Server SPARC e Netra SPARC T5 Series

Guida per la sicurezza

N. di parte: E40477-01
Aprile 2013

Indice

• • • Capitolo 1

Sicurezza dei server SPARC e Netra SPARC T5 Series

Il presente documento fornisce istruzioni di sicurezza generali per i server SPARC T5-1B, T5-2, T5-4, T5-8 e Netra SPARC T5-1B. Questa Guida è stata concepita per assistere l'utente nella definizione di un ambiente sicuro durante l'utilizzo di questi server con altri prodotti hardware Oracle, quali commutatori e schede di interfaccia di rete.

Nel presente capitolo sono riportate le sezioni seguenti:

Informazioni sui principi di sicurezza

I principi di sicurezza di base sono quattro: accesso, autenticazione, autorizzazione e accounting.

- **Accesso**

  Controlli fisici e software proteggono l'hardware o i dati dall'intrusione.
  - Per l'hardware, i limiti di accesso sono generalmente limiti all'accesso *fisico*.
  - Per il software, l'accesso viene limitato sia mediante mezzi fisici che virtuali.
  - Il firmware non può essere modificato se non tramite il processo di aggiornamento Oracle.
- **Autenticazione**

  In tutti i sistemi operativi della piattaforma sono disponibili le funzioni di autenticazione che è possibile impostare per garantire la convalida degli utenti.

  L'autenticazione fornisce vari livelli di sicurezza tramite misure quali badge e password.
- **Autorizzazione**

  L'autorizzazione consente al personale della società di utilizzare l'hardware e il software solo se correttamente formato e qualificato per tale scopo. Impostare un sistema di permessi di lettura, scrittura ed esecuzione per verificare l'accesso degli utenti a comandi, spazio su disco, dispositivi e applicazioni.

- **Accounting**

  Utilizzare le funzionalità di accounting hardware e software di Oracle per monitorare le attività di login e mantenere gli inventari hardware.
  - È possibile monitorare i login utente mediante i log di sistema. In particolare, gli account di servizio e amministratore di sistema dispongono di privilegi per l'accesso a importanti comandi pertanto è necessario monitorarli con attenzione utilizzando i log di sistema. In genere i log rimangono attivi per lunghi periodi di tempo, pertanto è importante rimuovere periodicamente i file di log quando superano una certa dimensione nel rispetto dei criteri in uso nella società del cliente.
  - Gli asset IT del cliente vengono in genere tracciati tramite i numeri di serie. I numeri di parte Oracle sono registrati elettronicamente su tutte le schede, i moduli e le schede madri ed è possibile utilizzarli per l'inventario.

Pianificazione di un ambiente sicuro

Utilizzare le note riportate di seguito durante le fasi preliminari e nel corso dell'installazione e della configurazione di un server e della relativa apparecchiatura.

Sicurezza hardware

L'hardware fisico può essere protetto piuttosto semplicemente limitando l'accesso all'hardware e registrando i numeri di serie.

- **Limitare l'accesso**
  - Installare i server e le apparecchiature relative in una stanza il cui accesso è riservato.
  - Se le apparecchiature sono installate in un rack dotato di sportello, chiudere sempre lo sportello fino a quando non è necessario effettuare un intervento sui componenti contenuti nel rack.
  - Limitare l'accesso alle console USB, che sono in grado di offrire un accesso con maggiori possibilità rispetto alle connessioni SSH. 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.
  - Limitare l'accesso a dispositivi con collegamento o swapping a caldo, in quanto vengono rimossi con facilità.
  - Conservare le unità di ricambio sostituibili in loco (FRU) o le unità sostituibili dal cliente (CRU) in un cabinet chiuso. Consentire l'accesso all'armadietto solo al personale autorizzato.
- **Registrare i 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 le speciali penne ultraviolette o etichette a 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.

Sicurezza del software

La sicurezza dell'hardware viene garantita principalmente tramite l'implementazione di misure software.

- Modificare tutte le password predefinite durante l'installazione di un nuovo sistema. La maggior parte delle apparecchiature utilizzano password predefinite, come **changeme**, conosciute a livello

globale e per questo motivo non sicure contro gli accessi non autorizzati. Inoltre, dispositivi come i commutatori di rete possono disporre di più account utente per impostazione predefinita. Assicurarsi di modificare tutte le password degli account.

- Limitare l'utilizzo dell'account superutente `root`. Quando possibile, si consiglia di utilizzare piuttosto i profili utente Oracle ILOM (Integrated Lights Out Manager) quali `operator` e `administrator`.
- Utilizzare una rete dedicata per i processori di servizi per separarli dalla rete generale.
- Fare riferimento alla documentazione fornita con il software per attivare le funzionalità di sicurezza disponibili per il software.
- Con WAN Boot o iSCSI Boot è possibile eseguire il boot di un server in modo sicuro.
  - Per una release Oracle Solaris 10, fare riferimento al manuale *Oracle Solaris Installation Guide: Network-Based Installations*.
  - Per una release Oracle Solaris 11, fare riferimento al manuale *Installing Oracle Solaris 11 Systems* per informazioni su WAN Boot e al manuale *System Administration Guide: Basic Administration* per informazioni su iSCSI Boot.

Nel documento *Istruzioni di sicurezza per Oracle Solaris* sono disponibili informazioni su:

- Come potenziare Oracle Solaris
- Come utilizzare le funzionalità di sicurezza di Oracle Solaris durante la configurazione dei sistemi
- Come aggiungere in modo sicuro applicazioni e utenti a un sistema
- Come proteggere le applicazioni basate su rete

Il documento *Istruzioni di sicurezza per Oracle Solaris* per la versione in uso è disponibile all'indirizzo:

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

Sicurezza firmware

Tutti i sottocomponenti del firmware di Oracle System possono essere aggiornati solo in gruppo. Per evitare che vengano apportate modifiche non autorizzate al firmware, nel firmware di Oracle System viene utilizzato un processo di aggiornamento controllato. Solo il superutente o un utente autenticato con l'autorizzazione appropriata può utilizzare il processo di aggiornamento.

Sicurezza di Oracle OpenBoot

È possibile proteggere tramite password l'accesso all'interfaccia a riga di comando del firmware Oracle OpenBoot utilizzando le variabili di sicurezza OpenBoot.

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

Firmware Oracle ILOM

Oracle ILOM (Oracle Integrated Lights Out Manager) è il firmware di gestione del sistema preinstallato su server, modulo server, sistema modulare e altro hardware Oracle. Oracle ILOM consente di gestire e monitorare attivamente i componenti installati nel sistema. Il modo in cui si

utilizza Oracle ILOM influisce sulla sicurezza del sistema. Per comprendere maggiormente l'uso di questo firmware nella configurazione di password, nella gestione degli utenti e nell'applicazione di funzioni relative alla sicurezza, tra cui l'autenticazione Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS, fare riferimento alla documentazione di Oracle ILOM:

- http://www.oracle.com/goto/ILOM/docs

Mantenimento di un ambiente sicuro

Dopo aver eseguito l'installazione e l'impostazione, utilizzare le funzioni di sicurezza hardware e software Oracle per mantenere il controllo sull'hardware e tenere traccia degli asset di sistema.

Controlli hardware

Alcuni sistemi Oracle possono essere impostati per essere attivati e disattivati mediante i comandi software. È inoltre possibile attivare e disattivare da remoto mediante i comandi software le unità di distribuzione dell'alimentazione (PDU) per alcuni cabinet di sistema. L'autorizzazione per tali comandi è solitamente impostata durante la configurazione del sistema ed è limitata agli amministratori di sistema e al personale di servizio. Fare riferimento alla documentazione relativa a cabinet o sistema per ulteriori informazioni.

Tracciabilità dell'asset

I numeri di serie Oracle sono incorporati nel firmware nelle schede opzionali e nelle schede madri del sistema. È possibile leggere questi numeri di serie tramite le connessioni LAN per la registrazione dell'inventario.

I reader wireless RFID (Radio Frequency Identification) consentono di semplificare ulteriormente la registrazione degli asset. Il white paper Oracle relativo al *tracciamento 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

Aggiornamenti per software e firmware

- Verificare con regolarità la presenza di aggiornamenti.
- Installare sempre la versione più recente del software o del firmware nell'apparecchiatura.
- Installare eventuali patch di sicurezza necessarie per il software.
- Tenere presente che i dispositivi come i commutatori di rete contengono anche un firmware e necessitano pertanto di aggiornamenti firmware e patch.

Accesso locale e remoto

Attenersi alle istruzioni fornite di seguito per garantire la sicurezza dell'accesso locale e remoto ai sistemi.

- Creare un banner che dichiari che l'accesso non autorizzato è proibito.
- Ove possibile, utilizzare le liste di controllo dell'accesso.
- Impostare timeout per le sessioni prolungate e livelli di privilegi.
- Utilizzare le funzioni di autenticazione, autorizzazione e accounting (AAA) per l'accesso locale e remoto a un commutatore.

- Se possibile, utilizzare i protocolli di sicurezza RADIUS e TACACS+:
  - RADIUS (Remote Authentication Dial In User Service) è un protocollo client/server che protegge le reti dall'accesso non autorizzato.
  - TACACS+ (Terminal Access Controller Access-Control System) è un protocollo che consente a un server di accesso remoto di comunicare con un server di autenticazione per determinare se un utente può accedere alla rete.
- Utilizzare la funzionalità di mirroring delle porte del commutatore per l'accesso al sistema di rilevamento delle intrusioni IDS (Intrusion Detection System).
- Implementare la sicurezza delle porte per limitare l'accesso basato su un indirizzo MAC. Disattivare il trunking automatico in tutte le porte.
- Limitare la configurazione remota a indirizzi IP specifici utilizzando SSH anziché Telnet. Telnet passa i nomi e le password utente con testo in chiaro, pertanto può consentire la visualizzazione delle credenziali di login a chiunque si trovi nel segmento LAN. Impostare una password sicura per SSH.
- Le prime versioni del protocollo SNMP non sono sicure e trasmettono i dati di autenticazione utilizzando testo non cifrato. Solo la versione 3 di SNMP è in grado di garantire trasmissioni sicure.
- Alcuni prodotti vengono rilasciati con la stringa community SNMP predefinita impostata su PUBLIC. Gli autori di attacchi possono inviare query a una comunità per ottenere una mappa di rete molto complessa e, se possibile, modificare i valori di base delle informazioni di gestione (MIB). Se il protocollo SNMP è necessario, sostituire la stringa community SNMP predefinita con una stringa community più efficace.
- Abilitare i log e inviarli a un host sicuro dedicato.
- Configurare i log in modo da includere informazioni precise sull'ora, utilizzando NTP e gli indicatori orari.
- Controllare la presenza di incidenti nei log e archiviare i log rispettando i criteri di sicurezza.
- Se il controller di sistema usa un'interfaccia browser, eseguire sempre il logout dopo averlo utilizzato.

Sicurezza dei dati

Attenersi alle istruzioni riportate di seguito per ottimizzare la sicurezza dei dati.

- Eseguire il backup dei dati più importanti mediante dispositivi quali dischi rigidi esterni, chiavette USB o memory stick. Memorizzare i dati acquisiti in una seconda posizione sicura in remoto.
- Utilizzare un software di cifratura dei dati per mantenere riservate le informazioni confidenziali su unità disco rigido sicure.
- Quando si desidera eliminare un'unità disco rigido obsoleta, distruggere fisicamente l'unità oppure eliminare totalmente i dati in essa presenti. La semplice eliminazione di tutti i file o la nuova formattazione dell'unità rimuove soltanto le tabelle degli indirizzi nell'unità. Dopo queste operazioni sarà ancora possibile recuperare le informazioni dall'unità. (Utilizzare un programma software di cancellazione del disco per cancellare completamente tutti i dati da un'unità.)

Sicurezza di rete

Attenersi alle istruzioni riportate di seguito per ottimizzare la sicurezza di rete.

- La maggior parte dei commutatori consente di definire le reti VLAN (Virtual Local Area Network). Se si utilizza il commutatore per definire le reti VLAN, separare i cluster di sistemi sensibili dal resto della rete. In questo modo, è possibile diminuire la probabilità di accessi non autorizzati a informazioni che si trovano sui questi client e server.

- Eseguire la gestione fuori banda dei commutatori (separati dal traffico di dati). Se la gestione fuori banda non è realizzabile, dedicare un numero VLAN per la gestione dei contenuti all'interno della banda.
- Mantenere sicuri gli host Infiniband. Un fabric Infiniband è sicuro tanto quanto il relativo host Infiniband meno sicuro.
- Tenere presente che il partizionamento non protegge un fabric Infiniband. Il partizionamento consente solo di impostare un isolamento del traffico Infiniband tra le macchine virtuali di un host.
- Conservare offline un file di configurazione del commutatore e limitarne l'accesso solo agli amministratori autorizzati. Il file di configurazione deve contenere commenti descrittivi per ciascuna impostazione.
- Utilizzare una configurazione VLAN statica, ove possibile.
- Disattivare le porte commutatore non utilizzate e assegnare loro un numero VLAN non utilizzato.
- Assegnare un numero VLAN nativo univoco alle porte trunk.
- Limitare il numero di reti VLAN trasportabili tramite un trunk solamente a quelle strettamente necessarie.
- Disattivare il protocollo VTP (VLAN Trunking Protocol), se possibile. In alternativa, impostare le seguenti opzioni per VTP: eliminazione, password e dominio di gestione. Quindi, impostare il protocollo VTP in modalità trasparente.
- Disattivare i servizi di rete non necessari, quali server di piccole dimensioni TCP o HTTP. Attivare i servizi di rete necessari e configurarli in modo sicuro.
- Commutatori differenti offrono diversi livelli di funzionalità di sicurezza delle porte. Utilizzare le funzionalità di sicurezza della porta riportate di seguito, se disponibili in corrispondenza del commutatore.
  - Bloccaggio MAC: implica il collegamento di un indirizzo MAC (Media Access Control) di uno o più dispositivi connessi a una porta fisica su un commutatore. Se si blocca una porta commutatore per un particolare indirizzo MAC, i superutenti non potranno creare backdoor nella rete con punti di accesso rogue.
  - Blocco MAC: consente di impedire a uno specifico indirizzo MAC di connettersi a un commutatore.
  - Apprendimento MAC: consente di utilizzare le informazioni su ciascuna connessione diretta della porta commutatore, in modo che sia possibile per il commutatore impostare la sicurezza in base alle connessioni correnti.