man zfs(1M).

TABELLA 2-4 Mappa delle attività per la protezione dei file system

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 «Managing ZFS File Systems in Oracle Solaris 11.2 »
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 «Managing ZFS File Systems in Oracle Solaris 11.2 »
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 «Managing ZFS File Systems in Oracle Solaris 11.2 » «Examples of Encrypting ZFS File Systems» in «Managing ZFS File Systems in Oracle Solaris 11.2 »
Limitare le dimensioni del file system tmpfs.	Consente di impedire a un utente malintenzionato di creare file di grandi dimensioni in /tmp con il fine di rallentare il sistema.	Come limitare le dimensioni del file system tmpfs [49]

▼ Come limitare le dimensioni del file system tmpfs

Per impostazione predefinita, le dimensioni del file system tmpfs non sono limitate. Pertanto le dimensioni del file system tmpfs possono aumentare fino a riempire la memoria di sistema disponibile e il dispositivo swap. Poiché la directory /tmp viene utilizzata da tutte le applicazioni e gli utenti, un'applicazione può occupare tutta la memoria di sistema disponibile. Similarmente, un utente non dotato di privilegi e intenzioni non lecite potrebbe causare un rallentamento del sistema creando file di grandi dimensioni nella directory /tmp. Per evitare un impatto sulle prestazioni, è possibile limitare le dimensioni di ogni mount tmpfs.

È possibile provare diversi valori per raggiungere le migliori prestazioni di sistema.

Prima di cominciare

Per modificare il file vfstab, è necessario diventare amministratore con autorizzazione solaris.admin.edit/etc/vfstab assegnata. Per eseguire il reboot del sistema, è necessario disporre del profilo dei diritti di manutenzione e riparazione. Il ruolo root dispone di tutti questi diritti. Per ulteriori informazioni, vedere «Using Your Assigned Administrative Rights» in «Securing Users and Processes in Oracle Solaris 11.2 ».

1. **Stabilire la quantità di memoria sul sistema.**

Nota - Il sistema della serie SPARC T3 utilizzato per il seguente esempio è dotato di un'unità ssd per I/O più rapido e di otto dischi da 279,40 MB. Il sistema dispone di circa 500 GB di memoria.

```
% prtconf | head
System Configuration:  Oracle Corporation  sun4v
Memory size: 523776 Megabytes
System Peripherals (Software Nodes):

ORCL,SPARC-T3-4
scsi_vhci, instance #0
disk, instance #4
disk, instance #5
disk, instance #6
disk, instance #8
```

2. **Calcolare un limite di memoria per `tmpfs`.**

   In base alle dimensioni della memoria di sistema, potrebbe essere necessario calcolare un limite di memoria corrispondente a circa il 20% per volumi di grandi dimensioni e circa il 30% per sistemi più piccoli.

   Quindi, per un sistema di dimensioni inferiori, utilizzare `.30` come moltiplicatore,

   ```
   10240M x .30 ≈ 340M
   ```

   mentre per sistemi di dimensioni superiori, utilizzare `.20` come moltiplicatore.

   ```
   523776M x .20 ≈ 10475M
   ```

3. **Modificare la voce `swap` nel file `/etc/vfstab` con il limite delle dimensioni.**

   ```
   # pfedit /etc/vfstab
   #device     device       mount       FS      fsck    mount mount
   #to mount   to fsck      point       type    pass    at boot options
   #
   ...
   #swap       -            /tmp        tmpfs   -       yes     -
   swap        -            /tmp        tmpfs   -       yes     size=10400m
   /dev/zvol/dsk/rpool/swap   -      -  swap    -       no      -
   ```

4. **Eseguire il reboot del sistema.**

   ```
   # reboot
   ```

5. **Verificare che il limite per le dimensioni sia in vigore.**

   ```
   % mount -v
   swap on /system/volatile type tmpfs
   read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
   swap on /tmp type tmpfs
   ```

```
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. **Monitorare l'utilizzo della memoria e regolarlo in base ai requisiti del sito.**

   Il comando `df` può rivelarsi utile. Il comando `swap` fornisce le statistiche più utili.

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

   Per ulteriori informazioni, consultare le pagine man `tmpfs`(7FS), `mount_tmpfs`(1M), `df`(1M) e `swap`(1M).

Protezione e modifica dei file

Per impostazione predefinita, solo il ruolo `root` può modificare le autorizzazioni del file di sistema. I ruoli e gli utenti a cui viene assegnata l'autorizzazione `solaris.admin.edit/`*percorso-file-di-sistema* possono modificare tale *file-di-sistema*. Solo il ruolo `root` ha la possibilità di cercare tutti i file.

TABELLA 2-5 Mappa delle attività per la protezione e la modifica dei file

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.	Come impostare un valore `umask` più restrittivo per gli utenti regolari [43]
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)
Mantenere l'integrità del file di sistema.	Trovare i file rogueware mediante uno script o utilizzando file BART.	«How to Find Files With Special File Permissions» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »

Sicurezza dell'accesso al sistema e del relativo utilizzo

È possibile configurare le funzioni di sicurezza di Oracle Solaris per proteggere l'uso del sistema, incluse applicazioni e servizi nel sistema e in rete.

TABELLA 2-6 Mappa delle attività per la sicurezza dell'accesso al sistema e del relativo utilizzo

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 «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »
Accertarsi che i binari contrassegnati per la sequenza casuale del layout spazio di indirizzamento (ASLR, Address Space Layout Randomization) possano utilizzare ASLR.	Consente di abilitare ASLR per i binari contrassegnati.	Come verificare se ASLR è abilitato [33]
Configurare l'auditing.	Consente di personalizzare la configurazione del'audit per la copertura e l'integrità dei file.	sezione chiamata «Utilizzo del servizio di audit» [56]
Proteggere i file core che potrebbero contenere informazioni importanti.	Creare una directory con accesso limitato dedicata ai file core.	«Enabling File Paths» in «Troubleshooting System Administration Issues in Oracle Solaris 11.2 » «Administering Your Core File Specifications» in «Troubleshooting System Administration Issues in Oracle Solaris 11.2 »
Proteggere un server Web con Proxy SSL Kernel.	Il protocollo SSL (Secure Sockets Layer) consente di cifrare e accelerare le comunicazioni con il server Web.	Capitolo 3, «Web Servers and the Secure Sockets Layer Protocol» in «Securing the Network in Oracle Solaris 11.2 »
Creare zone che contengano applicazioni.	Le zone sono contenitori che consentono di isolare i processi. Possono isolare 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.	«Introduction to Oracle Solaris Zones »
Gestire risorse in zone.	Le zone forniscono strumenti per la gestione delle relative risorse di zona.	«Administering Resource Management in Oracle Solaris 11.2 »

Protezione di un servizio legacy con SMF

È possibile limitare la configurazione dell'applicazione a utenti o ruoli sicuri aggiungendo l'applicazione alla funzione SMF (Service Management Facility) di Oracle Solaris, quindi richiedendo i diritti di avvio, aggiornamento e arresto del servizio.

Per maggiori informazioni e procedure, vedere:

- «Locking Down Resources by Using Extended Privileges» in «Securing Users and Processes in Oracle Solaris 11.2 »
- 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), `svcbundle`(1M) e `svccfg`(1M).

Configurazione di una rete 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 3, «Planning for the Kerberos Service» in «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- Capitolo 4, «Configuring the Kerberos Service» in «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- Le pagine man selezionate includono `kadmin`(1M), `pam_krb5`(5) e `kclient`(1M).

Aggiunta di sicurezza multilivello con etichetta

Trusted Extensions estende la sicurezza di Oracle Solaris applicando un criterio di controllo dell'accesso obbligatorio (MAC, mandatory access control) basato sulle etichette. 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 `system/trusted` e `system/trusted/trusted-global-zone` sono sufficienti per un sistema senza monitor o un server che non richiede un desktop multilivello. Il pacchetto `system/trusted/trusted-extensions` fornisce l'ambiente desktop Oracle Solaris sicuro e multilivello.

Configurazione di Trusted Extensions

È necessario installare i pacchetti Trusted Extensions quindi configurare il sistema. Quando si installa il pacchetto `trusted-extensions`, il sistema può eseguire un desktop con uno schermo bitmap direttamente connesso, ad esempio un laptop o una 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 6, «About IP Security Architecture» in «Securing the Network in Oracle Solaris 11.2 »
- «Administration of Labeled IPsec» in «Trusted Extensions Configuration and Administration »
- «Configuring Labeled IPsec» in «Trusted Extensions Configuration and Administration »

♦ ♦ ♦ CAPITOLO 3

Manutenzione e monitoraggio della sicurezza di Oracle Solaris

Dopo l'installazione e la configurazione iniziali, è possibile mantenere e monitorare le impostazioni di sicurezza del sistema effettuando le operazioni elencate di seguito.

- Visionare regolarmente i record di audit
- Eseguire controlli di integrità del pacchetto e dei file
- Monitorare l'attività di rete
- Eseguire i controlli di conformità

Manutenzione e monitoraggio della sicurezza del sistema

Le attività indicate di seguito consentono di mantenere e monitorare l'accesso al sistema e ai dati e il relativo utilizzo, nonché la conformità ai requisiti di sicurezza del sito.

TABELLA 3-1 Mappa delle attività per la manutenzione e il monitoraggio del sistema

Attività	Descrizione	Per istruzioni
Verificare i pacchetti nel sistema.	Consente di accertarsi che i pacchetti, dopo un aggiornamento, siano identici ai pacchetti di origine.	Come verificare i pacchetti [33]
Verificare l'integrità dei file.	Dopo la configurazione, consente di confrontare i file manifesto BART a intervalli regolari per accertarsi che vengano modificati solo i file che devono essere modificati.	sezione chiamata «Verifica dell'integrità del file utilizzando BART» [56]
Rilevare i file rogueware.	Consente di rilevare l'utilizzo potenzialmente non consentito delle autorizzazioni `setuid` e `setgid` nei programmi.	«How to Find Files With Special File Permissions» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »
Visionare i log di audit a intervalli regolari.	Consente di rilevare eventuali accessi al sistema e relativi utilizzi insoliti.	sezione chiamata «Utilizzo del servizio di audit» [56]
Visionare i log di audit per individuare eventi di login e logout in tempo reale.	Consente di identificare tentativi di violazione a poca distanza dal momento in cui si verificano.	sezione chiamata «Monitoraggio dei record di audit in tempo reale» [57]

Attività	Descrizione	Per istruzioni
Eseguire i test di conformità.	Consente di valutare la conformità del sistema ai benchmark di sicurezza.	«Guida alla verifica della conformità in tema di sicurezza di Oracle Solaris 11.2 » e la pagina man `compliance`(1M)

Verifica dell'integrità del file utilizzando BART

BART è uno strumento di reporting e scansione dell'integrità dei file basato su regole che utilizza hash protetti da cifratura e metadati di file system per eseguire report delle modifiche.

Per maggiori informazioni e procedure, vedere:

- «About BART» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »
- «About Using BART» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »
- «BART Manifests, Rules Files, and Reports» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »

For specific instructions on tracking changes to installed systems, see «How to Compare Manifests for the Same System Over Time» in «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 ».

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 «Managing Auditing in Oracle Solaris 11.2 ». Per un elenco delle pagine man e dei relativi collegamenti, vedere «Audit Service Man Pages» in «Managing Auditing in Oracle Solaris 11.2 ».

Le procedure del servizio di audit elencate di seguito sono utili in molti ambienti sicuri.

- Creare ruoli separati per configurare e verificare l'auditing e avviare e arrestare il servizio di audit. Assegnare i ruoli agli utenti sicuri.

  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 ruoli o utilizzare i ruoli ARMOR predefiniti, vedere «Assigning Rights to Users» in «Securing Users and Processes in Oracle Solaris 11.2 ».
- Eseguire l'audit di tutti gli amministratori con classe di audit `cusa`.

  Gli eventi nella classe di audit `cusa` coprono le azioni amministrative che incidono sulle impostazioni di sicurezza del sistema. Per una descrizione, vedere il file `/etc/security/`

`audit_class`. Per la procedura, vedere Come eseguire l'audit di eventi rilevanti oltre a Login/Logout [44].

- Inviare record di audit a un server centrale.
  - Configurare l'auditing per il funzionamento con il server di audit remoto (ARS, Audit Remote Server).

    Vedere «How to Send Audit Files to a Remote Repository» in «Managing Auditing in Oracle Solaris 11.2 ».
  - Pianificare il trasferimento sicuro di file di audit completi verso un file system di revisione dell'audit in un pool ZFS separato.
- Monitorare i riepiloghi in formato testo relativi agli eventi di audit selezionati nella utility `syslog`.

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

  Vedere «How to Configure syslog Audit Logs» in «Managing Auditing in Oracle Solaris 11.2 ».
- 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`.

  Per alcuni esempi, vedere «How to Assign Audit Space for the Audit Trail» in «Managing Auditing in Oracle Solaris 11.2 ».
- 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 record di audit in tempo reale

Il plugin `audit__syslog` consente di registrare riepiloghi di eventi audit preselezionati. Per visualizzare i riepiloghi di audit in una finestra di terminale quando vengono generati, eseguire un comando simile al seguente:

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

Per configurare il log di audit, vedere «How to Configure syslog Audit Logs» in «Managing Auditing in Oracle Solaris 11.2 ».

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 «Managing Auditing in Oracle Solaris 11.2 »
- «Preventing Audit Trail Overflow» in «Managing Auditing in Oracle Solaris 11.2 »
- «Displaying Audit Trail Data» in «Managing Auditing in Oracle Solaris 11.2 »

♦ ♦ ♦ 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 sulla sicurezza delle release precedenti di Oracle Solaris includono alcune informazioni utili e altre obsolete.

Riferimenti alla sicurezza su Oracle Technology Network

I manuali e gli articoli elencati di seguito, disponibili sul sito Web Oracle Technology Network, contengono descrizioni correlate alla sicurezza nei sistemi Oracle Solaris 11.

- «Securing Systems and Attached Devices in Oracle Solaris 11.2 »
- «Securing Files and Verifying File Integrity in Oracle Solaris 11.2 »
- «Securing the Network in Oracle Solaris 11.2 »
- «Securing Users and Processes in Oracle Solaris 11.2 »
- «Managing Encryption and Certificates in Oracle Solaris 11.2 »
- «Managing Auditing in Oracle Solaris 11.2 »
- «Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 »
- «Managing Secure Shell Access in Oracle Solaris 11.2 »
- «Guida alla verifica della conformità in tema di sicurezza di Oracle Solaris 11.2 »
- «Using a FIPS 140 Enabled System in Oracle Solaris 11.2 »

Riferimenti alla sicurezza di Oracle Solaris in pubblicazioni di terze parti

I manuali elencati di seguito contengono descrizioni correlate alla sicurezza nei sistemi Oracle Solaris 11.

- *Benchmark per la configurazione di sicurezza per Solaris 11 11/11 Versione 1.0.0, 11 giugno 2012*

Questo benchmark di sicurezza viene pubblicato dal Center for Internet Security (CIS) http://cisecurity.org/ per la community di sicurezza. Il presente documento fornisce le impostazioni di sicurezza per il Sistema operativo Oracle Solaris. L'audience di destinazione include amministratori di sistema e applicazioni, specialisti della sicurezza, auditor, ingegneri di supporto, nonché installatori e sviluppatori incaricati di sviluppare, installare, valutare o fornire soluzioni di sicurezza per Oracle Solaris. Per ottenere una copia, visitare il sito CIS Security Benchmarks (http://benchmarks.cisecurity.org/).

- *Oracle Solaris 11 System Administration: The Complete Reference*. Michael Jang, Harry Foxwell, Christine Tran e Alan Formy-Duval. 2012. McGraw-Hill. ISBN 978007179042.

  Questo manuale fornisce informazioni sulla sicurezza di Oracle Solaris.

- *Oracle Solaris 11: First Look*. Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

  Questo manuale contiene un'introduzione a Oracle Solaris e alla relativa sicurezza destinata agli amministratori.

- *Oracle Solaris 11 System Administration*, BiIl Calkins. 2013. Prentice Hall. ISBN 9780133007114.

  Questo manuale contiene una descrizione delle nuove funzioni di Oracle Solaris, incluse le funzioni di sicurezza.