Sun Blade X4-2B

Guida per la sicurezza

N. di parte: E50098-02
giugno 2014

Indice

Sicurezza di base

In questo documento vengono fornite le linee guida di sicurezza generali per proteggere il server Oracle o il modulo server, le relative interfacce di rete e i commutatori di rete connessi.

Per i requisiti di sicurezza aggiuntivi relativi al sistema e all'ambiente specifico, contattare il responsabile della sicurezza IT.

Esistono alcuni principi di sicurezza di base che devono essere soddisfatti quando si utilizzano tutti i componenti hardware e software. In questa sezione vengono descritti i quattro principi di sicurezza di base:

- sezione chiamata «Accesso» [5]
- sezione chiamata «Autenticazione» [6]
- sezione chiamata «Autorizzazione» [6]
- sezione chiamata «Accounting e controllo» [6]

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.
- Quando si installa un nuovo sistema, modificare tutte le password predefinite. Molti tipi di apparecchiature utilizzano password predefinite, come `changeme`, conosciute a livello globale e per questo motivo non sicure contro gli accessi non autorizzati all'hardware o al software.
- 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 fisico alle porte USB, alle porte di rete e alle console di sistema. I server e i commutatori di rete dispongono di porte e connessioni alle console, che forniscono accesso diretto al sistema.
- Limitare la possibilità di riavviare il sistema sulla rete.

- 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 indica il modo in cui un utente viene identificato, in genere mediante informazioni riservate quali il nome utente e la password. 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 stanza dei computer.
- Per gli account utente utilizzare, se necessario, le liste di controllo dell'accesso, impostare timeout per sessioni troppo prolungate e impostare livelli di privilegi per gli utenti.

Autorizzazione

L'autorizzazione consente agli amministratori di controllare le attività che un utente può eseguire o i privilegi che può utilizzare. Il personale può eseguire solo le attività ed utilizzare i privilegi assegnati. L'autorizzazione fa riferimento alle limitazioni per il personale in merito all'utilizzo di hardware e 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 e controllo

L'accounting e il controllo consentono di gestire un record dell'attività dell'utente sul sistema. Le funzionalità hardware e software Oracle consentono agli amministratori di monitorare l'attività di login e gestire gli inventari hardware.

- Utilizzare i log di sistema per monitorare i login utente. Monitorare in particolare gli account di servizio e amministratore di sistema in quanto garantiscono l'accesso a comandi

che, se non utilizzati correttamente, possono danneggiare il sistema o causare la predita di dati. L'accesso e i comandi devono essere monitorati attentamente mediante i log di sistema.

- Registrare i numeri di serie di tutti i dispositivi hardware. Utilizzare i numeri di serie dei componenti 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 l'inventario.
- 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 sicuro degli strumenti di gestione e configurazione del server

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

- sezione chiamata «Sicurezza di Oracle System Assistant» [9]
- sezione chiamata «Sicurezza di Oracle ILOM» [10]
- sezione chiamata «Sicurezza di Oracle Hardware Management Pack» [12]

Per i requisiti di sicurezza aggiuntivi relativi al sistema e all'ambiente specifico, contattare il responsabile della sicurezza IT.

Sicurezza di Oracle System Assistant

Oracle System Assistant è uno strumento preinstallato che consente di configurare e aggiornare 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 informazioni riportate di seguito descrivono problemi di sicurezza relativi a Oracle System Assistant.

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

  Oracle System Assistant è un'applicazione eseguita in un'unità flash USB interna e preinstallata Oracle System Assistant è situato in un ambiente root Linux di boot. Oracle System Assistant garantisce inoltre la possibilità di accedere a una shell root sottostante. Gli utenti con accesso fisico al sistema o che dispongono dell'accesso remoto a tastiera, video, mouse e archiviazione tramite Oracle ILOM, possono accedere a Oracle System Assistant e alla shell root.

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

La shell di Oracle System Assistant è progettata per consentire agli utenti con privilegi appropriati di utilizzare gli strumenti CLI di Oracle Hardware Management Pack per la gestione del sistema. La shell non è progettata per fornire servizi di rete. Per impostazione predefinita, i servizi di rete sono disattivati in modo da garantire i massimi livelli di sicurezza e non devono essere attivati.

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

  Oltre a essere un ambiente di boot, Oracle System Assistant prevede inoltre un dispositivo di archiviazione 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 archiviazione USB di Oracle System Assistant è leggibile e scrivibile e può essere soggetto all'attacco di virus.

  Per aumentare la sicurezza, applicare al dispositivo di archiviazione di Oracle System Assistant gli stessi metodi utilizzati per la protezione dei dischi, comprese la scansione regolare dei virus e la 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 non è possibile accettare le limitazioni di sicurezza descritte sopra o se lo strumento non è necessario, Oracle System Assistant può essere disattivato. Dopo la disattivazione di Oracle System Assistant, non sarà più possibile accedere al dispositivo di archiviazione USB dal sistema operativo host e gli utenti non saranno in grado di eseguire il boot di Oracle System Assistant.

  È possibile disattivare Oracle System Assistant dallo strumento stesso o dal BIOS. Una volta disattivato, Oracle System Assistant può essere riattivato solamente dalla utility di impostazione del BIOS. Si consiglia di proteggere con una password la utility di impostazione del BIOS, in modo che solo gli utenti autorizzati possano attivare nuovamente Oracle System Assistant.

- **Fare riferimento alla documentazione di Oracle System Assistant.**

  Per informazioni sulle funzionalità e sulle funzioni di 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), incorporato nei server Oracle basati su x86 e su alcuni server Oracle basati su SPARC. A seconda del livello di autorizzazione concesso agli amministratori di sistema, queste funzioni possono includere la possibilità di spegnere il server, creare account utente, installare dispositivi di archiviazione remoti e così via.

- **Utilizzare una rete sicura interna affidabile.**

  Indipendentemente dal fatto che venga stabilita o meno una connessione di gestione fisica a Oracle ILOM mediante la porta seriale locale, la porta di gestione di rete dedicata o la porta di rete dati standard, è fondamentale che questa porta fisica sul server sia sempre connessa a una rete sicura interna, a una rete di gestione sicura dedicata o a una rete privata.

  Non collegare mail il processore di servizio di Oracle ILOM a una rete pubblica, ad esempio Internet. È necessario mantenere il traffico di gestione del processore di servizio di Oracle ILOM su una rete di gestione separata e concedere l'accesso solo agli amministratori del sistema.

- **Limitare l'utilizzo dell'account amministratore predefinito.**

  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. La concessione dell'accesso all'account amministratore predefinito consente a un utente accesso illimitato a tutte le funzionalità di Oracle ILOM. Inoltre, definire nuovi account utente con password univoche e assegnare livelli di autorizzazione (ruoli utente) a ciascun nuovo utente di Oracle ILOM.

- **Considerare attentamente i rischi durante il collegamento della porta seriale a un server di terminale.**

  I dispositivi di terminali non sempre forniscono i livelli appropriati di autenticazione o autorizzazione utente necessari per proteggere la rete da intrusioni dannose. Per proteggere il sistema da intrusioni non desiderate alla rete, non stabilire una connessione seriale (porta seriale) a Oracle ILOM mediante qualsiasi tipo di dispositivo di reindirizzamento di rete, come un server di terminale, a meno che il server non disponga di un numero sufficiente di controlli dell'accesso.

  Inoltre, alcune funzioni di Oracle ILOM, ad esempio la reimpostazione delle password e il menu di preboot, sono disponibili solo se utilizza la porta seriale fisica. La connessione della porta seriale a una rete mediante un server di terminale non autenticato elimina la necessità dell'accesso fisico e riduce il livello di sicurezza associato a queste funzioni.

- **L'accesso al menu di preboot richiede l'accesso fisico al server.**

  Il menu di preboot di Oracle ILOM è un'importante utility che consente di reimpostare i valori predefiniti di Oracle ILOM e di aggiornare il firmware se Oracle ILOM non risponde. Una volta che Oracle ILOM è stato reimpostato, è necessario che un utente prema un pulsante sul server (l'impostazione predefinita) o digiti una password. La proprietà relativa alla presenza fisica di Oracle ILOM controlla questo funzionamento (`check_physical_presence= true`). Per una maggiore sicurezza durante l'accesso al menu di preboot, non modificare l'impostazione predefinita (`true`), in modo che l'acceso al menu di preboot richieda sempre l'accesso fisico al server.

- **Fare riferimento alla documentazione di Oracle ILOM.**

  Per ulteriori informazioni sull'impostazione delle password, sulla gestione degli utenti e sull'applicazione delle funzioni relative alla sicurezza, fare riferimento alla

documentazione di Oracle ILOM. Per le linee guida relative alla sicurezza specifiche per Oracle ILOM, fare riferimento alla *guida per la sicurezza di Oracle ILOM*, che fa parte della libreria della documentazione di Oracle ILOM. 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 Oracle x86 e solo per alcuni server basati su SPARC Oracle. In Oracle Hardware Management Pack sono disponibili due componenti: un agente di monitoraggio SNMP e una gamma di strumenti CLI (interfaccia della riga di comando) per la gestione del server.

- **Utilizzare i plug-in SNMP di Hardware Management Agent.**

  SNMP è un protocollo standard utilizzato per monitorare o gestire un sistema. Grazie ai plugin SNMP di Hardware Management Agent, è possibile utilizzare il protocollo SNMP per monitorare i server Oracle 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.

  I plugin SNMP vengono eseguiti sul sistema operativo host dei server Oracle. Il modulo del plugin SNMP estende l'agente SNMP nativo nel sistema operativo host per fornire funzionalità aggiuntive di Oracle MIB. Oracle Hardware Management Pack stesso non contiene un agente SNMP. Per Linux, viene aggiunto un modulo all'agente net-snmp. Per Oracle Solaris, viene aggiunto un modulo all'agente di gestione Oracle Solaris. Per Microsoft Windows, il plugin estende il servizio SNMP nativo. Tutte le impostazioni di sicurezza relative a SNMP per Oracle Hardware Management Pack vengono determinate dalle impostazioni dell'agente o servizio SNMP nativo e non dal plugin.

  SNMPv1 e SNMPv2c non forniscono alcuna cifratura e utilizzano stringhe comunità come metodo di autenticazione. SNMPv3 è più sicuro ed è la versione consigliata poiché utilizza la cifratura per fornire un canale sicuro, nonché password e nomi utente singoli.

- **Fare riferimento alla documentazione di Oracle Hardware Management Pack.**

  Fare riferimento alla documentazione di Oracle Hardware Management Pack per maggiori informazioni su queste funzioni. 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

Prima dell'arrivo del sistema, è necessario verificare la disponibilità delle linee guida sulla sicurezza. Successivamente, è necessario esaminarle periodicamente e modificarle in modo da renderle conformi ai requisiti di sicurezza correnti dell'organizzazione. Utilizzare le informazioni riportate in questa sezione durante le fasi preliminari e nel corso dell'installazione e della configurazione di un server e della relativa apparecchiatura.

Vengono trattati gli argomenti seguenti:

Per i requisiti di sicurezza aggiuntivi relativi al sistema e all'ambiente specifico, contattare il responsabile della sicurezza IT.

Protezione delle password

Le password sono un elemento importante per la sicurezza poiché le password scelte con poca attenzione possono determinare un accesso non autorizzato alle risorse aziendali. L'implementazione di procedure consigliate per la gestione delle password assicura che gli utenti seguano una serie di linee guida per la creazione e la protezione delle relative password. I componenti tipici di un criterio delle password devono definire:

- Lunghezza e sicurezza delle password
- Durata delle password
- Procedure comuni per le password

Applicare le procedure standard riportate di seguito per creare password complesse e sicure.

- Non creare una password che contenga il nome utente, il nome del dipendente o i nomi dei familiari.
- Non selezionare password facili da indovinare.

- Non creare password contenenti una stringa consecutiva di numeri, ad esempio 12345.
- Non creare password contenenti una parola o una stringa facile da individuare mediante una semplice ricerca su Internet.
- Non consentire agli utenti di riutilizzare la stessa password su più sistemi.
- Non consentire agli utenti di riutilizzare password vecchie.

Modificare regolarmente le password. In questo modo è possibile impedire attività dannose e garantire che le password siano conformi ai criteri delle password correnti.

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://www.oracle.com/technetwork/documentation/ol-1-1861776.html
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, Microsoft Windows e VMware ESXi, fare riferimento alla documentazione del fornitore.

Commutatori e porte di rete

I commutatori di rete 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 VLAN (rete locale virtuale) 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 commutatore, in modo che sia possibile per il commutatore di rete 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.

- Quando si utilizzano le reti VLAN, 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.
- Utilizzare configurazioni VLAN statiche, ove possibile.
- Disattivare le porte commutatore non utilizzate e assegnare loro un numero VLAN non utilizzato.

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.

Gestione di un ambiente sicuro

Dopo aver eseguito l'installazione e l'impostazione iniziale, utilizzare le funzioni di sicurezza hardware e software Oracle per continuare a controllare gli asset hardware e software.

Per i requisiti di sicurezza aggiuntivi relativi al sistema e all'ambiente specifico, contattare il responsabile della sicurezza IT.

Controllo dell'alimentazione

È possibile utilizzare il software per attivare e disattivare l'alimentazione di alcuni sistemi Oracle. Le unità di distribuzione dell'alimentazione (PDU) per alcuni cabinet di sistema possono essere abilitate e disabilitate in remoto. 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.

Tracciabilità degli asset

Utilizzare i numeri di serie per tenere traccia dell'inventario. Oracle include numeri di serie all'interno del firmware, nelle schede opzionali e nelle schede madri del sistema. È possibile leggere questi numeri di serie mediante connessioni di rete locali (LAN).

Per semplificare ulteriormente la tracciabilità degli asset, è inoltre possibile utilizzare lettori wireless di identificazione a radiofrequenza (RFID, radio frequency identification). Il white paper Oracle relativo alla *tracciabilità 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

I miglioramenti alla sicurezza vengono introdotti mediante nuove release e patch software. La gestione efficace e proattiva delle patch è una parte fondamentale della sicurezza del sistema. Per una maggiore sicurezza, aggiornare il sistema con la release software più recente e con tutte le patch di sicurezza necessarie

- Verificare con regolarità la presenza di aggiornamenti software e patch di sicurezza.
- Installare sempre la versione più recente di software o firmware.
- Installare tutte le patch di sicurezza necessarie per il software.
- Tenere presente che i dispositivi come i commutatori di rete contengono inoltre firmware e potrebbero richiedere aggiornamenti firmware e patch.

Sicurezza di rete

Dopo aver configurato le reti in base ai principi di sicurezza, è necessario svolgere regolarmente le attività di controllo e manutenzione.

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 non cifrato, consentendo potenzialmente a chiunque si trovi nel segmento della rete locale (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 molto complessa e, se possibile, modificare i valori di base delle informazioni di gestione (MIB).
- Se il controllo di sistema utilizza un'interfaccia browser, eseguire sempre il logout dopo aver utilizzato il controller di sistema.
- 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.

- Creare un messaggio di avvio visualizzato quando si esegue il login per indicare che l'accesso non autorizzato è proibito. È possibile informare gli utenti sui criteri o sulle regole importanti. Il messaggio di avvio può essere utilizzato per avvisare gli utenti della presenza di speciali limitazioni di accesso a un dato sistema o per ricordare loro i criteri delle password e l'utilizzo appropriato.
- Ove possibile, per applicare le limitazioni, 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 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.
- Adottare le misure di sicurezza LDAP quando si utilizza il protocollo LDAP per l'accesso al sistema.
- 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.

Per ulteriori informazioni sulla sicurezza di rete, fare riferimento alla *guida per la sicurezza di Oracle ILOM*, che fa parte della libreria della documentazione di Oracle ILOM. È possibile reperire la documentazione di Oracle ILOM all'indirizzo:

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

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 archiviazione USB. Memorizzare i dati acquisiti in una seconda posizione sicura in remoto.
- 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, utilizzando il protocollo NTP e data/ora.
- Eseguire scansioni pianificate a intervalli regolari dei log dei dispositivi di rete per monitorare l'attività o l'accesso inusuale alla rete.
- Riesaminare i log per individuare possibili anomalie e archiviarli in conformità con i criteri di sicurezza.
- Ritirare periodicamente i file di log quando raggiungono dimensioni troppo elevate. Conservare copie dei file ritirati per riferimenti futuri o analisi statistiche.