Guida per la sicurezza dei server SPARC M8 e SPARC M7

N. di parte: E63782-02
Settembre 2017

N. di parte: E63782-02

Accessibilità alla documentazione

Per informazioni sull'impegno di Oracle per l'accessibilità, visitare il sito Oracle Accessibility Program all'indirizzo: http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso il portale Oracle My Oracle Support. Per tutte le necessarie informazioni, si prega di visitare il sito http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oppure http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs per clienti non udenti.

Référence: E63782-02

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 dagli accessi non autorizzati. Allo stesso modo, la registrazione di tutti i numeri di serie aiuta a evitare l'uso di componenti hardware non autorizzati.

In queste sezioni vengono fornite linee guida generali relative alla sicurezza dei componenti hardware per i server.

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

Limitazioni di accesso

- Installare server e apparecchiature correlate in una stanza 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 tutte le parti di ricambio 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

Per impedire l'uso di componenti hardware non autorizzati, registrare attentamente tutti i numeri di serie quando si ricevono e si controllano i componenti. Prima di installare o utilizzare qualsiasi componente, verificarne l'autenticità confrontandone il numero di serie con quello registrato al momento della ricezione. Attenersi alle procedure indicate di seguito per proteggere i componenti hardware.

- Tenere traccia dei numeri di serie di tutti i componenti 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 licenze e le chiavi di attivazione dell'hardware in un luogo sicuro e facilmente accessibile ai system manager in caso di emergenze relative al sistema. I documenti stampati potrebbero essere la sola prova della proprietà del materiale.

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 (unità disco rigido e SSD) 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, quale il comando Oracle Solaris `format` (1M), per cancellare completamente tutti i dati dall'unità disco rigido.
- Le organizzazioni devono far 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 dei componenti hardware viene implementata principalmente mediante misure software. In queste sezioni vengono fornite linee guida generali relative alla sicurezza dei componenti software per i server.

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 *Oracle Solaris Security Guidelines* per le versione in uso è disponibile all'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 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. **Se possibile, 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 *Guida all'amministrazione dei server SPARC M8 e SPARC M7* è disponibile a questo indirizzo:

   `http://docs.oracle.com/cd/E55211_01/`

▼ 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 (OBP)

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

Per informazioni sull'impostazione delle variabili di sicurezza OpenBoot, fare riferimento alla documentazione 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 un massimo di otto caratteri. Se si immettono più di otto caratteri, verranno utilizzati solo i primi otto. Sono consentiti tutti i caratteri stampabili. I caratteri di controllo non sono consentiti.

Nota - L'impostazione della password su zero caratteri disattiva la sicurezza ed equivale all'impostazione del parametro `security-mode` su `none`. Non modifica tuttavia l'impostazione.

Abilitazione della modalità sicura

1. **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 come il `boot`, 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 di 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. **Visualizzare il prompt della modalità sicura.**

   Dopo aver impostato la modalità sicura come descritto in precedenza, è possibile visualizzare il prompt della modalità sicura in uno dei due modi indicati di seguito.

   - **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 sicura, utilizzare i nomi `logout` e `login`.

- **Utilizzare il comando `reset-all`.**

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

  Questo comando reimposta il sistema. Quando il sistema viene ripristinato, OpenBoot visualizza il prompt della modalità sicura. Per eseguire di nuovo il login al prompt di comando (o eseguire il logout dalla modalità sicura), utilizzare i nomi `logout` e `login`, quindi immettere la password, come descritto in precedenza.

Disabilitazione della modalità sicura

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

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

2. **Impostare la password sulla lunghezza zero digitando Return dopo entrambi i prompt della password.**

Controllo dei login non riusciti (OBP)

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

2. **Reimpostare il parametro digitando:**

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

Specifica di un banner di accensione

Sebbene non si tratti di un controllo preventivo o di rilevamento diretto, un banner può essere utilizzato per i motivi indicati di seguito.

- Comunicare la proprietà.

- Avvisare gli utenti degli usi accettabili del server.
- Indicare che l'accesso o le modifiche ai parametri OpenBoot è limitato 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 consentiti 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 all'indirizzo riportato di seguito.

http://docs.oracle.com/cd/E55211_01/

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 nel manuale *Guida all'installazione di Oracle Solaris: installazione di rete*.

  Vedere http://www.oracle.com/goto/solaris10/docs
- Per il sistema operativo Oracle Solaris 11, fare riferimento a *Protezione della rete in Oracle Solaris*.

  Vedere http://www.oracle.com/goto/solaris11/docs