

Linee guida per la sicurezza di Oracle® Solaris 10

Il software e la relativa documentazione vengono distribuiti sulla base di specifiche condizioni di licenza che prevedono restrizioni relative all'uso e alla divulgazione e sono inoltre protetti dalle leggi vigenti sulla proprietà intellettuale. Ad eccezione di quanto espressamente consentito dal contratto di licenza o dalle disposizioni di legge, nessuna parte può essere utilizzata, copiata, riprodotta, tradotta, diffusa, modificata, concessa in licenza, trasmessa, distribuita, presentata, eseguita, pubblicata o visualizzata in alcuna forma o con alcun mezzo. La decodificazione, il disassemblaggio o la decompilazione del software sono vietati, salvo che per garantire l'interoperabilità nei casi espressamente previsti dalla legge.

Le informazioni contenute nella presente documentazione potranno essere soggette a modifiche senza preavviso. Non si garantisce che la presente documentazione sia priva di errori. Qualora l'utente riscontrasse dei problemi, è pregato di segnalarli per iscritto a Oracle.

Qualora il software o la relativa documentazione vengano forniti al Governo degli Stati Uniti o a chiunque li abbia in licenza per conto del Governo degli Stati Uniti, sarà applicabile la clausola riportata di seguito:

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Il presente software o hardware è stato sviluppato per un uso generico in varie applicazioni di gestione delle informazioni. Non è stato sviluppato né concepito per l'uso in campi intrinsecamente pericolosi, incluse le applicazioni che implicano un rischio di lesioni personali. Qualora il software o l'hardware venga utilizzato per impieghi pericolosi, è responsabilità dell'utente adottare tutte le necessarie misure di emergenza, backup e di altro tipo per garantirne la massima sicurezza di utilizzo. Oracle Corporation e le sue consociate declinano ogni responsabilità per eventuali danni causati dall'uso del software o dell'hardware per impieghi pericolosi.

Oracle e Java sono marchi registrati di Oracle e/o delle relative consociate. Altri nomi possono essere marchi dei rispettivi proprietari.

Intel e Intel Xeon sono marchi o marchi registrati di Intel Corporation. Tutti i marchi SPARC sono utilizzati in base alla relativa licenza e sono marchi o marchi registrati di SPARC International, Inc. AMD, Opteron, il logo AMD e il logo AMD Opteron sono marchi o marchi registrati di Advanced Micro Devices. UNIX è un marchio registrato di The Open Group.

Il software o l'hardware e la documentazione possono includere informazioni su contenuti, prodotti e servizi di terze parti o collegamenti agli stessi. Oracle Corporation e le sue consociate declinano ogni responsabilità ed escludono espressamente qualsiasi tipo di garanzia relativa a contenuti, prodotti e servizi di terze parti. Oracle Corporation e le sue consociate non potranno quindi essere ritenute responsabili per qualsiasi perdita, costo o danno causato dall'accesso a contenuti, prodotti o servizi di terze parti o dall'utilizzo degli stessi.

Indice

Prefazione5

1 Linee guida per la sicurezza di Oracle Solaris 107

 Riferimenti per la protezione avanzata del sistema Oracle Solaris 107

 Ulteriori riferimenti per la sicurezza per Oracle Solaris 108

Prefazione

Questa guida include rimandi a e descrizioni in merito alle linee guida di sicurezza del Sistema operativo Oracle Solaris (Sistema operativo Oracle Solaris). I riferimenti alla protezione avanzata di sistema descrivono le modalità di impostazione della protezione avanzata per i sistemi Oracle Solaris 10 e di utilizzo delle funzioni di sicurezza di Oracle Solaris per proteggere i dati e le applicazioni. È possibile adattare le raccomandazioni riportate in questi riferimenti ai criteri di sicurezza dei singoli siti.

Questa guida fornisce inoltre indicazioni in merito alle informazioni generali sulla sicurezza di Oracle Solaris nonché white paper che forniscono informazioni relative alle implementazioni più comuni.

Audience

Il documento *Linee guida per la sicurezza di Oracle Solaris 10* è destinato agli amministratori della sicurezza e ad altri amministratori incaricati delle seguenti operazioni:

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

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

Accesso al supporto Oracle

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

Convenzioni tipografiche

La tabella seguente descrive le convenzioni tipografiche usate nel manuale.

TABELLA P-1 Convenzioni tipografiche

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

Prompt della shell negli esempi di comando

Nella tabella seguente sono riportati i prompt di sistema UNIX e superutente per le shell incluse nel sistema operativo Oracle Solaris. Negli esempi dei comandi, il prompt della shell indica se il comando dovrebbe essere eseguito da un utente regolare o con privilegi.

TABELLA P-2 Prompt della shell

Shell	Prompt
Shell Bash, shell Korn e shell Bourne	\$
Shell Bash, shell Korn e shell Bourne per superutenti	#
C shell	machine_name%
C shell, superutente	machine_name#

Linee guida per la sicurezza di Oracle Solaris 10

Oracle Solaris 10 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 le modalità di accesso ai file da parte degli utenti, il tipo di protezione dei database di sistema e l'utilizzo delle risorse, Oracle Solaris 10 è in grado di soddisfare esigenze di sicurezza di qualsiasi tipo. Mentre i sistemi operativi tradizionali possono contenere punti deboli nella protezione, la flessibilità di Oracle Solaris 10 consente di soddisfare una gran varietà di obiettivi relativi alla sicurezza, dai server aziendali ai client per desktop.

Riferimenti per la protezione avanzata del sistema Oracle Solaris 10

I seguenti due documenti descrivono come impostare la protezione avanzata per Oracle Solaris, come utilizzare le funzioni di sicurezza per configurare i sistemi per operare in sicurezza durante l'aggiunta di applicazioni e utenti e come utilizzare funzioni di sicurezza specifiche per proteggere le applicazioni basate sulla rete. Ogni titolo è accompagnato da una breve descrizione del documento.

- *CIS Solaris 10 Benchmark v5.0.0* (<http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500>), 9 luglio 2010.

Un altro nome di questo documento è *Benchmark per la configurazione di sicurezza per Solaris 10 11/06 tramite 10/09*. Questo benchmark è il risultato di oltre sette anni di lavoro di molti collaboratori, tra cui Sun Microsystems, Defense Information Systems Agency (DISA), Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), National Security Agency (NSA) e diverse altre aziende, istituzioni accademiche e individui. Questo documento riporta una serie di linee guida di base relative alla protezione avanzata concordate da Sun, CIS, NSA e DISA.

- *An Overview of Oracle Solaris 10 Security Controls* (<http://www.oracle.com/technetwork/server-storage/solaris/documentation/o11-076-s10-cis-appendix-487450.pdf>), Glenn Brunette, settembre 2011

Questa appendice al documento *Benchmark per la configurazione di sicurezza per Solaris 10 11/06 tramite 10/09* è incentrata sui controlli di sicurezza contenuti in Oracle Solaris 10 che non rientrano nella protezione avanzata del sistema e nella convalida della configurazione di sicurezza. Questa appendice fornisce una panoramica completa delle funzioni di sicurezza e delle funzionalità di Oracle Solaris 10 e offre consigli specifici, ove possibile.

Ulteriori riferimenti per la sicurezza per Oracle Solaris 10

Le seguenti guide e articoli fungono da supplemento alle linee guida relative alla protezione avanzata di sistema riportate nella sezione precedente:

- *System Administration Guide: Security Services*

Questa guida per la sicurezza è stata pubblicata dagli amministratori di Oracle for Oracle Solaris 10 e descrive le funzioni di sicurezza del sistema operativo Oracle Solaris 10 nonché il loro utilizzo per la configurazione dei sistemi. A differenza del documento *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*, questa guida non è stata sviluppata come documento relativo a protezione avanzata di sistema o best practice.

- *Solaris 10 Security Essentials*, Sun engineers, 2009. ISBN 978-0137012336

In questo manuale, gli ingegneri e tecnici di Solaris descrivono 12 tecnologie di sicurezza Solaris accompagnandole con esempi. A differenza del documento *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*, questa guida non è stata sviluppata come documento relativo a protezione avanzata di sistema o best practice.

- *Using Oracle® Solaris 10 to Overcome Security Challenges* (<http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf>), agosto 2010.

Questo white paper di Oracle è rivolto alle organizzazioni che richiedono funzioni di sicurezza di sistema complete. I dipartimenti IT che necessitano di una soluzione efficace per quanto riguarda la sicurezza dei computer possono utilizzare le funzioni di sicurezza uniche e qualitative di Oracle Solaris 10 per proteggere la propria attività dalle potenziali minacce, il tutto nel pieno rispetto dei requisiti aziendali e normativi, per affrontare senza problemi qualsiasi tipo di sfida di sicurezza. Questo white paper fornisce una descrizione estremamente dettagliata delle funzionalità di sicurezza di Oracle Solaris e non è stato sviluppato come documento relativo a protezione avanzata o best practice.