

Server SPARC M5-32 e SPARC M6-32

Guida per la sicurezza

Copyright © 2014 Oracle e/o relative consociate. Tutti i diritti riservati.

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

1. Informazioni sulla sicurezza dei componenti hardware	5
Limitazioni di accesso	5
Numeri di serie	6
Unità disco rigido	6
2. Informazioni sulla sicurezza dei componenti software	7
▼ Prevenzione dell'accesso non autorizzato (Sistema operativo Oracle Solaris)	7
▼ Prevenzione dell'accesso non autorizzato (Oracle ILOM)	7
▼ Prevenzione dell'accesso non autorizzato (server Oracle VM for SPARC)	8
Limitazione dell'accesso (OpenBoot)	8
▼ Implementazione della protezione mediante password (OpenBoot)	8
▼ Controllo dei login non riusciti (OpenBoot)	9
▼ Specifica di un banner di accensione (OpenBoot)	9
Firmware Oracle System	9
Boot WAN sicuro	9

1

... C a p i t o l o 1

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).

In questo capitolo vengono fornite le linee guida generali relative alla sicurezza dei componenti hardware per i server SPARC M5-32 e M6-32.

Il capitolo include le sezioni riportate di seguito.

- [sezione chiamata «Limitazioni di accesso» \[5\]](#)
- [sezione chiamata «Numeri di serie» \[6\]](#)
- [sezione chiamata «Unità disco rigido» \[6\]](#)

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 con collegamento o swapping a caldo.
- Conservare le unità di ricambio sostituibili in loco (FRU) o le unità sostituibili dal cliente (CRU) in un cabinet chiuso. Limitare l'accesso al cabinet chiuso al personale autorizzato.
- Verificare periodicamente lo stato e l'integrità delle serrature nel rack e del cabinet dei ricambi per evitare, o rilevare, eventuali tentativi di manomissione o sportelli lasciati aperti.
- Conservare le chiavi del cabinet 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 i commutatori 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 la sola prova della proprietà del materiale.

I reader wireless RFID consentono di semplificare ulteriormente la registrazione degli asset. Per ulteriori informazioni, leggere il documento relativo al *tracciamento degli asset del sistema Oracle Sun mediante RFID* disponibile all'indirizzo:

<http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-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, è necessario ripulire le unità disco rigido prima di riutilizzarle, decommissionarle o disfarsene.

- Utilizzare gli strumenti di cancellazione del disco, quale il comando Oracle Solaris **format** (1M), per cancellare completamente tutti i dati dall'unità disco rigido. In alternativa, è possibile utilizzare strumenti di degaussing fisico, se appropriati e disponibili.
- In alcuni casi, le informazioni contenute nelle unità disco rigido hanno un livello di riservatezza talmente elevato da far considerare la distruzione fisica mediante polverizzazione o incinerazione come unico metodo di ripulitura.

Si consiglia alle organizzazioni di far riferimento ai criteri di protezione dei dati esistenti per determinare il metodo più appropriato per ripulire le unità disco fisso.



Attenzione

Gli strumenti di cancellazione del disco potrebbero non essere in grado di eliminare alcuni dati contenuti nelle unità disco fisso più recenti, in special modo le unità SSD, a causa delle modalità di gestione dell'accesso ai dati che le contraddistinguono.

2

... C a p i t o l o 2

Informazioni sulla sicurezza dei componenti software

La sicurezza dei componenti hardware viene implementata principalmente mediante misure software. In questo capitolo vengono fornite le linee guida generali relative alla sicurezza dei componenti software per i server SPARC M5-32 e M6-32.

Il capitolo include le sezioni riportate di seguito.

- [Prevenzione dell'accesso non autorizzato \(Sistema operativo Oracle Solaris\) \[7\]](#)
- [Prevenzione dell'accesso non autorizzato \(Oracle ILOM\) \[7\]](#)
- [Prevenzione dell'accesso non autorizzato \(server Oracle VM for SPARC\) \[8\]](#)
- [sezione chiamata «Limitazione dell'accesso \(OpenBoot\)» \[8\]](#)
- [sezione chiamata «Firmware Oracle System» \[9\]](#)
- [sezione chiamata «Boot WAN sicuro» \[9\]](#)

▼ 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.
Il documento con le istruzioni di sicurezza Oracle Solaris per la versione del sistema operativo in uso è disponibile a questo indirizzo:
<http://www.oracle.com/goto/Solaris11/docs>
<http://www.oracle.com/goto/Solaris10/docs>

▼ Prevenzione dell'accesso non autorizzato (Oracle ILOM)

1. Utilizzare i comandi Oracle ILOM per limitare l'accesso degli utenti 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 a questo indirizzo:
<http://www.oracle.com/goto/ILOM/docs>
2. Utilizzare i comandi Oracle ILOM specifici della piattaforma per proteggere i singoli domini mediante la creazione di account utente con ruoli che si applicano a un dominio fisico specifico.

Quando si assegnano i ruoli utente a un dominio fisico, le capacità del dominio interessato riflettono quelle dei ruoli utente assegnati per la piattaforma, ma sono limitate ai comandi eseguiti sul componente specificato.



Nota

Solo i ruoli utente amministratore (**a**), console (**c**) e reimpostazione (**r**) possono essere assegnati per i singoli domini fisici.

Il manuale *SPARC M5-32 and SPARC M6-32 Servers Administration Guide* è disponibile a questo indirizzo:

<http://www.oracle.com/goto/M6-32/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.
Il manuale *Guida per la sicurezza di Oracle VM for SPARC* è disponibile a questo 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 \(OpenBoot\) \[8\]](#)
- [Controllo dei login non riusciti \(OpenBoot\) \[9\]](#)
- [Specifica di un banner di accensione \(OpenBoot\) \[9\]](#)

Informazioni correlate

- Per informazioni sull'impostazione delle variabili di sicurezza OpenBoot, fare riferimento al manuale *OpenBoot 4.x Command Reference Manual* disponibile all'indirizzo: <http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069>

▼ Implementazione della protezione mediante password (OpenBoot)

- Impostare il parametro `security-mode` su **full** o **command**.
Quando il parametro è impostato su **full**, per l'esecuzione di qualsiasi azione, comprese le operazioni normali quale l'avvio, è necessario fornire la password. 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 relativi alla continuità operativa, si consiglia di impostare il parametro `security-mode` su **command**, come mostrato nell'esempio seguente.

```
ok password
ok setenv security-mode command
ok password
```

▼ Controllo dei login non riusciti (OpenBoot)

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

```
ok printenv security-#badlogins
```

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

2. Reimpostare il parametro **security-#badlogins** digitando il comando riportato di seguito.

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

▼ Specifica di un banner di accensione (OpenBoot)

- Utilizzare i comando riportati di seguito per abilitare un messaggio di avvertenza personalizzato.

```
ok setenv oem-banner banner-message  
ok setenv oem-banner? true
```

Firmware 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 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 adattare 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, vedere la sezione " 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 11.1*.

<http://www.oracle.com/goto/Solaris10/docs>

<http://www.oracle.com/goto/Solaris11/docs>

