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

N. di parte: E77186-01
Giugno 2016

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

Part No: E77186-01

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

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

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/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, 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)

- **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.

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*.