Sun Server X4-4

Guida per la sicurezza

N. di parte: E54170–01
Aprile 2014

140617@25097

Indice

Panoramica

In questo documento vengono fornite le linee guida di sicurezza generali per garantire la sicurezza di Oracle Sun Blade X4-4, delle relative interfacce di rete e dei commutatori di rete ai quali è connesso.

In questa sezione vengono trattati i seguenti argomenti:

Panoramica del sistema

Sun Server X4-supporta i seguenti componenti:

- Processori Intel Xeon® E7-8895 v2 con 15 core a 2,8 GHz con le seguenti configurazioni:
  - Due processori installati nei socket 0 e 1
  - Quattro processori installati nei socket da 0 a 3
- Sono supportati fino a otto moduli riser di memoria (due riser per CPU) nello chassis del server. Ciascun modulo riser supporta fino a dodici DIMM a bassa tensione registrati DDR3-1600 ECC e consente fino a 24 DIMM per processore. I DIMM installati devono essere dello stesso tipo e dimensione.
  - Un sistema con due CPU che utilizza quattro moduli riser. Nella configurazione minima ciascun riser contiene quattro DIMM (DIMM da 8 GB, DIMM da 16 GB o LRDIMM da 32 GB). È possibile aggiungere ulteriori DIMM fino a un massimo di 1,5 TB di memoria di sistema.
  - Un sistema con quattro CPU che utilizza otto moduli riser. Nella configurazione minima ciascun riser contiene quattro DIMM (DIMM da 8 GB, DIMM da 16 GB o LRDIMM da 32 GB). È possibile aggiungere ulteriori DIMM fino a un massimo di 3 TB di memoria di sistema.
- Undici slot PCI Express 3.0 contenenti schede PCIe di basso profilo. Nelle configurazioni che includono una scheda HBA SAS, la scheda HBA viene installata nello slot 2. Tutti gli slot supportano le connessioni PCIe x8. Due slot sono in grado di supportare anche schede PCIe x16.
  - Slot da 1 a 7, 9 e 10: connettore x8

- Slot 8 e 11: connettore x8 o x16

Nota – Gli slot PCIe da 7 a 11 funzionano solo nei sistemi con quattro CPU.

- Per la memorizzazione, lo chassis del server fornisce:
  - Sei alloggiamenti di unità da 2,5 pollici accessibili mediante il pannello anteriore. Tutti gli alloggiamenti possono contenere HDD SAS-2 o SSD SATA-3.
  - Un'unità DVD+/-RW opzionale sulla parte anteriore del server, sotto gli alloggiamenti dell'unità. Questo DVD SATA è connesso a un bridge SATA USB. Per questo motivo viene riconosciuto dal software di sistema come dispositivo di memorizzazione USB.
  - Opzioni delle schede PCIe HBA SAS-2:
    - Sun Storage 6 Gb SAS PCIe HBA. Supporta i livelli RAID: 0, 1, 10.
    - Sun Storage 6 Gb SAS PCIe RAID HBA. Supporta i livelli RAID: 0, 1, 1E, 10, 5, 5EE, 6 con BBWC (Battery Backed Write Cache).
- Due alimentatori sostituibili a caldo, ad intervallo automatico, CA da 1030/2060 Watt.

  Un sistema con due CPU può funzionare con fonti di alimentazione da 100 a 127 VAC a bassa tensione. Un sistema con quattro CPU può funzionare solo con fonti di alimentazione da 200 a 240 VAC ad alta tensione, ma l'alta tensione è supportata anche per una configurazione di sistema con due CPU.
- Il controller BMC (Integrated Baseboard Management Controller), che supporta quanto segue:
  - Set di funzioni IPMI standard di settore
  - Sistema KVMS remoto, DVD e floppy su IP
  - Include una porta seriale
  - Accesso Ethernet al processore di servizio mediante una porta di gestione GbE (Giga Ethernet) 10/100/1000 RJ-45 dedicata e opzionalmente mediante una delle porte GbE host (gestione di banda laterale)
- Lo strumento di impostazione server Oracle System Assistant, integrato in un'unità flash USB preinstallata.

Principi di sicurezza

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

- **Accesso**

  L'accesso fa riferimento all'accesso fisico all'hardware o all'accesso fisico o virtuale al software.

- Eseguire controlli fisici e al software per proteggere il proprio hardware e i dati da eventuali intrusioni.
- Fare riferimento alla documentazione fornita con il software per attivare le funzionalità di sicurezza disponibili per il software.
- Installare server e apparecchiature correlate in una stanza con accesso limitato.
- Se l'apparecchiatura è installata in un rack dotato di sportello, non lasciare mai lo sportello aperto, tranne quando è necessario agire sui componenti all'interno.
- Limitare l'accesso a connettori o porte, che sono in grado di offrire un accesso con maggiori possibilità rispetto alle connessioni SSH. I dispositivi come i controller di sistema, le unità di distribuzione dell'alimentazione (PDU, power distribution unit) e i commutatori di rete forniscono connettori e porte.
- Limitare l'accesso in particolare a dispositivi con collegamento o swapping a caldo, in quanto possono essere facilmente rimossi.
- Archiviare le unità sostituibili sul campo (FRU, field-replaceable units) e le unità sostituibili dall'utente (CRU, customer-replaceable unit) di riserva in un armadietto chiuso a chiave. Consentire l'accesso all'armadietto solo al personale autorizzato.

- **Autenticazione**

  L'autenticazione garantisce la convalida degli utenti di hardware o software.

  - Impostare funzionalità di autenticazione, come ad esempio un sistema di password, nei sistemi operativi della piattaforma per garantire la convalida degli utenti.
  - Assicurarsi che il personale utilizzi i badge dei dipendenti in modo adeguato per accedere alla sala computer.
  - Per gli account utente utilizzare, se necessario, le liste di controllo degli accessi, impostare timeout per sessioni troppo prolungate e impostare livelli di privilegi per gli utenti.

- **Autorizzazione**

  L'autorizzazione fa riferimento alle limitazioni per il personale in merito all'utilizzo di hardware o software.

  - Consentire al personale di utilizzare solamente hardware e software per i quali si dispone di qualifiche e si è ricevuta un'adeguata formazione.
  - Impostare un sistema di autorizzazioni di lettura, scrittura ed esecuzione per controllare l'accesso utente a comandi, spazio su disco, dispositivi e applicazioni.

- **Accounting**

  L'accounting fa riferimento alle funzioni software e hardware utilizzate per monitorare le attività di login e la gestione dei magazzini hardware.

  - Utilizzare i log di sistema per monitorare i login utente. Monitorare gli account di amministratore di sistema e di servizio poiché tali account dispongono di privilegi per l'accesso a comandi potenti.

- Tenere traccia dei numeri di serie di tutti i dispositivi hardware. Utilizzare i numeri di serie del componente per tenere traccia degli asset di sistema. I numeri di parte Oracle sono registrati elettronicamente su schede, moduli e schede madri ed è possibile utilizzarli per il magazzino.
- Per rilevare e tenere traccia dei componenti, fornire un contrassegno di sicurezza per tutti gli elementi significativi dell'hardware del computer, come le FRU. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.

Uso degli strumenti di gestione e configurazione server

Seguire le linee guida di sicurezza riportate di seguito durante l'utilizzo degli strumenti software e firmware per configurare e gestire il server.

Sicurezza di Oracle System Assistant

Oracle System Assistant è uno strumento preinstallato che consente di aggiornare e configurare localmente o in remoto l'hardware del server e di installare i sistemi operativi supportati. Per informazioni sull'utilizzo di Oracle System Assistant, fare riferimento alla *guida di amministrazione dei server Oracle serie X4* all'indirizzo:

`http://www.oracle.com/goto/x86AdminDiag/docs`

Le seguenti informazioni consentono di analizzare i problemi di sicurezza di Oracle System Assistant.

- **Oracle System Assistant contiene un ambiente root di boot.**

  Oracle System Assistant è un'applicazione eseguita su un'unità flash USB interna preinstallata ed è situata in un ambiente root Linux di boot. Oracle System Assistant fornisce inoltre la capacità di accedere alla relativa shell root di base. Gli utenti con accesso fisico al sistema o che dispongono dell'accesso remoto a tastiera, video, mouse e archiviazione tramite Oracle ILOM, potranno accedere a Oracle System Assistant e alla shell root.

  È possibile utilizzare un ambiente root per modificare la configurazione e i criteri del sistema, nonché per accedere ai dati su altri dischi. Si consiglia di proteggere l'accesso fisico al server e assegnare privilegi console e amministratore agli utenti Oracle ILOM con moderazione.

- **In Oracle System Assistant è disponibile un dispositivo di memorizzazione USB accessibile dal sistema operativo.**

  Oltre a essere un ambiente di boot, Oracle System Assistant prevede inoltre un dispositivo di memorizzazione USB (unità flash) accessibile dal sistema operativo host dopo l'installazione. Tale funzionalità è utile durante l'accesso a strumenti e driver per interventi

di manutenzione e riconfigurazione. Il dispositivo di memorizzazione USB di Oracle System Assistant è leggibile e scrivibile e può essere soggetto all'attacco di virus.

Si consiglia di utilizzare gli stessi metodi di protezione dei dischi nel dispositivo di memorizzazione di Oracle System Assistant, compresi scansione regolare dei virus e verifica dell'integrità.

- **È possibile disattivare Oracle System Assistant.**

  Oracle System Assistant è uno strumento estremamente utile per l'impostazione del server, l'aggiornamento e la configurazione del firmware e l'installazione del sistema operativo host. Tuttavia, se i requisiti di sicurezza descritti sopra non vengono soddisfatti oppure se lo strumento non è necessario, Oracle System Assistant può essere disattivato. Disattivando Oracle System Assistant non sarà più possibile accedere al dispositivo di memorizzazione USB dal sistema operativo host. Inoltre, non sarà possibile eseguire il boot di Oracle System Assistant.

  È possibile disattivare Oracle System Assistant dallo strumento stesso o da BIOS. Una volta disattivato, Oracle System Assistant può essere riattivato solamente dall'utilità di impostazione del BIOS. Si consiglia di proteggere con una password l'impostazione del BIOS, in modo che solo gli utenti autorizzati possano attivare nuovamente Oracle System Assistant. Per informazioni su come disattivare e attivare nuovamente Oracle System Assistant, fare riferimento alla guida di amministrazione dei server Oracle serie X4 all'indirizzo:

  `http://www.oracle.com/goto/x86AdminDiag/docs`

Sicurezza di Oracle ILOM

È possibile proteggere, gestire e monitorare attivamente i componenti di sistema mediante il firmware di gestione di Oracle ILOM (Oracle Integrated Lights Out Manager), preinstallato su questo server, su altri server basati su Oracle x86 e su alcuni server basati su SPARC Oracle.

Utilizzare una rete interna dedicata per il processore di servizio per separarlo dalla rete generale. Oracle ILOM fornisce agli amministratori di sistema funzioni di controllo e monitoraggio del server. A seconda del livello di autorizzazione concesso agli amministratori, queste funzioni possono includere la possibilità di spegnere il server, creare account utente, installare dispositivi di memorizzazione remoti e così via. Pertanto, per mantenere un ambiente il più affidabile e sicuro possibile per Oracle ILOM, la porta di gestione di rete dedicata o la porta di gestione di banda laterale sul server deve essere sempre collegata a una rete affidabile interna o a una rete di gestione/privata sicura dedicata.

Limitare l'utilizzo dell'account amministratore predefinito (`root`) al login iniziale a Oracle ILOM. Questo account amministratore predefinito viene fornito solo per facilitare l'installazione iniziale del server. Pertanto, per garantire un ambiente il più sicuro possibile, è necessario modificare la password predefinita dell'amministratore `changeme` durante l'impostazione iniziale del sistema. Per ogni nuovo utente Oracle ILOM è necessario definire

nuovi account utente con password univoche e livelli di autorizzazione assegnati, oltre alla possibilità di modificare la password per l'account amministratore predefinito.

Fare riferimento alla documentazione di Oracle ILOM per maggiori informazioni sull'impostazione delle password, la gestione degli utenti e l'applicazione di funzionalità relative alla sicurezza, che includono l'autenticazione Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS. Per le linee guida di sicurezza specifiche per Oracle ILOM, fare riferimento alla *guida per la sicurezza di Oracle Integrated Lights Out Manager (ILOM)*, che fa parte della libreria della documentazione per la release di Oracle ILOM in uso. È possibile reperire la documentazione di Oracle ILOM all'indirizzo:

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

Sicurezza di Oracle Hardware Management Pack

Oracle Hardware Management Pack è disponibile per il server, per molti altri server basati su x86 e solo per alcuni server SPARC. In Oracle Hardware Management Pack sono disponibili due componenti: un agente di monitoraggio SNMP e una gamma di strumenti CLI (interfaccia a riga di comando) per la gestione del server.

Grazie ai plugin SNMP di Hardware Management Agent, è possibile utilizzare il protocollo SNMP per monitorare i server Oracle e i moduli server nel centro dati, con il vantaggio di non dover eseguire la connessione a due punti di gestione, l'host e Oracle ILOM. Questa funzionalità consente di utilizzare un singolo indirizzo IP (quello dell'host) per monitorare più server e moduli server. I plugin SNMP vengono eseguiti sul sistema operativo host dei server Oracle.

È possibile utilizzare gli strumenti CLI di Oracle Server per configurare i server Oracle. Gli strumenti CLI sono compatibili con Oracle Solaris, Oracle Linux, Oracle VM, altre varianti di Linux e sistemi operativi Microsoft Windows.

Fare riferimento alla documentazione di Oracle Hardware Management Pack per maggiori informazioni su queste funzionalità. Per le linee guida di sicurezza specifiche per Oracle Hardware Management Pack, fare riferimento alla *guida per la sicurezza di Oracle Hardware Management Pack (HMP)*, che fa parte della libreria della documentazione di Oracle Hardware Management Pack. È possibile reperire la documentazione di Oracle Hardware Management Pack all'indirizzo:

`http://www.oracle.com/goto/OHMP/docs`

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.

Vengono trattati gli argomenti seguenti:

Linee guida di sicurezza per il sistema operativo

Fare riferimento ai documenti del sistema operativo Oracle per informazioni su:

- Come utilizzare le funzionalità di sicurezza durante la configurazione dei sistemi.
- Come eseguire operazioni in maniera sicura durante l'aggiunta di applicazioni e utenti a un sistema
- Come proteggere le applicazioni basate sulla rete

I documenti della guida per la sicurezza per i sistemi operativi Oracle supportati sono parte della libreria della documentazione del sistema operativo. Per consultare il documento della guida per la sicurezza di un sistema operativo Oracle, individuare la libreria della documentazione del sistema operativo Oracle:

Sistema operativo	Collegamento
Sistema operativo Oracle Solaris	`http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html`
Sistema operativo Oracle Linux	`http://linux.oracle.com`
Sistema operativo Oracle VM	`http://www.oracle.com/technetwork/documentation/vm-096300.html`

Per informazioni sui sistemi operativi di altri fornitori, ad esempio Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows e VMware ESXi, fare riferimento alla documentazione del fornitore.

Commutatori e porte di rete

Diversi commutatori offrono differenti livelli di funzionalità di sicurezza delle porte. Per ulteriori informazioni sulle operazioni riportate di seguito, fare riferimento alla documentazione relativa ai commutatori.

- Utilizzare funzionalità di autenticazione, autorizzazione e accounting per l'accesso locale e remoto al commutatore.
- Modificare tutte le password dei commutatori di rete che potrebbero presentare, per impostazione predefinita, più password e account utente.
- Eseguire la gestione fuori banda dei commutatori (separati dal traffico dati). Se non è possibile eseguire la gestione fuori banda, predisporre un numero di VLAN (rete locale virtuale) separate per la gestione in banda.
- Utilizzare la funzionalità di mirroring delle porte del commutatore di rete per l'accesso al sistema di rilevamento delle intrusioni IDS (Intrusion Detection System).
- Mantenere un file di configurazione dello switch offline e limitare l'accesso solamente agli amministratori autorizzati. Il file di configurazione deve contenere commenti descrittivi per ciascuna impostazione.
- Implementare la sicurezza della porta per limitare l'accesso basato su indirizzi MAC. Disattivare il trunking automatico su tutte le porte.
- Utilizzare queste funzionalità di sicurezza della porta se disponibili nello switch in uso:
  - La funzione di **blocco MAC** prevede l'associazione di un indirizzo MAC (Media Access Control) di uno o più dispositivi connessi a una porta fisica su uno switch. Se viene bloccata una porta dello switch di uno specifico indirizzo MAC, ai superutenti non sarà consentito creare backdoor nella rete con punti di accesso rogue.
  - La funzione di **blocco MAC** consente di disattivare la connessione di un indirizzo MAC a uno switch.
  - La funzione di **apprendimento MAC**consente di utilizzare le informazioni su ciascuna connessione diretta della porta dello switch, in modo da consentire al commutatore di rete di impostare la sicurezza in base alle connessioni correnti.

Sicurezza VLAN

Se viene impostata una rete locale virtuale (VLAN), tenere presente che le VLAN condividono la larghezza di banda della rete e richiedono misure di sicurezza aggiuntive.

- Definire le reti VLAN per separare i cluster sensibili dei sistemi dal resto della rete. In questo modo viene limitata la possibilità che gli utenti possano accedere alle informazioni su questi client e server.
- 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. Impostare quindi il protocollo VTP in modalità trasparente.

Sicurezza di Infiniband

Proteggere gli host Infiniband. Un fabric Infiniband è sicuro quanto il relativo host Infiniband meno sicuro.

- Il partizionamento non protegge un fabric Infiniband. Il partizionamento offre solo l'isolamento del traffico Infiniband tra macchine virtuali su un host.
- Utilizzare una configurazione VLAN statica, se possibile.
- Disattivare le porte dei commutatori non utilizzate e assegnare loro un numero di VLAN non utilizzato.

Sicurezza fisica dell'hardware

I componenti hardware fisici possono essere protetti in modo relativamente semplice: è necessario limitare l'accesso e registrare i numeri di serie.

- **Limitare l'accesso**
  - Installare server e apparecchiature correlate in una stanza con accesso limitato.
  - Se l'apparecchiatura è installata in un rack dotato di sportello, non lasciare mai lo sportello aperto, tranne quando è necessario agire sui componenti all'interno. Chiudere lo sportello dopo qualsiasi intervento sull'apparecchiatura.
  - 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 in particolare a dispositivi con collegamento o swapping a caldo, in quanto possono essere facilmente rimossi.
- Conservare le unità sostituibili sul campo (FRU, field-replaceable units) o le unità sostituibili dall'utente (CRU, customer-replaceable unit) di riserva in un armadietto chiuso a chiave. Consentire l'accesso all'armadietto solo al personale autorizzato.

- **Registrare i numeri di serie**
  - Posizionare un contrassegno di sicurezza su tutti gli elementi significativi dell'hardware del computer, come le FRU. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.
  - Tenere traccia dei numeri di serie di tutti i dispositivi hardware.
  - 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.

Sicurezza del software

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

- Quando si installa un nuovo sistema, modificare tutte le password predefinite. Per la maggior parte dei dispositivi vengono utilizzate password predefinite, ad esempio 'changeme', che facilitano gli accessi non autorizzati all'apparecchiatura in quanto conosciute.
- Modificare tutte le password dei commutatori di rete che possono includere più account e password utente per impostazione predefinita.
- Limitare l'uso dell'account amministratore predefinito (root) a un unico utente amministratore. Creare sempre un nuovo account Oracle ILOM per ogni nuovo utente. Assicurarsi che a ciascun account utente Oracle ILOM siano sempre assegnati una password univoca e un livello appropriato di privilegi di autorizzazione (operatore, amministratore e così via).
- Utilizzare una rete dedicata per i processori di servizio per separarli dalla rete generale.
- Proteggere l'accesso alle console USB. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU) e gli switch di rete possono essere dotati di connessioni USB, che sono in grado di offrire un accesso con maggiori possibilità rispetto alle connessioni SSH.
- Fare riferimento alla documentazione fornita con il software per attivare le funzionalità di sicurezza disponibili per il software.
- Implementare la sicurezza della porta per limitare l'accesso basato su indirizzi MAC. Disattivare il trunking automatico su tutte le porte.

Gestione 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.

Controllo dell'alimentazione dell'hardware

È possibile utilizzare il software per attivare e disattivare l'alimentazione di alcuni sistemi Oracle. È possibile attivare e disattivare da remoto 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 del cabinet o del sistema per ulteriori informazioni.

Registrazione degli asset

Utilizzare i numeri di serie per tenere traccia del magazzino. Oracle incorpora i numeri di serie nel firmware sulle schede opzionali e sulle schede madri del sistema. È possibile leggere questi numeri di serie mediante connessioni di rete locale.

Per semplificare ulteriormente la registrazione degli asset, è inoltre possibile utilizzare lettori wireless di identificazione a radiofrequenza (RFID, radio frequency identification). Il white pater Oracle relativo alla *registrazione degli asset del sistema Oracle Sun mediante RFID* è disponibile al seguente indirizzo:

```
http://www.oracle.com/
technetwork/articles/systems-hardware-architecture/
o11-001-rfid-oracle-214567.pdf
```

Aggiornamenti per software e firmware

Mantenere sempre aggiornate le versioni di software e firmware nell'apparecchiatura server.

- Verificare con regolarità la presenza di aggiornamenti.
- Installare sempre la versione più recente del software o del firmware nell'apparecchiatura.
- Installare tutte le patch di sicurezza necessarie per il software.
- Tenere presente che anche dispositivi quali i commutatori di rete e gli Express Module contengono il firmware e potrebbero richiedere gli aggiornamenti delle patch e del firmware.

Sicurezza di rete

Per proteggere l'accesso locale e remoto ai sistemi, attenersi alle linee guida riportate di seguito.

- Limitare la configurazione remota a indirizzi IP specifici utilizzando SSH anziché Telnet. Telnet consente di trasmettere nomi utente e password tramite testo in chiaro, consentendo potenzialmente a chiunque si trovi nel segmento LAN di visualizzare le credenziali di login. Impostare una password sicura per SSH.
- Utilizzare la versione 3 del protocollo SNMP (Simple Network Management Protocol) per garantire trasmissioni sicure. Le versioni precedenti di SNMP non sono sicure e trasmettono dati di autenticazione utilizzando un formato di testo non cifrato.
- Modificare la stringa comunità SNMP predefinita in una stringa comunità sicura se SNMP è necessario. In alcuni prodotti il valore PUBLIC è impostato come stringa comunità SNMP predefinita. Gli autori di attacchi possono inviare query a una comunità per ottenere una mappa di rete completa e, se possibile, modificare i valori di base delle informazioni di gestione (MIB).
- Eseguire sempre il logout dopo aver utilizzato il controller di sistema, se questo utilizza un'interfaccia browser.
- Disattivare i servizi di rete non necessari, come il protocollo TCP (Transmission Control Protocol) o quello HTTP (Hypertext Transfer Protocol). Attivare i servizi di rete necessari e configurarli in maniera sicura.
- Adottare le misure di sicurezza LDAP quando si utilizza il protocollo LDAP per l'accesso al sistema. Fare riferimento alla guida per la sicurezza di Oracle ILOM all'indirizzo: `http://www.oracle.com/goto/ILOM/docs`.
- 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 uno switch.

- 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 su tutte le porte.

Protezione e sicurezza dei dati

Per ottimizzare la protezione e la sicurezza dei dati, seguire le linee guida indicate di seguito.

- Eseguire il backup dei dati importanti utilizzando dispositivi quali unità disco rigido esterne o dispositivi di memorizzazione USB. Memorizzare i dati di cui si è eseguito il backup in un luogo diverso, remoto e sicuro.
- Utilizzare il software di cifratura dei dati per proteggere le informazioni riservate sulle unità disco rigido.
- Quando si sostituisce un'unità disco rigido obsoleta, distruggerla fisicamente o eliminare totalmente tutti i dati al suo interno. È comunque possibile recuperare le informazioni da un disco dopo che tutti i file sono stati eliminati o il disco è stato riformattato. L'eliminazione dei file o la riformattazione del disco consentono di rimuovere solo le tabelle di indirizzi sul disco. Utilizzare il software di cancellazione del disco per eliminare completamente tutti i dati da un'unità.

Gestione dei log

Controllare e gestire i file di log regolarmente. Utilizzare i seguenti metodi per proteggere i file di log.

- Attivare il log e inviare i log di sistema a un host sicuro dedicato.
- Configurare il log per includere informazioni temporali accurate, mediante NTP (Network Time Protocol) e gli indicatori orari.
- Esaminare i log per individuare possibili anomalie e archiviarli seguendo i criteri di sicurezza.
- Archiviare periodicamente i file di log quando raggiungono dimensioni troppo elevate. Conservare copie dei file archiviati per riferimenti futuri o analisi statistiche.