Guida per la sicurezza di Oracle® Server X6-2L

N. di parte: E73726-01
Aprile 2016

N. di parte: E73726-01

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.

Indice

Sicurezza di base 7
Accesso 7
Autenticazione 8
Autorizzazione 8
Accounting e controllo 8

Uso sicuro degli strumenti di configurazione e gestione del server 11
Sicurezza di Oracle ILOM 11
Sicurezza di Oracle Hardware Management Pack 12

Pianificazione di un ambiente sicuro 15
Protezione delle password 15
Linee guida di sicurezza per il sistema operativo 16
Switch e porte di rete 16
Sicurezza VLAN 17
Sicurezza di InfiniBand 18

Gestione di un ambiente sicuro 19
Controllo dell'alimentazione 19
Tracciabilità degli asset 19
Aggiornamenti per software e firmware 20
Sicurezza di rete 20
Protezione e sicurezza dei dati 21
Gestione dei log 22

Sicurezza di base

In questo documento vengono fornite le linee guida di sicurezza generali per proteggere il server Oracle, le relative interfacce di rete e gli switch 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» [7]
- sezione chiamata «Autenticazione» [8]
- sezione chiamata «Autorizzazione» [8]
- sezione chiamata «Accounting e controllo» [8]

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 il server e le apparecchiature correlate in una stanza chiusa a chiave con accesso limitato.
- Se l'apparecchiatura è installata in uno scaffale dotato di sportello, non lasciare mai lo sportello aperto, tranne quando è necessario agire sui componenti al suo interno.
- Limitare l'accesso a porte e console USB. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU) e gli switch di rete sono dotati di connessioni USB, in grado di offrire accesso diretto al sistema. L'accesso fisico è il metodo di accesso ai componenti più sicuro, in quanto non è soggetto ad attacchi che sfruttano la rete.

- Limitare la possibilità di riavviare il sistema sulla rete.
- Limitare l'accesso in particolare a dispositivi hot plug o hot swap, in quanto possono essere facilmente rimossi.
- Archiviare le unità sostituibili sul campo (FRU, Field-Replaceable Unit) e 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.

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, ad esempio un sistema di password nel sistema operativo della piattaforma in uso 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 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 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, è necessario dotare di contrassegno di sicurezza tutti gli elementi significativi dell'hardware del computer, come ad esempio FRU e CRU. 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 agli amministratori di sistema, in particolare durante le emergenze del sistema. I documenti stampati potrebbero essere la sola prova della proprietà del materiale.

Uso sicuro degli strumenti di configurazione e gestione del server

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

- sezione chiamata «Sicurezza di Oracle ILOM» [11]
- 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 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, la porta di gestione della banda laterale 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 mai 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.**

  Fare riferimento alla documentazione Oracle ILOM per ottenere maggiori informazioni sull'impostazione di password, la gestione degli utenti e l'applicazione di funzionalità relative alla sicurezza, comprese l'autenticazione Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS. 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 Oracle SPARC. 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. 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 i sistemi operativi Microsoft Windows.

- **Utilizzare i plugin 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 queste sezioni durante le fasi preliminari e nel corso dell'installazione e della configurazione di un server e della relativa apparecchiatura.

- sezione chiamata «Protezione delle password» [15]
- sezione chiamata «Linee guida di sicurezza per il sistema operativo» [16]
- sezione chiamata «Switch e porte di rete» [16]
- sezione chiamata «Sicurezza VLAN» [17]
- sezione chiamata «Sicurezza di InfiniBand» [18]

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://www.oracle.com/technetwork/documentation/solaris-11-192991.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.

Switch e porte di rete

Gli switch di rete offrono differenti livelli di funzionalità di sicurezza delle porte. Per ulteriori informazioni sulle operazioni riportate di seguito, fare riferimento alla documentazione relativa agli switch.

- Utilizzare funzionalità di autenticazione, autorizzazione e accounting per l'accesso locale e remoto allo switch.

- Modificare tutte le password degli switch di rete che potrebbero presentare, per impostazione predefinita, più password e account utente.
- Eseguire la gestione fuori banda degli switch (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 dello switch 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. Nel file di configurazione dovrebbero essere contenuti commenti descrittivi per ciascuna impostazione.
- Implementare la sicurezza delle porte per limitare l'accesso basato sugli indirizzi MAC. Disattivare il trunking automatico su tutte le porte.
- Utilizzare le funzionalità di sicurezza delle porte riportate di seguito, se disponibili nello switch in uso.
  - La funzione di **bloccaggio 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 che sia possibile per lo switch 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. Per misure di sicurezza aggiuntive, attenersi alle linee guida riportate di seguito.

- 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. Quindi, impostare il protocollo VTP in modalità trasparente.
- Utilizzare configurazioni VLAN statiche, ove possibile.
- Disattivare le porte degli switch non utilizzate e assegnare loro un numero di VLAN non utilizzato.

Sicurezza di InfiniBand

Per aumentare la sicurezza quando si utilizza InfiniBand, attenersi alle linee guida riportate di seguito.

- Proteggere gli host InfiniBand. Un fabric InfiniBand è sicuro 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.

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.

Utilizzare le informazioni contenute in queste sezioni per la gestione di un ambiente sicuro.

- sezione chiamata «Controllo dell'alimentazione» [19]
- sezione chiamata «Tracciabilità degli asset» [19]
- sezione chiamata «Aggiornamenti per software e firmware» [20]
- sezione chiamata «Sicurezza di rete» [20]
- sezione chiamata «Protezione e sicurezza dei dati» [21]
- sezione chiamata «Gestione dei log» [22]

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 o firmware e patch di sicurezza.
- 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 i dispositivi come gli switch di rete contengono anche un firmware e necessitano pertanto di aggiornamenti firmware e patch.

Gli aggiornamenti software e le patch di sicurezza sono disponibili sul sito Web My Oracle Support all'indirizzo:

https://support.oracle.com

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 efficace per SSH.
- Utilizzare la versione 3 del protocollo SNMP (Simple Network Management Protocol) per garantire trasmissioni sicure. Versioni precedenti di SNMP non sono sicure e trasmettono i dati di autenticazione come testo non cifrato. SNMPv3 utilizza la cifratura per fornire un canale sicuro, nonché password e nomi utente singoli.
- Se è necessario il protocollo SNMPv1 o SNMPv2, sostituire la stringa comunità SNMP predefinita con una stringa comunità più efficace. 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.
- Attivare i servizi di rete necessari e configurarli in modo sicuro. Disattivare i servizi di rete non necessari, come il protocollo TCP (Transmission Control Protocol) o HTTP (Hypertext Transfer Protocol).
- Adottare le misure di sicurezza LDAP quando si utilizza il protocollo LDAP per l'accesso al sistema.
- 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 uno switch.
- Utilizzare questi servizi di rete in ambienti molto sicuri in quanto sono protetti da certificati e altre forme di cifratura sicura per la protezione del canale.
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- Utilizzare questi servizi di rete su reti sicure e private in cui non sono presenti utenti malintenzionati.
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- Utilizzare la funzionalità di mirroring delle porte dello switch per l'accesso al sistema di rilevamento delle intrusioni IDS (Intrusion Detection System).
- Implementare la sicurezza delle porte per limitare l'accesso in base a 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 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 nelle 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 dell'unità consentono di rimuovere solo le tabelle di indirizzi sull'unità. Utilizzare il software di cancellazione del disco per eliminare completamente tutti i dati da un'unità.
- Le unità disco rigido vengono spesso utilizzate per memorizzare informazioni riservate. Per proteggere queste informazioni dalla diffusione non autorizzata, è necessario 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. In alternativa, è possibile utilizzare strumenti di degaussing fisico, se appropriati e disponibili.
  - In alcuni casi, le informazioni contenute nelle unità disco rigido hanno un livello di riservatezza talmente elevato da far considerare la distruzione fisica mediante polverizzazione o incinerazione come unico metodo di ripulitura.
  - Si consiglia alle organizzazioni di far riferimento ai criteri di protezione dei dati esistenti per determinare il metodo più appropriato per ripulire le unità disco fisso.

Attenzione - Gli strumenti di cancellazione del disco potrebbero non essere in grado di eliminare alcuni dati contenuti nelle unità disco fisso più recenti, in special modo le unità SSD (Solid State Drive), a causa delle modalità di gestione dell'accesso ai dati che le contraddistingue.

Gestione dei log

Verificare ed eseguire la manutenzione dei file di log con regolarità. Utilizzare i metodi indicati di seguito 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 ai 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.