

Guida per la sicurezza dei server SPARC e Netra SPARC S7-2 Series

ORACLE®

N. di parte: E77186-01
Giugno 2016

Guida per la sicurezza dei server SPARC e Netra SPARC S7-2 Series

Part No: E77186-01

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Référence: E77186-01

Copyright © 2016, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

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.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Indice

Informazioni sulla sicurezza dei componenti hardware	7
Limitazioni di accesso	7
Numeri di serie	8
Unità disco rigido	8
Informazioni sulla sicurezza dei componenti software	9
▼ Prevenzione dell'accesso non autorizzato (Sistema operativo Oracle Solaris)	9
▼ Prevenzione dell'accesso non autorizzato (Oracle ILOM)	9
▼ Prevenzione dell'accesso non autorizzato (server Oracle VM for SPARC)	10
Limitazione dell'accesso (OpenBoot)	10
▼ Implementazione della protezione mediante password	10
▼ Abilitazione della modalità di sicurezza	11
▼ Disabilitazione della modalità di sicurezza	11
▼ Controllo dei login non riusciti	12
▼ Specifica di un banner di accensione	12
Firmware di Oracle System	12
Boot WAN sicuro	13
Boot verificato	13

Informazioni sulla sicurezza dei componenti hardware

L'isolamento fisico e il controllo dell'accesso costituiscono gli elementi di base per la creazione dell'architettura di sicurezza. L'installazione in un ambiente sicuro protegge il server fisico dagli accessi non autorizzati. In modo analogo, la registrazione di tutti i numeri di serie aiuta a evitare i rischi di furto, rivendita o inerenti alla supply chain (ovvero l'inserimento di componenti falsificati o che non funzionano correttamente nella supply chain dell'organizzazione alla quale si appartiene).

Nelle sezioni indicate vengono fornite le linee guida generali relative alla sicurezza dei componenti hardware per i server SPARC e Netra SPARC S7-2 Series.

- [sezione chiamata «Limitazioni di accesso» \[7\]](#)
- [sezione chiamata «Numeri di serie» \[8\]](#)
- [sezione chiamata «Unità disco rigido» \[8\]](#)

Limitazioni di accesso

- Installare il server e le apparecchiature correlate in una stanza chiusa a chiave con accesso limitato.
- Se le apparecchiature sono installate in un rack dotato di sportello, chiudere sempre lo sportello finché non sarà necessario effettuare un intervento sui componenti contenuti nel rack. La chiusura degli sportelli limita anche l'accesso ai dispositivi hot plug o hot swap.
- Conservare le unità sostituibili sul campo (FRU, Field-Replaceable Units) o le unità sostituibili dall'utente (CRU, Customer-Replaceable Unit) di riserva in un armadio chiuso a chiave. Consentire l'accesso all'armadio chiuso a chiave solo al personale autorizzato.
- Verificare periodicamente lo stato e l'integrità delle serrature nel rack e dell'armadio dei ricambi per evitare o rilevare eventuali tentativi di manomissione o sportelli lasciati inavvertitamente aperti.
- Conservare le chiavi dell'armadio in un luogo sicuro con accesso limitato.
- Limitare l'accesso alle console USB. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU, Power Distribution Unit) e gli switch di rete possono essere dotati di connessioni USB. L'accesso fisico è il metodo di accesso a un componente più sicuro, in quanto non è soggetto ad attacchi che sfruttano la rete.

- Connettere la console a un dispositivo KVM esterno per abilitare l'accesso remoto alla console. I dispositivi KVM supportano spesso l'autenticazione basata su due fattori: il controllo dell'accesso centralizzato e l'audit. Per ulteriori informazioni sulle istruzioni di sicurezza e sulle procedure ottimali per i dispositivi KVM, consultare la documentazione fornita con il dispositivo KVM in uso.

Numeri di serie

- Tenere traccia dei numeri di serie di tutti i dispositivi hardware.
- Contrassegnare per la sicurezza tutti gli elementi significativi dell'hardware del computer, ad esempio i pezzi di ricambio. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.
- Conservare le chiavi di attivazione hardware e le licenze in un luogo sicuro che possa essere raggiunto con facilità dal responsabile del sistema in caso di emergenza. I documenti stampati potrebbero essere l'unica prova di proprietà.

I reader wireless RFID (Radio Frequency Identification) consentono di semplificare ulteriormente la registrazione degli asset. Il white paper Oracle relativo alla *registrazione degli asset del sistema Oracle Sun mediante RFID* è disponibile all'indirizzo:

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/011-001-rfid-oracle-214567.pdf>

Unità disco rigido

Le unità disco rigido vengono spesso utilizzate per memorizzare informazioni riservate. Per proteggere queste informazioni dalla diffusione non autorizzata, ripulire le unità disco rigido prima di riutilizzarle, decommissionarle o disfarsene.

- Utilizzare gli strumenti di cancellazione del disco, come il comando Oracle Solaris `format (1M)`, per cancellare completamente tutti i dati dall'unità disco rigido.
- Le organizzazioni sono tenute a fare riferimento ai criteri di protezione dei dati esistenti per determinare il metodo più appropriato per ripulire le unità disco fisso.
- Se necessario, usufruire del servizio di conservazione dei dispositivi e dei dati del cliente di Oracle

<http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf>

Informazioni sulla sicurezza dei componenti software

La sicurezza dell'hardware viene garantita principalmente tramite l'implementazione di misure software. Nelle sezioni indicate vengono fornite le linee guida generali relative alla sicurezza dei componenti software per i server SPARC e Netra SPARC S7-2 Series.

- [Prevenzione dell'accesso non autorizzato \(Sistema operativo Oracle Solaris\) \[9\]](#)
- [Prevenzione dell'accesso non autorizzato \(Oracle ILOM\) \[9\]](#)
- [Prevenzione dell'accesso non autorizzato \(server Oracle VM for SPARC\) \[10\]](#)
- [sezione chiamata «Limitazione dell'accesso \(OpenBoot\)» \[10\]](#)
- [sezione chiamata «Firmware di Oracle System» \[12\]](#)
- [sezione chiamata «Boot WAN sicuro» \[13\]](#)
- [sezione chiamata «Boot verificato» \[13\]](#)

▼ Prevenzione dell'accesso non autorizzato (Sistema operativo Oracle Solaris)

- **Utilizzare i comandi del sistema operativo Oracle Solaris per limitare l'accesso al software Oracle Solaris, rafforzare il sistema operativo, utilizzare le funzioni di sicurezza e proteggere le applicazioni.**

Le *Linee guida sulla sicurezza di Oracle Solaris* per la versione del sistema operativo in uso sono disponibili ai seguenti indirizzi:

- <http://www.oracle.com/goto/solaris11/docs>
- <http://www.oracle.com/goto/solaris10/docs>

▼ Prevenzione dell'accesso non autorizzato (Oracle ILOM)

- **Utilizzare i comandi Oracle ILOM per limitare l'accesso al software Oracle ILOM, modificare la password impostata in fabbrica, limitare l'utilizzo dell'account superutente root e proteggere la rete privata presso il processore di servizi.**

La *Guida per la sicurezza di Oracle ILOM* è disponibile al seguente indirizzo:

- <http://www.oracle.com/goto/ilom/docs>

▼ Prevenzione dell'accesso non autorizzato (server Oracle VM for SPARC)

- **Utilizzare i comandi di Oracle VM for SPARC per limitare l'accesso al software Oracle VM for SPARC.**

La *Guida per la sicurezza di Oracle VM for SPARC* è disponibile al seguente indirizzo:

<http://www.oracle.com/goto/vm-sparc/docs>

Limitazione dell'accesso (OpenBoot)

In questi argomenti viene descritto come limitare l'accesso al prompt OpenBoot.

- [Implementazione della protezione mediante password \[10\]](#)
- [Abilitazione della modalità di sicurezza \[11\]](#)
- [Disabilitazione della modalità di sicurezza \[11\]](#)
- [Controllo dei login non riusciti \[12\]](#)
- [Specificazione di un banner di accensione \[12\]](#)

Per informazioni sull'impostazione delle variabili di sicurezza OpenBoot, fare riferimento alla documentazione OpenBoot disponibile all'indirizzo:

<http://www.oracle.com/goto/openboot/docs>

▼ Implementazione della protezione mediante password

- **Se non si è ancora impostata una password, eseguire questa operazione.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

La password può essere composta da 1-8 caratteri. Se si immettono più di otto caratteri, verranno utilizzati solo i primi otto. Sono accettati tutti i caratteri stampabili. I caratteri di controllo non sono accettati.

Nota - L'impostazione della password su zero caratteri disattiva la sicurezza ed equivale all'impostazione dei parametri `security-mode` su `none`. L'impostazione, tuttavia, non viene modificata.

▼ Abilitazione della modalità di sicurezza

1. Impostare il parametro `security-mode` su `full` o `command`.

Quando il parametro è impostato su `full`, è necessaria una password per eseguire qualsiasi azione, incluse le operazioni normali come il `boot`. Quando il parametro è impostato su `command`, la password non è necessaria per i comandi `boot` e `go`, ma è necessaria per tutti gli altri comandi. Per motivi correlati alla continuità operativa, si consiglia di impostare il parametro `security-mode` su `command`, come mostrato nell'esempio seguente.

```
{0} ok setenv security-mode command
{0} ok
```

2. Ottenere il prompt della modalità di sicurezza.

Una volta impostata la modalità di sicurezza come descritto in precedenza, esistono due modi per ottenere il prompt di tale modalità.

■ Utilizzare i comandi `logout` e `login`.

```
{0} ok logout
Type boot, go (continue), or login (command mode)
>
> login
Firmware Password: password
Type help for more information
{0} ok
```

Per uscire dalla modalità di sicurezza, utilizzare i comandi `logout` e `login`, come indicato nell'esempio.

■ Utilizzare il comando `reset-all`.

```
{0} ok reset-all
```

Questo comando determina la reimpostazione del sistema. Quando il sistema è di nuovo attivo, OpenBoot visualizza il prompt della modalità di sicurezza. Per eseguire di nuovo il `login` al prompt del comando (o il `logout` dalla modalità di sicurezza), utilizzare i comandi `logout` e `login`, quindi immettere la password, come descritto in precedenza.

▼ Disabilitazione della modalità di sicurezza

1. Impostare il parametro `security-mode` su `none`.

```
{0} ok setenv security-mode none
```

2. Impostare la password su zero caratteri digitando `Return` dopo entrambi i prompt della password.

▼ Controllo dei login non riusciti

1. **Per determinare se qualcuno ha tentato di accedere all'ambiente OpenBoot senza riuscirci, utilizzare il parametro `security-#badlogins`, come mostrato nell'esempio seguente.**

```
{0} ok printenv security-#badlogins
```

Se questo comando restituisce un valore maggiore di zero, è stato registrato un tentativo di accesso non riuscito all'ambiente OpenBoot.

2. **Reimpostare il parametro digitando questo comando.**

```
{0} ok setenv security-#badlogins 0
```

▼ Specifica di un banner di accensione

Sebbene non si tratti di un controllo di prevenzione o rilevamento diretto, è possibile utilizzare un banner per i motivi elencati di seguito.

- Trasferire la proprietà.
 - Avvisare gli utenti dell'uso accettabile del server.
 - Indicare che l'accesso o le modifiche ai parametri di OpenBoot sono limitati al personale autorizzato.
- **Utilizzare i comandi riportati di seguito per abilitare un messaggio di avvertenza personalizzato.**

```
{0} ok setenv oem-banner banner-message  
{0} ok setenv oem-banner? true
```

Il messaggio del banner può essere composto da un massimo di 68 caratteri. Sono accettati tutti i caratteri stampabili.

Firmware di Oracle System

Il firmware di Oracle System utilizza un processo di aggiornamento controllato per impedire le modifiche non autorizzate. Solo il superutente o un utente autenticato con l'autorizzazione appropriata può utilizzare il processo di aggiornamento.

Per informazioni su come ottenere gli aggiornamenti o le patch più recenti, fare riferimento alle note di prodotto per il server in uso.

Boot WAN sicuro

Il metodo di installazione boot WAN supporta diversi livelli di sicurezza. È possibile usare una combinazione delle funzioni di sicurezza supportate dal metodo boot WAN per adattarle alle esigenze della rete in uso. Le configurazioni più sicure hanno maggiori esigenze di amministrazione, ma proteggono in modo più efficace i dati del sistema.

- Per il sistema operativo Oracle Solaris 10, consultare le informazioni sulla configurazione sicura per l'installazione boot WAN in *Guida all'installazione di Oracle Solaris: installazione di rete*.
- Per il sistema operativo Oracle Solaris 11, fare riferimento a *Protezione della rete in Oracle Solaris 11.3*.

Boot verificato

Il boot verificato può essere utilizzato per verificare i blocchi di boot del sistema e i moduli kernel di Oracle Solaris prima che questi vengano caricati nel sistema. Utilizzare Oracle ILOM per abilitare il boot verificato e per specificare la modalità di risposta del sistema in caso di verifica non riuscita. L'abilitazione del boot verificato può impedire che vengano apportate modifiche dannose ai blocchi di boot del sistema o ai moduli kernel di Oracle Solaris.

Fare riferimento alle informazioni relative alla configurazione delle proprietà del boot verificato SPARC nella *guida per gli amministratori relativa a configurazione e manutenzione di Oracle ILOM*.

