Guida sulla sicurezza di Oracle® ILOM - Release firmware 3.0, 3.1 e 3.2

N. di parte: E40364-04
Ottobre 2015

N. di parte: E40364-04

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

Uso della presente documentazione

- **Panoramica**: fornisce informazioni sull'interfaccia Web e CLI e sulle linee guida relative ai task di sicurezza di Oracle ILOM. Usare la presente guida insieme alle altre guide presenti nella libreria della documentazione di Oracle ILOM.
- **Destinatari**: tecnici, amministratori del sistema, fornitori di servizi Oracle autorizzati e utenti esperti nella gestione dell'hardware di sistema.
- **Competenze richieste**: esperienza nella configurazione e gestione dei server Oracle.

Libreria della documentazione sul prodotto

La documentazione e le risorse per questo e per i prodotti correlati sono disponibili all'indirizzo http://www.oracle.com/goto/ilom/docs.

Commenti

Inviare commenti su questa documentazione all'indirizzo http://www.oracle.com/goto/docfeedback

Funzionalità di sicurezza per ogni release firmware di Oracle ILOM

Utilizzare la tabella riportata di seguito per identificare la release firmware in cui è stata resa disponibile una funzionalità di sicurezza di Oracle ILOM.

Disponibilità versione firmware	Funzionalità di sicurezza	Per i dettagli, vedere:
Tutte	Autenticazione e autorizzazione	■ sezione chiamata «Protezione dell'accesso utente in Oracle ILOM» [25]
Tutte	Connessione di gestione sicura dedicata	■ sezione chiamata «Protezione della connessione di gestione fisica» [15] ■ sezione chiamata «Come mantenere una connessione di gestione sicura» [55]
Tutte	Porte di rete preconfigurate cifrate	■ sezione chiamata «Servizi e porte di rete preconfigurati» [20]
Tutte	Gestione sicura IPMI 2.0	■ sezione chiamata «Configurare l'accesso alla gestione del protocollo IPMI per una maggiore sicurezza» [51]
Tutte	Configurazione della cifratura delle chiavi SSH (Secure Shell)	■ Utilizzare chiavi lato server per cifrare le connessioni SSH [46] ■ Aggiungere chiavi SSH agli account utente per l'autenticazione CLI automatizzata [47]
Tutte	Gestione sicura SNMP 3.0	■ sezione chiamata «Configurare l'accesso alla gestione del protocollo SNMP per una maggiore sicurezza» [49]
Tutte	Protocolli e certificati SSL	■ Caricamento di un certificato e di una chiave privata SSL personalizzati in Oracle ILOM [40] ■ Ottenere un certificato e una chiave privata SSL mediante OpenSSL [39] ■ Abilitazione delle proprietà di cifratura SSL e TLS più efficaci [41]
Tutte	Protocolli di cifratura e sicuri della console remota	■ sezione chiamata «Utilizzo sicuro del sistema KVMS remoto» [59]
3.0.4 e versioni successive	Configurazione di blocco host KVMS	■ Bloccare l'accesso host all'uscita da una sessione KVMS [34]
3.0.4 e versioni successive	Configurazione del timeout della sessione	■ Impostare un intervallo di timeout per le sessioni Web inattive [43] ■ Impostare un intervallo di timeout per le sessioni CLI inattive [45]

Disponibilità versione firmware	Funzionalità di sicurezza	Per i dettagli, vedere:
3.0.12 e versioni successive	Sessioni autenticate dall'interconnessione host locale	■ sezione chiamata «Accesso di interconnessione host autenticata preferenziale» [56]
3.0.8 e versioni successive	Configurazione del messaggio di avvio di login	Accesso sicuro al sistema con il messaggio di avvio di login (3.0.8 e versioni successive) [36]
Dalla versione 3.0.8 alla versione 3.1.2	Accesso sicuro WS-Management	■ sezione chiamata «Configurare l'accesso WS-Management per una maggiore sicurezza» [53]
3.1.0 e versioni successive	Log di controllo separato	■ sezione chiamata «Monitorare gli eventi di controllo per individuare accessi non autorizzati» [64]
3.1.0 e versioni successive	Controllo presenza di sicurezza fisica	■ sezione chiamata «Presenza di sicurezza fisica per la reimpostazione della password predefinita dell'account `root`» [63]
3.2.4 e versioni successive	Proprietà configurabile IPMI 1.5	■ sezione chiamata «Configurare l'accesso alla gestione del protocollo IPMI per una maggiore sicurezza» [51]
3.2.4 e versioni successive	Versioni protocollo TLS 1.1 e 1.2	■ Abilitazione delle proprietà di cifratura SSL e TLS più efficaci [41]
3.2.4 e versioni successive	Conteggio delle sessioni KVMS	■ Limitazione delle sessioni KVMS visualizzabili per Remote System Console Plus (3.2.4 o versioni successive) [35]
3.2.4 e versioni successive	Supporto cifratura per conformità a FIPS	■ sezione chiamata «Come scegliere se configurare la modalità FIPS al momento della distribuzione» [16] ■ sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19] ■ sezione chiamata «Considerazioni successive alla distribuzione per la protezione dell'accesso utente» [61]
3.2.5 e versioni successive	Stato del server SSH e crittografie meno avanzate	■ Gestione dello stato del server SSH e delle crittografie meno avanzate (3.2.5 e versioni successive) [45]
3.2.5 e versioni successive	Criterio della password per gli account utente locali	■ Impostazione di limitazioni per il criterio della password per tutti gli utenti locali (3.2.5 e versioni successive) [30]

Ulteriori informazioni sulla sicurezza

Per ulteriori informazioni sulla protezione di Oracle ILOM, consultare le seguenti sezioni presenti in questa guida:

- Elenchi di controllo delle procedure consigliate per la sicurezza di Oracle ILOM
- Procedure di sicurezza consigliate per la distribuzione di Oracle ILOM
- Procedure di sicurezza consigliate successive alla distribuzione di Oracle ILOM

Elenchi di controllo delle procedure consigliate per la sicurezza di Oracle ILOM

Oracle ILOM (Integrated Lights Out Manager) è un processore di servizio (SP) preinstallato su tutti i server Oracle e sulla maggior parte dei server SUN precedenti. Gli amministratori di sistema usano le interfacce utente di Oracle ILOM per eseguire task di gestione del server remoto nonché operazioni di monitoraggio dell'integrità del server in tempo reale.

Per verificare che per Oracle ILOM siano implementate le migliori procedure per la sicurezza dell'ambiente, gli amministratori di sistema devono consultare i task di sicurezza consigliati nei seguenti elenchi di controllo:

- sezione chiamata «Elenchi di controllo di sicurezza per la distribuzione del server» [11]
- sezione chiamata «Elenchi di controllo di sicurezza relativi alle procedure successive alla distribuzione del server» [12]

Informazioni correlate

- Procedure di sicurezza consigliate per la distribuzione di Oracle ILOM .
- Procedure di sicurezza consigliate successive alla distribuzione di Oracle ILOM
- Funzionalità di sicurezza per ogni release firmware di Oracle ILOM [9]

Elenchi di controllo di sicurezza per la distribuzione del server

Per stabilire quale sia la procedura di sicurezza migliore per Oracle ILOM quando si pianifica la distribuzione di un nuovo server, gli amministratori di sistema devono consultare l'elenco dei task di sicurezza consigliati nell'Tabella 1, «Elenco di controllo - Configurazione della sicurezza di Oracle ILOM al momento della distribuzione del server »riportato di seguito.

TABELLA 1 Elenco di controllo - Configurazione della sicurezza di Oracle ILOM al momento della distribuzione del server

✓	Task di sicurezza	Versione o versioni firmware applicabili	Per i dettagli, vedere:
	Stabilire una connessione di gestione dedicata sicura a Oracle ILOM.	Tutte le versioni firmware	■ sezione chiamata «Protezione della connessione di gestione fisica» [15]
	Decidere se la conformità alla sicurezza FIPS 140-2 è necessaria al momento della distribuzione, dopo la distribuzione o se non lo è affatto.	Firmware 3.2.4 e versioni successive	■ sezione chiamata «Come scegliere se configurare la modalità FIPS al momento della distribuzione» [16] ■ sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19]
	Impostazione del criterio della password per tutti gli account utente locali	Firmware 3.2.5 e versioni successive	■ Impostazione di limitazioni per il criterio della password per tutti gli utenti locali (3.2.5 e versioni successive) [30]
	Modificare la password predefinita fornita per l'account `root` preconfigurato dell'amministratore.	Tutte le versioni firmware	■ sezione chiamata «Evitare la creazione di account utente condivisi» [25] ■ Modifica della password predefinita per l'account `root` al primo login [31]
	Decidere se i servizi Oracle ILOM preconfigurati e le relative porte di rete aperte sono applicabili per l'ambiente di destinazione in uso.	Tutte le versioni firmware	■ sezione chiamata «Protezione di servizi e porte di rete aperte» [19]
	Configurare l'accesso utente a Oracle ILOM.	Tutte le versioni firmware	■ sezione chiamata «Protezione dell'accesso utente in Oracle ILOM» [25] ■ Creare account utente locali con privilegi basati sui ruoli [33]
	Decidere se l'accesso al sistema operativo host deve essere bloccato all'uscita di una sessione KVMS remota.	Firmware 3.0.4 e versioni successive	■ Bloccare l'accesso host all'uscita da una sessione KVMS [34]
	Decidere se limitare ad altri utenti la visualizzazione di sessioni KVMS remote avviate da SP.	Firmware 3.2.4 e versioni successive	■ Limitazione delle sessioni KVMS visualizzabili per Remote System Console Plus (3.2.4 o versioni successive) [35]
	Decidere se visualizzare un messaggio di avvio di sicurezza al login dell'utente o immediatamente dopo.	Firmware 3.0.8 e versioni successive	■ Accesso sicuro al sistema con il messaggio di avvio di login (3.0.8 e versioni successive) [36]
	Verificare che per tutte le interfacce utente di Oracle ILOM siano impostate le proprietà di sicurezza massima.	Tutte le versioni firmware	■ sezione chiamata «Configurazione delle interfacce di Oracle ILOM per una maggiore sicurezza» [37]

Elenchi di controllo di sicurezza relativi alle procedure successive alla distribuzione del server

Per stabilire quale sia la procedura di sicurezza migliore per Oracle ILOM da mantenere sui server esistenti nell'ambiente in uso, gli amministratori di sistema devono consultare l'elenco dei task di sicurezza consigliati nell'Tabella 2, «Elenco di controllo - Mantenimento della sicurezza di Oracle ILOM dopo la distribuzione del server »riportato di seguito.

TABELLA 2 Elenco di controllo - Mantenimento della sicurezza di Oracle ILOM dopo la distribuzione del server

✓	**Task di sicurezza**	**Versione o versioni firmware applicabili**	**Per i dettagli, vedere:**
	Mantenere una connessione di gestione sicura a Oracle ILOM	Tutte le versioni firmware	■ sezione chiamata «Evitare l'accesso al dispositivo KCS host non autenticato» [56] ■ sezione chiamata «Accesso di interconnessione host autenticata preferenziale» [56] ■ sezione chiamata «Usare la cifratura IPMI 2.0 per proteggere il canale» [57]
	Verificare che le sessioni KVMS remote e le sessioni seriali basate su testo vengano avviate in modo sicuro da Oracle ILOM.	Tutte le versioni firmware	■ sezione chiamata «Comunicazione KVMS remota e cifratura» [59] ■ sezione chiamata «Protezione dall'accesso condiviso del servizio KVMS remoto» [60] ■ sezione chiamata «Proteggersi dall'accesso condiviso della console seriale host» [60]
	Conservare e tenere traccia dell'accesso utente a Oracle ILOM.	Tutte le versioni firmware	■ sezione chiamata «Considerazioni successive alla distribuzione per la protezione dell'accesso utente» [61]
	Azioni di sicurezza necessarie per la reimpostazione di una password perduta per l'account `root` preconfigurato dell'amministratore.	Firmware 3.1 e versioni successive	■ sezione chiamata «Presenza di sicurezza fisica per la reimpostazione della password predefinita dell'account `root`» [63]
	Azioni di sicurezza necessarie se la modalità di conformità a FIPS 140-2 deve essere modificata in Oracle ILOM dopo la distribuzione del server.	Firmware 3.2.4 e versioni successive	■ Modifica della modalità FIPS dopo la distribuzione [66] ■ sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19]
	Verificare che il software e il firmware siano aggiornati sul server.	Tutte le release firmware	■ sezione chiamata «Aggiornamento alle versioni software e firmware più recenti» [68]

Procedure di sicurezza consigliate per la distribuzione di Oracle ILOM

Gli argomenti riportati di seguito consentono di decidere quali siano le procedure di sicurezza migliori per Oracle ILOM da implementare al momento della distribuzione del server.

- sezione chiamata «Protezione della connessione di gestione fisica» [15]
- sezione chiamata «Come scegliere se configurare la modalità FIPS al momento della distribuzione» [16]
- sezione chiamata «Protezione di servizi e porte di rete aperte» [19]
- sezione chiamata «Protezione dell'accesso utente in Oracle ILOM» [25]
- sezione chiamata «Configurazione delle interfacce di Oracle ILOM per una maggiore sicurezza» [37]

Informazioni correlate

- Elenchi di controllo delle procedure consigliate per la sicurezza di Oracle ILOM.
- Procedure di sicurezza consigliate successive alla distribuzione di Oracle ILOM
- Funzionalità di sicurezza per ogni release firmware di Oracle ILOM [9]

Protezione della connessione di gestione fisica

Oracle ILOM è uno strumento di gestione fuori banda (OOB) che utilizza un canale di gestione dedicato per gestire e monitorare i server Oracle. A differenza dei server provvisti di strumenti di gestione in banda, i server Oracle sono dotati di funzionalità di gestione remota incorporate che consentono agli amministratori di sistema di accedere in modo sicuro a Oracle ILOM mediante un connettore di rete dedicato separato sul processore di servizio. Sebbene la funzionalità di gestione di Oracle ILOM fornisca agli amministratori di sistema funzionalità specifiche per il monitoraggio e la gestione dei server Oracle, Oracle ILOM non è stato progettato per essere un motore di elaborazione generico o per consentire l'accesso da una connessione di rete non protetta e non trusted.

Indipendentemente dal fatto che una connessione di gestione fisica a Oracle ILOM venga stabilita 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 o sul modulo CMM (Chassis

Monitoring Module) sia sempre connessa a una rete trusted interna, a una rete di gestione sicura dedicata o a una rete privata. Per ulteriori linee guida relative al momento in cui si stabilisce una connessione di gestione fisica a Oracle ILOM, vedere la tabella riportata di seguito.

Connessione di gestione delle porte fisiche a Oracle ILOM	Hardware Oracle supportato	Linee guida sulla sicurezza delle connessioni di gestione
Connessione dedicata	■ Server (Porta: `NET MGT`) ■ CMM (Porta: `NET MGT`)	Utilizzare una rete interna dedicata per il processore di servizio (SP) per separarlo dal traffico della rete dati generale. Per ulteriori informazioni su come stabilire una connessione di gestione di rete dedicata a Oracle ILOM, vedere ■ Connessione di gestione di una rete dedicata nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (3.2.x)*
Connessione locale	■ Server (Porta: `SER MGT`) ■ CMM (Porta: `SER MGT`)	Utilizzare una connessione di gestione seriale locale per accedere a Oracle ILOM direttamente dal server fisico o dal modulo CMM. Per ulteriori informazioni su come stabilire una connessione di gestione seriale locale a Oracle ILOM, vedere: ■ Connessione di gestione di una rete seriale locale a Oracle ILOM nella *guida per gli amministratori relativa alla configurazione e gestione di Oracle ILOM (3.2.x)*
Connessione della banda laterale	Server (Porte: `NET0, NET1`, `NET2`, `NET3`)	Utilizzare una rete dati Ethernet condivisa per accedere al processore di servizio SP ogni volta che è necessario semplificare la gestione dei cavi e la configurazione di rete evitando di dover predisporre due connessioni di rete separate. Per ulteriori informazioni su come stabilire una connessione di gestione della banda laterale a Oracle ILOM, vedere ■ Connessione di gestione della banda laterale nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (3.2.x)* **Nota -** La gestione della banda laterale è supportata sulla maggior parte dei server Oracle.

Nota - Per proteggersi dagli attacchi alla sicurezza, l'**utente non deve mai connettere Oracle ILOM SP 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.

Come scegliere se configurare la modalità FIPS al momento della distribuzione

A partire dalla release firmware 3.2.4 di Oracle ILOM, l'interfaccia CLI e l'interfaccia Web di Oracle ILOM offrono una modalità configurabile per la conformità al Livello 1 degli standard FIPS (Federal Information Processing Standards). Quando questa modalità è abilitata,

Oracle utilizza algoritmi crittografici in conformità agli standard di sicurezza FIPS 140-2 per proteggere dati sensibili o preziosi del sistema.

Gli amministratori di sistema che distribuiscono server con firmware 3.2.4 o versioni successive devono decidere se configurare o meno la modalità FIPS prima di configurare altre proprietà di Oracle ILOM. Per impostazione predefinita, la modalità di conformità agli standard FIPS in Oracle ILOM è disabilitata. Eventuali modifiche alla modalità di conformità agli standard FIPS comporterà il ripristino dei valori predefiniti di tutti i dati di configurazione.

Per abilitare la modalità di conformità agli standard FIPS al momento della distribuzione (prima di configurare le proprietà di Oracle ILOM), vedere Abilitazione della modalità FIPS al momento della distribuzione [17]. Qualora le proprietà di configurazione definite dall'utente siano già state impostate in Oracle ILOM e sia necessario modificare la proprietà FIPS, vedere sezione chiamata «Azioni successive alla distribuzione per la modifica della modalità FIPS» [65].

▼ Abilitazione della modalità FIPS al momento della distribuzione

Nota - La modalità di conformità agli standard FIPS in Oracle ILOM è rappresentata dalle proprietà di stato configurazione e di stato operativo. La proprietà di stato configurazione e la proprietà di stato operativo rappresentano rispettivamente la modalità configurata e la modalità operativa in Oracle ILOM. Quando viene modificata la proprietà di stato configurazione di FIPS, la modifica non ha effetto sulla modalità operativa (proprietà di stato operativo di FIPS) fino al successivo reboot di Oracle ILOM.

Informazioni preliminari

- Le proprietà di stato configurazione e stato operativo di FIPS sono disabilitate per impostazione predefinita.
- Quando FIPS è abilitato (in modalità configurata e operativa), alcune funzionalità in Oracle ILOM non sono supportate. Per un elenco di funzionalità non supportate quando FIPS è abilitato, vedere Tabella 3, «Funzionalità non supportate in Oracle ILOM quando la modalità FIPS è abilitata».
- Per modificare la proprietà di stato configurazione di FIPS è richiesto il ruolo Admin (a).
- La proprietà configurabile per la conformità agli standard FIPS è disponibile in Oracle ILOM a partire dal firmware 3.2.4 o versioni successive. Prima della release firmware 3.2.4, Oracle ILOM non offriva una proprietà configurabile per la conformità agli standard FIPS.
- I valori predefiniti di tutte le impostazioni di configurazione definite dall'utente vengono ripristinati alla modifica delle proprietà di stato configurazione e stato operativo della modalità FIPS in Oracle ILOM.

1. **Nell'interfaccia Web di Oracle ILOM fare clic su ILOM Administration -> Management Access -> FIPS.**

2. **Nella pagina FIPS eseguire le operazioni riportate di seguito.**

   a. **Selezionare la casella di controllo FIPS State per abilitare la proprietà FIPS configurata.**

   b. **Fare clic su Save per applicare la modifica.**

   Per ulteriori informazioni sulla configurazione, fare clic sul collegamento `More details`.... sulla pagina Web di FIPS.

3. **Per modificare lo stato della modalità operativa di FIPS in Oracle ILOM, attenersi alla procedura descritta di seguito per il reboot di Oracle ILOM.**

   a. **Nell'interfaccia Web fare clic su ILOM Administration -> Maintenance -> SP Reset.**

   b. **Nella pagina SP Reset fare clic sul pulsante SP Reset.**

   Al reboot di Oracle ILOM si verifica quanto riportato di seguito.

   - Al sistema viene applicato l'ultimo stato FIPS (abilitato) configurato.
   - Vengono ripristinati i valori predefiniti di qualsiasi impostazione di configurazione definita dall'utente precedentemente configurata in Oracle ILOM.
   - La proprietà di stato operativo di FIPS viene aggiornata per riflettere lo stato operativo abilitato corrente in Oracle ILOM.

     Per un elenco e una descrizione completi dei messaggi relativi alla proprietà di stato operativo di FIPS, fare clic sul collegamento `More details` sulla pagina FIPS.
   - Nell'area della testata dell'interfaccia Web appare un'icona a forma di scudo FIPS.
   - Tutte le funzionalità FIPS non supportate vengono disabilitate o rimosse dall'interfaccia CLI e Web.

     Per un elenco e una descrizione completi delle funzionalità FIPS non supportate, fare clic sul collegamento `More details` nella pagina FIPS.

Informazioni correlate

- sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19]
- sezione chiamata «Azioni successive alla distribuzione per la modifica della modalità FIPS» [65]
- Configurare le proprietà della modalità FIPS nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (3.2.x)*

Funzionalità non supportate quando la modalità FIPS è abilitata

Quando viene abilita la conformità a FIPS in Oracle ILOM, le seguenti funzionalità FIPS 140-2 non conformi in Oracle ILOM non sono supportate.

TABELLA 3 Funzionalità non supportate in Oracle ILOM quando la modalità FIPS è abilitata

Funzionalità della modalità FIPS non supportate	Descrizione
IPMI 1.5	Quando la modalità FIPS è abilitata e in esecuzione sul sistema, la proprietà di configurazione IPMI 1.5 viene rimossa dalle interfacce CLI e Web di Oracle ILOM. Il servizio IPMI 2.0 viene abilitato automaticamente in Oracle ILOM. IPMI 2.0 supporta sia la modalità conforme che quella non conforme a FIPS.
Compatibilità firmware per Oracle ILOM System Remote Console	La modalità FIPS in Oracle ILOM impedisce la compatibilità tra le versioni firmware precedenti e successive di Oracle ILOM Remote System Console. Ad esempio, la versione firmware 3.2.4 del client Oracle ILOM Remote System Console è compatibile con la versione firmware 3.2.3 e versioni precedenti di Oracle ILOM Remote System Console. Tuttavia, la versione firmware 3.2.2 e versioni precedenti del client Oracle ILOM Remote System Console non è compatibile con la versione firmware 3.2.4 e versioni successive di Oracle ILOM Remote System Console. **Nota -** Questo limite di compatibilità del firmware non è valido per Oracle ILOM Remote System Console Plus. L'applicazione Oracle ILOM Remote System Console Plus viene fornita sui sistemi processore di servizio più recenti quali SPARC T5 e sistemi successivi, e/o su Oracle Server x4-4, x4-8 e sistemi successivi. L'applicazione Oracle ILOM Remote System Console viene fornita sui sistemi processore di servizio meno recenti quali SPARC T3 e T4 e su Sun Server x4-2/2L/2B e sistemi precedenti.
Protocollo LDAP (Lightweight Directory Access Protocol)	Quando la modalità FIPS è abilitata e in esecuzione sul sistema, le proprietà di configurazione LDAP in Oracle ILOM vengono rimosse automaticamente dalle interfacce CLI e Web di Oracle ILOM. **Nota -** I seguenti servizi di autenticazione remota sono supportati sia nella modalità conforme che nella modalità non conforme a FIPS: Active Directory e LDAP/SSL.
RADIUS (Remote Authentication Dial In User Service)	Quando la modalità FIPS è abilitata e in esecuzione sul sistema, le proprietà di configurazione RADIUS in Oracle ILOM vengono rimosse automaticamente dalle interfacce CLI e Web di Oracle ILOM. **Nota -** I seguenti servizi di autenticazione remota sono supportati sia nella modalità conforme che nella modalità non conforme a FIPS: Active Directory e LDAP/SSL.
Protocollo SNMP (Simple Network Management Protocol) - DES e MD5	Quando la modalità FIPS è abilitata e in esecuzione sul sistema, le proprietà di configurazione SNMP per il protocollo di riservatezza DES e il protocollo di autenticazione MD5 non sono supportate nelle interfacce CLI e Web di Oracle ILOM.

Protezione di servizi e porte di rete aperte

Per verificare che i servizi e le rispettive porte di rete siano configurati in modo appropriato in Oracle ILOM, consultare i seguenti argomenti:

- sezione chiamata «Servizi e porte di rete preconfigurati» [20]
- sezione chiamata «Gestione di servizi e porte aperte non desiderati» [20]

- sezione chiamata «Configurazione di servizi e porte di rete» [22]

Servizi e porte di rete preconfigurati

Per impostazione predefinita, in Oracle ILOM molti servizi sono già attivati. In questo modo la distribuzione di Oracle ILOM avviene in maniera più rapida e veloce. Tuttavia, ciascuna porta di rete di servizio aperta sul server rappresenta un potenziale punto di attacco da parte di un utente malintenzionato. È perciò importante comprendere le impostazioni iniziali di Oracle ILOM e i relativi scopi e scegliere quali servizi sono effettivamente necessari per un sistema distribuito. Per una maggiore sicurezza, attivare solo i servizi Oracle ILOM necessari.

Nella seguente tabella vengono elencati i servizi attivati per impostazione predefinita con Oracle ILOM.

TABELLA 4 Servizi e porte abilitati per impostazione predefinita

Servizio	Porte
Reindirizzamento HTTP a HTTPS	80
HTTPS	443
IPMI	623
KVMS remoto per Oracle ILOM Remote Console	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
KVMS remoto per Oracle ILOM Remote Console Plus	5120, 5555
Tag servizio	6481
SNMP	161
Single Sign-on	11626
SSH	22

Nella seguente tabella vengono visualizzati i servizi disattivati per impostazione predefinita con Oracle ILOM.

TABELLA 5 Servizi e porte disabilitati per impostazione predefinita

Servizio	Porte
HTTP	80

Gestione di servizi e porte aperte non desiderati

Tutti i servizi Oracle ILOM possono essere disattivati, determinando in tal modo la chiusura delle rispettive porte di rete aperte per tali servizi. Benché molti servizi siano attivati per

impostazione predefinita, potrebbe essere necessario disattivare alcune funzionalità o modificare le impostazioni predefinite per proteggere l'ambiente di Oracle ILOM. È possibile disattivare qualsiasi servizio Oracle ILOM, ma in questo modo verranno perse le funzionalità. Come regola generale, attivare solo i servizi assolutamente necessari nell'ambiente di distribuzione. La perdita di funzionalità è compensata dalla maggiore sicurezza data dal minor numero di servizi di rete attivati.

Nella seguente tabella è descritto l'impatto provocato dall'attivazione o disattivazione di ciascun servizio.

TABELLA 6 Conseguenze della disattivazione dei servizi

Servizio	Descrizione	Risultato dell'attivazione/disattivazione
HTTP	Un protocollo non cifrato per l'accesso all'interfaccia Web Oracle ILOM.	L'attivazione di tale servizio garantisce migliori prestazioni rispetto all'HTTP cifrato (HTTPS). Tuttavia, l'utilizzo di tale protocollo potrebbe provocare la diffusione di informazioni sensibili in Internet senza cifratura.
HTTPS	Un protocollo cifrato per l'accesso all'interfaccia Web Oracle ILOM.	L'attivazione di tale servizio garantisce comunicazioni sicure tra un browser Web e Oracle ILOM. Tuttavia, poiché richiede la presenza di una porta di rete aperta in Oracle ILOM, si verifica una maggiore vulnerabilità agli attacchi, ad esempio all'attacco DoS (Denial of Service, negazione del servizio).
Servicetag	Un protocollo Oracle discovery utilizzato per identificare i server e semplificare le richieste di servizio	La disattivazione di tale servizio rende impossibile per Oracle Enterprise Manager Ops Center scoprire Oracle ILOM e impedisce l'integrazione in altre soluzioni di servizio automatico Oracle. Lo stato configurazione Servicetag è configurabile solo dall'interfaccia CLI di Oracle ILOM. Ad esempio, per modificare la proprietà di stato configurazione servicetag digitare: `set /SP/services/servicetag state=`*enabled*|*disabled*
IPMI	Un protocollo di gestione standard	La disattivazione di tale servizio potrebbe impedire a Oracle Enterprise Manager Ops Center, nonché ad alcuni connettori di gestione Oracle a software di terze parti, di gestire il sistema.
SNMP	Un protocollo di gestione standard per il monitoraggio dell'integrità di Oracle ILOM e delle notifiche trap ricevute.	La disattivazione di tale servizio potrebbe impedire a Oracle Enterprise Manager Ops Center, nonché ad alcuni connettori di gestione Oracle a software di terze parti, di gestire il sistema.
KVMS	Un insieme di protocolli per fornire memorizzazione, mouse, video e tastiera remoti.	La disattivazione di tale servizio rende non disponibili le funzionalità di archiviazione remota e console host, impedendo l'utilizzo da parte delle applicazioni Remote System Console (console di sistema remota) o Remote System Console Plus e Storage Redirection CLI (interfaccia della riga di comando di reindirizzamento archiviazione) di Oracle ILOM.
SSH	Un protocollo sicuro per accedere alla shell remota	La disattivazione di tale servizio impedisce l'accesso alla riga di comando sulla rete e a Oracle Enterprise Manager Ops Center di scoprire Oracle ILOM.
SSO	Una funzionalità Single Sign-On che riduce il numero di tentativi di inserimento di nome utente e password da parte di un utente.	La disabilitazione di tale servizio richiede la reimmissione di una password quando si avvia KVMS e richiede agli utenti di reimmettere una password anche durante l'esecuzione del drill-down da un modulo CMM a un blade.

Per informazioni sull'abilitazione e disabilitazione dei singoli servizi di rete, consultare il seguente argomento sezione chiamata «Configurazione di servizi e porte di rete» [22].

Configurazione di servizi e porte di rete

Per istruzioni su come configurare i servizi di gestione e le rispettive porte di rete in Oracle ILOM, vedere le procedure riportate di seguito.

- Modifica degli stati configurazione e delle porte del servizio di gestione del protocollo [22]
- Modifica dello stato configurazione e delle porte del servizio KVMS [23]
- Modifica dello stato configurazione e della porta del servizio Single Sign-On [24]

È possibile disabilitare o abilitare i servizi e le rispettive porte di rete usando l'interfaccia della riga di comando (CLI, Command-Line Interface) o l'interfaccia Web di Oracle ILOM. Le procedure descritte in questa sezione forniscono istruzioni per la navigazione Web relative a tutte le release firmware di Oracle ILOM. Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà di configurazione, consultare la documentazione appropriata riportata nella sezione Informazioni correlate che segue ciascuna procedura.

▼ Modifica degli stati configurazione e delle porte del servizio di gestione del protocollo

Prima di cominciare

- Esaminare le tabelle riportate di seguito per conoscere quali sono i servizi di protocollo e le porte di rete abilitate o disabilitate per impostazione predefinita in Oracle ILOM.
  - Tabella 4, «Servizi e porte abilitati per impostazione predefinita» Servizi e porte abilitati per impostazione predefinita
  - Tabella 5, «Servizi e porte disabilitati per impostazione predefinita» Servizi e porte disabilitati per impostazione predefinita
- Per modificare la proprietà di stato configurazione dei servizi di protocollo in Oracle ILOM è richiesto il ruolo Admin (a).

Attenersi alla procedura riportata di seguito per modificare la proprietà di stato configurazione di un servizio di rete.

1. **Nell'interfaccia Web di Oracle ILOM passare ai servizi Management Access.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Configuration -> System Management Access;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access.**

2. **Fare clic sulla scheda Management Access -> servizio appropriata tra quelle elencate di seguito.**

Management Access ->	Descrizione
Web Server	Utilizzare la pagina Web Server per gestire lo stato configurazione del servizio e le assegnazioni delle porte per l'accesso alla gestione dei protocolli HTTP e HTTPS.
IPMI	Utilizzare la pagina IPMI per gestire lo stato configurazione del servizio e le proprietà delle porte per l'accesso alla gestione del protocollo IPMI.
SNMP	Utilizzare la pagina SNMP per gestire lo stato configurazione del servizio e le proprietà delle porte per l'accesso alla gestione del protocollo SNMP.
SSH	Utilizzare la pagina SSH per gestire la proprietà di stato configurazione del servizio per l'accesso alla gestione della shell sicura.

3. **Modificare la proprietà di stato configurazione nella pagina Management Access -> servizio, quindi fare clic su Save per applicare la modifica.**

Tenere presente che la disabilitazione della proprietà di stato configurazione di un servizio di protocollo determina la chiusura della rispettiva porta di rete del servizio di protocollo, impedendo quindi l'uso del servizio di protocollo con Oracle ILOM.

Informazioni correlate

- Servizi di gestione e proprietà predefinite della rete nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Servizi di gestione e proprietà predefinite della rete nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Configurazione delle impostazioni di rete nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Configurazione delle impostazioni di rete nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Modifica dello stato configurazione e delle porte del servizio KVMS

Prima di cominciare

- In Oracle ILOM la proprietà di stato configurazione del servizio KVMS è abilitata per impostazione predefinita. Per un elenco delle porte di rete aperte associate al servizio KVMS, vedere Tabella 4, «Servizi e porte abilitati per impostazione predefinita».
- Per modificare la proprietà di stato configurazione di KVMS in Oracle ILOM è richiesto il ruolo Admin (a).

1. **Passare alla scheda KVMS nell'interfaccia Web di Oracle ILOM.**

Ad esempio:

- **nell'interfaccia Web 3.0.x fare clic su Remote Control -> KVMS;**

- **nell'interfaccia Web 3.1 e versioni successive fare clic su Remote Console -> KVMS.**

2. **Nella scheda KVMS modificare la proprietà di stato configurazione di KVMS, quindi fare clic su Save per applicare la modifica.**

   Tenere presente che la disabilitazione della proprietà di stato configurazione determina la chiusura delle porte di rete aperte del rispettivo servizio KVMS, impedendo quindi l'uso: a) della console host remota e b) di Oracle ILOM Remote Console e dell'interfaccia CLI Oracle ILOM Remote Storage oppure di Oracle ILOM Remote Console Plus.

Informazioni correlate

- Configurare le impostazioni KVMS del client locale nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Configurare le impostazioni KVMS del client locale nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Task di impostazione iniziale nel manuale *Oracle ILOM 3.0 Remote Redirection Console - Web and CLI Guide*

▼ Modifica dello stato configurazione e della porta del servizio Single Sign-On

Prima di cominciare

- In Oracle ILOM la proprietà di stato configurazione del servizio SSO (Single Sign-On) e la rispettiva porta di rete (1126) sono abilitate per impostazione predefinita.
- Per modificare la proprietà di stato configurazione del servizio SSO in Oracle ILOM è richiesto il ruolo Admin (a).

1. **Passare alla scheda User Account nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su User Management -> User Account;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> User Account.**

2. **Nella pagina User Account modificare la proprietà di stato configurazione di SSO, quindi fare clic su Save per applicare la modifica.**

   Tenere presente che la disabilitazione della proprietà di stato configurazione di SSO in Oracle ILOM determina: a) la chiusura della porta di rete SSO aperta, b) la richiesta agli utenti di reimmettere la password all'avvio di una console KVMS e c) la possibilità per gli utenti CMM di passare a un SP blade server senza dover reimmettere la password.

Informazioni correlate

- Servizio Single Sign-On nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Servizio Single Sign-On nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Configurazione di Single Sign-On nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Configurazione di Single Sign-On nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Protezione dell'accesso utente in Oracle ILOM

Per proteggere l'accesso utente in Oracle ILOM, consultare i seguenti argomenti:

- sezione chiamata «Evitare la creazione di account utente condivisi» [25]
- sezione chiamata «Assegnazione di privilegi basati sui ruoli» [26]
- sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27]
- sezione chiamata «Servizi di autenticazione remota e profili di sicurezza» [28]
- sezione chiamata «Configurazione dell'accesso utente per una maggiore sicurezza» [30]

Evitare la creazione di account utente condivisi

Mantenere un ambiente sicuro evitando di creare account condivisi. Gli account condivisi sono account utente che condividono una password dell'account utente fornita. Anziché creare account condivisi, il metodo ideale per gestire gli account utente è quello di creare una password univoca per ciascun utente che ha accesso a Oracle ILOM. Verificare che solo un utente conosca ciascuna combinazione di account utente e password.

Nota - Oracle ILOM supporta al massimo 10 account utente locali. Se è necessario che più utenti accedano a Oracle ILOM, è possibile configurare i servizi di directory, come LDAP o Active Directory, per supportare più account mediante un database centralizzato. Per ulteriori informazioni, vedere sezione chiamata «Servizi di autenticazione remota e profili di sicurezza» [28].

Dopo aver impostato i singoli account utente con password univoche, l'amministratore di sistema deve assicurarsi che una password univoca sia stata assegnata all'account `root` preconfigurato dell'amministratore. In caso contrario, in assenza di una password univoca, l'account `root` preconfigurato dell'amministratore viene considerato un account condiviso. Per impedire a utenti non autorizzati di utilizzare l'account `root` preconfigurato dell'amministratore,

è necessario modificare la password o rimuovere l'account `root` preconfigurato da Oracle ILOM. Per ulteriori informazioni sull'account `root` preconfigurato dell'amministratore, vedere Modifica della password predefinita per l'account `root` al primo login [31].

Per ulteriore assistenza su come impostare account sicuri con password univoche, consultare sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27].

Per informazioni sulla configurazione degli account utente, vedere sezione chiamata «Configurazione dell'accesso utente per una maggiore sicurezza» [30].

Assegnazione di privilegi basati sui ruoli

A tutti gli account utente Oracle ILOM viene assegnato un insieme di privilegi basati sui ruoli. Tali privilegi basati sui ruoli forniscono accesso a funzionalità distinte all'interno di Oracle ILOM. È possibile configurare un account utente in modo che l'utente possa monitorare il sistema, ma non apportare modifiche alla configurazione. In alternativa, è possibile consentire a un utente di modificare la maggior parte delle opzioni di configurazione, ad eccezione della creazione e della modifica degli account utente. È inoltre possibile limitare l'accesso all'alimentazione del server e alla console remota. È importante comprendere i livelli dei privilegi e assegnarli in modo appropriato agli utenti all'interno dell'organizzazione.

Nella seguente tabella vengono elencati i privilegi che è possibile assegnare a un singolo account utente di Oracle ILOM.

TABELLA 7 Descrizione dei privilegi dell'account utente

Ruolo	Descrizione
`Admin` (`a`)	Consente a un utente di modificare tutte le opzioni di configurazione di Oracle ILOM, ad eccezione di quelle esplicitamente autorizzate da altri privilegi (come User Management).
`User Management` (`u`)	Consente a un utente di aggiungere e rimuovere utenti, modificare password utenti e configurare i servizi di autenticazione. Un utente con tale ruolo può creare un secondo account utente completo di tutti i privilegi e, di conseguenza, tale ruolo prevede livelli di privilegio maggiori rispetto a tutti i ruoli utente.
`Console` (`c`)	Consente a un utente di accedere in remoto alla console host. Tale accesso alla console remota potrebbe consentire all'utente di accedere a BIOS o OpenBoot PROM (OBP), offrendogli la possibilità di modificare il comportamento di boot in modo da ottenere l'accesso al sistema.
`Reset and Host Control` (`r`)	Consente a un utente di controllare l'alimentazione host e ripristinare Oracle ILOM.
`Read-only` (`o`)	Consente a un utente di acquisire l'accesso in sola lettura alle interfacce utente Oracle ILOM. Questo accesso è consentito a tutti gli utenti e garantisce la visualizzazione di log e informazioni ambientali, nonché delle impostazioni di configurazione.

Per ulteriori informazioni sulla creazione di un account utente locale e sull'assegnazione dei privilegi basati sui ruoli, vedere Creare account utente locali con privilegi basati sui ruoli [33].

Linee guida di sicurezza per la gestione di account utente e password

Prendere in considerazione le linee guida di sicurezza riportate di seguito durante la gestione di account utente e password.

- sezione chiamata «Linee guida per la gestione di account utente» [27]
- sezione chiamata «Linee guida per la gestione delle password» [28]

Linee guida per la gestione di account utente

Linee guida per la gestione degli account utente	Descrizione
Non incoraggiare mai la condivisione degli account utente	Creare sempre un account separato per ciascun utente di Oracle ILOM. Oracle ILOM supporta al massimo 10 account utente locali. Se si gestisce un sito più grande e sono necessari più di 10 account utente, considerare la possibilità di utilizzare un servizio di autenticazione utente di terze parti, ad esempio LDAP o Active Directory. Per ulteriori informazioni sull'implementazione dell'autenticazione utente in Oracle ILOM mediante un servizio di autenticazione esterno, vederesezione chiamata «Servizi di autenticazione remota e profili di sicurezza» [28].
Selezionare nomi conformi per gli account utente locali	Quando si seleziona un nome utente per un account utente Oracle ILOM locale, il nome utente deve avere le seguenti caratteristiche: ■ Deve avere una lunghezza compresa tra 4 e 16 caratteri (il primo carattere deve essere una lettera). ■ Deve essere univoco all'interno dell'organizzazione. ■ Non deve contenere spazi, un punto (.) o due punti (:).
Selezionare password conformi per gli account utenti locali	Quando si seleziona una password per un account utente Oracle ILOM locale, la password deve avere le seguenti caratteristiche: ■ Deve sempre essere una password efficace contenente al massimo 16 caratteri. ■ Deve contenere una combinazione di caratteri minuscoli e maiuscoli, nonché uno o due caratteri speciali in modo da creare una password complessa efficace. ■ Non deve contenere spazi, un punto (.) o due punti (:). ■ Deve essere conforme ai criteri di gestione delle password dell'azienda. Per ulteriori informazioni sulla gestione delle password in Oracle ILOM, vedere sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27].
Limitare i privilegi degli account utente in base al ruolo lavorativo (*Principi di privilegio minimo*)	Il principio di privilegio minimo richiede che, per motivi di sicurezza, a un utente venga assegnata la minore quantità di privilegi per eseguire il proprio lavoro. Responsabilità, ruoli e altri privilegi troppo elevati (soprattutto nelle fasi iniziali del ciclo di vita di un'organizzazione) possono portare a rischi di abusi del sistema. Verificare periodicamente i privilegi degli utenti per stabilirne l'importanza per le responsabilità lavorative correnti di ciascun utente. Oracle ILOM consente di controllare i privilegi di ciascun utente. Verificare che a ogni account utente vengano assegnate le autorizzazioni appropriate per il ruolo utente, in base al ruolo lavorativo. Per informazioni su come creare un account utente con privilegi basati sui ruoli, vedere: Creare account utente locali con privilegi basati sui ruoli [33]

Linee guida per la gestione delle password

Linee guida per la gestione delle password	Descrizione
Modifica della password predefinita `root` (`changeme`) subito dopo il login iniziale	Per abilitare il primo login e il primo accesso a Oracle ILOM, con il sistema viene fornito un account amministratore `root` locale. Per creare un ambiente sicuro, è necessario modificare la password di amministratore fornita (`changeme`) dopo il login iniziale a Oracle ILOM. L'accesso non autorizzato all'account amministratore `root` consente a un utente accesso illimitato a tutte le funzionalità di Oracle ILOM. Per questo motivo è necessario indicare una password complessa e sicura.
Modifica delle password degli account di Oracle ILOM a intervalli regolari	Per impedire attività dannose e garantire che le password siano sempre conformi ai criteri delle password correnti, è necessario modificare regolarmente tutte le password di Oracle ILOM.
Applicare procedure comuni per la creazione di password efficaci e complesse	Applicare le procedure comuni riportate di seguito per creare password efficaci e complesse. ■ Non creare una password di lunghezza inferiore a 16 caratteri. ■ 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. ■ Per una maggiore sicurezza, è opportuno mascherare sempre le nuove password immesse nell'interfaccia CLI utilizzando la seguente sintassi: **`set [`***SP*|*CMM*`]/users/root password=`**[*non digitare la password, premere Invio*] - oppure- **`set [`***SP*|*CMM*`]/users/newuser password=`**[*non digitare la password, premere Invio*] Viene richiesto di immettere il nuovo valore della password nell'interfaccia CLI, mascherando la password in modo che non venga visualizzata.
Impostazione di limitazioni per il criterio della password per gli utenti locali (disponibile per il firmware 3.2.5 e versioni successive)	Applicare un criterio della password per tutti gli account utente locali. Per maggiori dettagli, vedere Impostazione di limitazioni per il criterio della password per tutti gli utenti locali (3.2.5 e versioni successive) [30]
Consultare il responsabile della sicurezza IT per i criteri di gestione delle password	Consultare il responsabile della sicurezza IT per assicurare la conformità ai requisiti e ai criteri di gestione delle password dell'azienda.

Servizi di autenticazione remota e profili di sicurezza

Oracle ILOM può essere configurato per usare un'area di memorizzazione utenti centralizzata esterna invece di dover configurare gli utenti locali su ciascuna istanza di Oracle ILOM. In

questo modo è possibile modificare e creare in maniera centralizzata le credenziali utente e consentire agli utenti di accedere a numerosi sistemi diversi.

Prima di scegliere e configurare un servizio di autenticazione, comprendere il funzionamento di questi servizi e le modalità di configurazione. Oltre all'autenticazione, ciascuno dei servizi supportati fornisce la possibilità di configurare regole di autorizzazione che definiscono le modalità con cui i privilegi utente di Oracle ILOM vengono assegnati a un determinato utente remoto. Assicurarsi che venga assegnato il corretto privilegio o ruolo utente.

Nella seguente tabella vengono descritti i servizi di autenticazione utente supportati da Oracle ILOM.

TABELLA 8 Servizi di autenticazione remota e profili di sicurezza

Nome servizio	Profilo di sicurezza	Informazioni
Active Directory	Elevato	■ Questo servizio è sicuro per impostazione predefinita. ■ L'utilizzo di una modalità di certificazione rigorosa richiede un server di certificazione, ma aggiunge un ulteriore livello di sicurezza.
Lightweight Directory Access Protocol/Secure Socket Layer (LDAP/SSL)	Elevato	■ Questo servizio è sicuro per impostazione predefinita. ■ L'utilizzo di una modalità di certificazione rigorosa richiede un server di certificazione, ma aggiunge un ulteriore livello di sicurezza.
Legacy LDAP	Basso	■ Utilizzare questo servizio su reti sicure e private in cui non sono presenti utenti malintenzionati.
Remote Authentication Dial In User Service (RADIUS)	Basso	■ Utilizzare questo servizio su reti sicure e private in cui non sono presenti utenti malintenzionati.

I servizi con un profilo di sicurezza elevato possono essere utilizzati in ambienti molto sicuri, poiché sono protetti da certificati e altre forme di cifratura sicura per la protezione del canale. I servizi con un basso profilo di sicurezza sono disattivati per impostazione predefinita. Attivare questi bassi profili di sicurezza solo se ne conoscono i limiti per la sicurezza.

Per informazioni sulla configurazione dei servizi di autenticazione remota, consultare la documentazione appropriata di Oracle ILOM riportata di seguito.

- Impostazione e gestione degli account utente nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Impostazione e gestione degli account utente nella *guida relativa a configurazione e gestione* di Oracle ILOM 3.1
- Gestione degli account utente nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Gestione degli account utente nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Configurazione dell'accesso utente per una maggiore sicurezza

Consultare gli argomenti riportati di seguito relativi a come configurare al meglio l'accesso utente di Oracle ILOM per una maggiore sicurezza.

È possibile configurare le proprietà di accesso utente in Oracle ILOM utilizzando l'interfaccia della riga di comando (CLI, Command-Line Interface) o l'interfaccia Web. Le procedure descritte in questa sezione forniscono istruzioni per la navigazione Web relative a tutte le release firmware di Oracle ILOM. Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà di configurazione, consultare la documentazione appropriata riportata nella sezione Informazioni correlate che segue ciascuna procedura.

▼ Impostazione di limitazioni per il criterio della password per tutti gli utenti locali (3.2.5 e versioni successive)

Oracle ILOM, a partire dalla release 3.2.5 del firmware, applica un criterio della password per tutti gli account utente locali. Il criterio della password include un insieme di limitazioni. Gli amministratori di sistema possono scegliere di utilizzare le proprietà predefinite disponibili o di modificarle per soddisfare le esigenze del criterio della password.

Nota - Le modifiche apportate alle proprietà dei criteri della password devono essere impostate prima della creazione degli account utente locali. Qualora le proprietà del criterio della password vengano modificate dopo la configurazione degli account utente locali, Oracle ILOM eseguirà automaticamente le seguenti operazioni: 1) rimozione della configurazione di tutti gli account utente locali; 2) ripristino dell'account root inizialmente fornito con il sistema.

Informazioni preliminari

- Per configurare le proprietà del criterio della password è richiesto il ruolo Admin (a).
- Il criterio della password si applica solo agli account utente locali. Non ha impatto sugli account del servizio di autenticazione degli utenti remoti come LDAP o Active Directory.

- Al momento di salvare le modifiche alle proprietà del criterio della password, si verifica quanto indicato di seguito.
  - Tutte le configurazioni dell'account utente locale vengono eliminate da Oracle ILOM.
  - Viene ripristinato l'account utente locale predefinito (root) fornito con il sistema.
  - Al momento del login iniziale, all'utente root viene richiesto di modificare la password dell'account root.

Attenersi alle istruzioni basate sul Web riportate di seguito per impostare un criterio della password per tutti gli utenti locali.

Nota - Per istruzioni sul criterio della password dell'interfaccia CLI, fare clic sul riferimento Oracle ILOM Administration Guide riportato nella sezione Informazioni correlate di questa procedura.

---

1. **Per visualizzare le limitazioni del criterio della password in Oracle ILOM, fare clic su ILOM Administration > User Management > Password Policy.**
2. **Per ulteriori istruzioni su come modificare le limitazioni del criterio della password, fare clic sul collegamento More Details... nella pagina Password Policy.**
3. **Per salvare le modifiche, fare clic su Save.**

Informazioni correlate

- «Modify Password Policy Restrictions for Local Users» in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

▼ Modifica della password predefinita per l'account `root` al primo login

Per abilitare il primo login e il primo accesso a Oracle ILOM, con il sistema vengono forniti un account amministratore (`root`) preconfigurato e una password predefinita (`changme`). Per impedire l'accesso non autorizzato a Oracle ILOM, al primo login è necessario modificare la password predefinita (`changeme`) fornita con l'account `root` preconfigurato. In caso contrario, l'account `root` preconfigurato e la password predefinita (`changeme`) agiranno come un account condiviso, abilitando l'accesso amministratore per qualsiasi utente.

Attenersi alle istruzioni basate sul Web riportate di seguito per modificare la password predefinita (`changeme`) fornita con l'account `root` preconfigurato dell'amministratore.

Nota - Se non si ha accesso all'account root preconfigurato ed è necessario accedere alle funzionalità di amministratore di Oracle ILOM, contattare l'amministratore di sistema per richiedere un account utente con privilegi di amministratore.

Informazioni preliminari

- Esaminare le sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27].

  Nota - È fondamentale assegnare una password efficace e sicura all'account root per impedire l'accesso non autorizzato alle funzionalità di Oracle ILOM. Una password efficace deve contenere una combinazione di caratteri minuscoli e maiuscoli e almeno un carattere speciale, ad esempio % oppure $.

- Per modificare le password degli account utente locali in Oracle ILOM è richiesto il ruolo User Management (u).

1. **Passare alla pagina User Account nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su User Management -> User Accounts;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su User Management -> User Accounts.**

2. **Nella pagina User Account fare clic su Edit per l'account root.**
   Viene visualizzata la finestra di dialogo Edit: User Root.

3. **Nella finestra di dialogo Edit: User Root eseguire le operazioni riportate di seguito.**

   - **Immettere una password univoca nella casella di testo New Password, quindi reimmettere la stessa password nella casella di testo Confirm New Password.**
   - **Fare clic su Save per applicare la modifica.**

Informazioni correlate

- Configurazione di un account utente locale nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Configurazione di un account utente locale nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*

- Modifica di un account utente nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modifica di un account utente nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- sezione chiamata «Presenza di sicurezza fisica per la reimpostazione della password predefinita dell'account `root`» [63]

▼ Creare account utente locali con privilegi basati sui ruoli

Prima di cominciare

Oracle ILOM supporta la creazione e la memorizzazione di un massimo di 10 account utente locali su un singolo SP o modulo CMM (Chassis Monitoring Module). Agli utenti di Oracle ILOM viene assegnato un insieme di privilegi che garantisce l'utilizzo delle funzionalità nella misura in cui tale uso è consentito dall'account configurato di cui dispongono.

Nota - In alternativa, gli amministratori di sistema possono configurare Oracle ILOM in modo che supporti ulteriori account utente tramite un servizio di autenticazione remota. Nel caso di una configurazione di servizio di autenticazione remota, i login, le password e i privilegi provengono da un'area di memorizzazione utenti esterna. Per ulteriori informazioni, vedere sezione chiamata «Servizi di autenticazione remota e profili di sicurezza» [28].

Per istruzioni basate sul Web relative alla configurazione di un account utente locale con privilegi di accesso basati sui ruoli, vedere di seguito.

Informazioni preliminari

- Esaminare le sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27].
- Rivedere i browser Web supportati in Tabella 7, «Descrizione dei privilegi dell'account utente» per Oracle ILOM.
- Per creare un account utente locale con privilegi in Oracle ILOM è richiesto il ruolo User Management (u).

1. **Passare alla pagina User Account nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su User Management -> User Accounts;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su User Management -> User Accounts.**

2. **Nella pagina User Account fare clic su Add.**
   Viene visualizzata la finestra di dialogo Add User.

3. **Nella finestra di dialogo Add User eseguire le operazioni riportate di seguito.**

a. **Specificare il nome dell'utente nella casella di testo User Name.**

b. **Nell'elenco a discesa Roles selezionare il profilo del ruolo utente appropriato (Administrator, Operator o Advanced).**

c. **Immettere una password univoca nella casella di testo New Password, quindi reimmettere la stessa password nella casella di testo Confirm New Password.**

d. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Creare un account utente e assegnare un ruolo utente nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Creare un account utente e assegnare un ruolo utente nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Aggiunta di un account utente e assegnazione di ruoli nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Aggiunta di un account utente e assegnazione di ruoli nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Bloccare l'accesso host all'uscita da una sessione KVMS

Poiché durante l'utilizzo del servizio KVMS remoto la console host è considerata una risorsa di rete condivisa, se un utente esegue il login alla console host e chiude l'applicazione Oracle ILOM Remote System Console, Remote System Console Plus o CLI Storage Redirection senza aver eseguito il logout dal sistema operativo host, un secondo utente che esegue la connessione alla stessa console mediante KVMS remoto potrà utilizzare la sessione del sistema operativo precedentemente autenticata. Per questo motivo, Oracle ILOM consente di bloccare automaticamente il sistema operativo host ogni volta che viene disconnessa una sessione del servizio KVMS remoto. Per una maggiore sicurezza, abilitare o configurare tale funzionalità in Oracle ILOM.

Per bloccare il desktop host remoto dopo aver terminato una sessione KVMS, vedere le istruzioni basate sul Web riportate di seguito. Per informazioni su come abilitare la funzionalità di blocco host, consultare la *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x).*

Informazioni preliminari

- Per modificare la proprietà della modalità blocco host in Oracle ILOM è richiesto il ruolo Console (c).

- Per usare la funzionalità modalità blocco host in Oracle ILOM è richiesto il firmware 3.0.4 o versione successiva.
- La funzionalità modalità blocco host è disabilitata per impostazione predefinita.

1. **Passare alla pagina KVMS nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Remote Console -> KVMS;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su Remote Control -> KVMS.**

2. **Nella sezione Host Lock Settings della pagina KVMS eseguire una delle operazioni riportate di seguito.**

   - **Specificare una modalità di blocco (Windows, Custom o Disabled).**
   - **Fare clic su Save per applicare la modifica.**

Informazioni correlate

- Bloccare il desktop host nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Bloccare il desktop host nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Blocco di KVMS nel manuale *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide*

▼ Limitazione delle sessioni KVMS visualizzabili per Remote System Console Plus (3.2.4 o versioni successive)

A partire dalla release firmware 3.2.4, un utente Remote System Console Plus primario può impedire ad altri utenti della sessione collegata su SP di visualizzare dati riservati immessi durante una sessione di reindirizzamento video limitando il conteggio massimo delle sessioni client (Maximum Client Session Count) a un solo (1) visualizzatore di sessioni. Per impostazione predefinita, la proprietà Maximum Client Session Count per Oracle ILOM Remote System Console Plus è impostata su quattro visualizzatori di sessione.

Per modificare la proprietà Maximum Client Session Count per Oracle ILOM Remote System Console Plus, vedere le istruzioni basate sul Web riportate di seguito.

Prima di cominciare

- La proprietà KVMS Maximum Client Session Count per Oracle ILOM Remote System Console Plus è disponibile a partire dalla release firmware 3.2.4 o versioni successive.

Nota - La proprietà KVMS Maximum Client Session Count non è configurabile sui sistemi che supportano Oracle ILOM Remote Console.

- L'applicazione Oracle ILOM Remote System Console Plus è disponibile solo sui sistemi SP appena rilasciati, a partire dalla release firmware 3.2.1.
- Per modificare la proprietà Maximum Client Session Count di KVMS in Oracle ILOM è richiesto il ruolo Console (`c`).
- Alla reimpostazione della proprietà Maximum Client Session Count in Oracle ILOM, tutte le sessioni video attive di Oracle ILOM Remote System Console Plus sul processore SP verranno terminate.
- Per impostazione predefinita, è possibile avviare al massimo quattro sessioni di reindirizzamento video di Remote System Console Plus, per ogni SP, dalla pagina Redirection in Oracle ILOM.

1. **Passare alla pagina KVMS nell'interfaccia Web di Oracle ILOM facendo clic su Remote Console -> KVMS.**
2. **Nella pagina KVMS modificare la proprietà Maximum Client Session Count (valore accettabile: *4* (predefinito)|*1*|*2*|*3*).**
3. **Fare clic su Save per applicare la modifica.**

Informazioni correlate

- Proprietà di reindirizzamento dei dispositivi remoti nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*

▼ Accesso sicuro al sistema con il messaggio di avvio di login (3.0.8 e versioni successive)

A partire dalla release firmware 3.0.8, Oracle ILOM consente agli amministratori di sistema di visualizzare un messaggio di avvio a tutti gli utenti al momento del login alle interfacce CLI e Web di Oracle ILOM. L'uso di un messaggio di avvio di login agevola la protezione dall'accesso non autorizzato al sistema da parte di dispositivi remoti e avverte gli utenti autorizzati e legittimi dei loro obblighi in materia di utilizzo accettabile del sistema.

Il messaggio di avvio implementato dall'utente deve essere scritto rispettando i criteri di sicurezza delle informazioni. Per ulteriori linee guida sul messaggio scritto, consultare l'amministratore del sito o il responsabile della sicurezza.

Per visualizzare un messaggio di avvio a tutti gli utenti durante o dopo il login, vedere le istruzioni basate sul Web riportate di seguito.

Prima di cominciare

- Per creare un messaggio di avvio è richiesto il ruolo Admin (a).
- Il messaggio di avvio è disponibile per la configurazione a partire dalla release firmware 3.0.8 di Oracle ILOM e versioni successive.
- Gli amministratori possono configurare il messaggio di avvio da visualizzare sulla pagina Login o in una finestra di dialogo visualizzata dopo che l'utente ha eseguito il login a Oracle ILOM.

1. **Passare alla pagina Banner Message nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su System Information -> Banner Messages;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> Banner Messages.**

2. **Per determinare come configurare un messaggio di avvio, nella pagina Banner Message fare clic sul collegamento** *More Details...***.**

   Per istruzioni per l'interfaccia CLI, consultare il manuale *Oracle ILOM Administration Guide* applicabile disponibile nella sezione Informazioni correlate di questa procedura.

3. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- «Management of Banner Messages at Log-In» in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- Gestione dei messaggi di avvio nel manuale *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*
- Proprietà di configurazione del messaggio di avvio nel manuale *Oracle ILOM 3.1 Configuration and Maintenance Guide*
- Visualizzazione di un messaggio di avvio nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Visualizzazione di un messaggio di avvio nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Configurazione delle interfacce di Oracle ILOM per una maggiore sicurezza

Per configurare le interfacce di Oracle ILOM per una maggiore sicurezza, consultare i seguenti argomenti:

Configurare l'interfaccia Web per una maggiore sicurezza

Consultare gli argomenti riportati di seguito relativi a come configurare al meglio l'interfaccia Web di Oracle ILOM per una maggiore sicurezza.

Nota - È possibile configurare le proprietà dell'interfaccia di gestione Web in Oracle ILOM utilizzando usando l'interfaccia della riga di comando (CLI, Command-Line Interface) o l'interfaccia Web. Le procedure descritte in questa sezione forniscono istruzioni per la navigazione Web relative a tutte le release firmware di Oracle ILOM. Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà di configurazione, consultare la documentazione appropriata riportata nella sezione Informazioni correlate che segue ciascuna procedura.

Migliorare la sicurezza mediante un certificato e una chiave privata SSL trusted

I certificati SSL (Secure Socket Layer) sono utilizzati per la cifratura di comunicazioni su una rete e per garantire l'autenticità di un server o di un client. In Oracle ILOM è disponibile un certificato SSL autofirmato che consente al protocollo HTTP su SSL di essere utilizzato immediatamente, senza la necessità di caricare un certificato. Quando si esegue la connessione all'interfaccia Web Oracle ILOM per la prima volta, all'utente viene comunicato l'utilizzo di un certificato autofirmato e ne viene richiesta la conferma di utilizzo. Utilizzando il certificato fornito, tutte le comunicazioni tra il browser Web e Oracle ILOM sono totalmente cifrate.

Tuttavia, è anche possibile creare e caricare un certificato trusted per aumentare la sicurezza. Per certificato attendibile si intende un certificato concesso in collaborazione con un'autorità di

certificazione sicura. L'utilizzo di un certificato trusted da parte di un'autorità di certificazione nota garantisce l'autenticità del server Web Oracle ILOM. I certificati non attendibili (autofirmati) possono provocare attacchi MITM (man-in-the-middle).

Per ottenere e caricare un certificato autofirmato temporaneo o un certificato firmato da un'autorità di certificazione, attenersi alle procedure riportate di seguito.

- Ottenere un certificato e una chiave privata SSL mediante OpenSSL [39]
- Caricamento di un certificato e di una chiave privata SSL personalizzati in Oracle ILOM [40]

▼ Ottenere un certificato e una chiave privata SSL mediante OpenSSL

Questa procedura è una descrizione semplificata della modalità di creazione di un certificato e una chiave privata SSL mediante il toolkit OpenSSL.

Nota - Oracle ILOM *non* richiede l'uso di OpenSSL per generare certificati SSL. OpenSSL viene utilizzato in questa procedura solo a scopo dimostrativo. Per la generazione di certificati SSL sono disponibili altri strumenti.

La necessità di usare un certificato autofirmato temporaneo o un certificato firmato da un'autorità di certificazione deve essere stabilita dall'amministratore del sito o dal responsabile della sicurezza. Qualora non sia necessario ottenere un certificato SSL (autofirmato temporaneo o firmato da un'autorità di certificazione), è possibile seguire le istruzioni della riga di comando OpenSSL di esempio riportate di seguito.

Nota - Se sono necessarie ulteriori istruzioni OpenSSL per generare il certificato SSL, si consiglia di consultare la documentazione per l'utente fornita insieme al toolkit OpenSSL.

---

1. **Creare una condivisione di rete o una directory locale in cui memorizzare il certificato e la chiave privata.**

2. **Per generare una nuova chiave privata RSA mediante il toolkit OpenSSL, digitare:**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   Dove <*foo*> equivale al nome della chiave privata.

   Nota - La chiave privata è una chiave RSA a 2048 bit memorizzata in formato PEM in modo da renderla leggibile come testo ASCII.

   ---

3. **Per generare una richiesta di firma certificato (CSR, Certificate Signing Request) mediante il toolkit OpenSSL, digitare:**

`openssl req -new -key <foo>.key -out <foo>.csr`

Dove <*foo*> equivale al nome della richiesta di firma certificato.

Nota - Durante la generazione della richiesta CSR, verranno richieste diverse informazioni.

A questo punto, nella directory di lavoro corrente deve essere visualizzato un file `<foo>.csr`.

4. **Per generare un certificato SSL, eseguire una delle operazioni riportate di seguito.**

   - **Generare un certificato autofirmato temporaneo (valido per 365 giorni).**

     Il certificato SSL autofirmato viene generato dalla chiave privata `server.key` e dai file `server.csr`.

     Usando il toolkit OpenSSL digitare:

     `openssl x509 -req -days 365 -in <foo>.csr`

     `-signkey <foo>.key -out <foo>.cert`

     Dove <*foo*> equivale al nome assegnato alla chiave privata (`.key`) o al certificato (`.cert`).

     Nota - Questo certificato temporaneo genererà un errore nel browser client a dimostrazione del fatto che l'autorità che firma il certificato è sconosciuta e non trusted. Se questo errore è inaccettabile, si consiglia di richiedere all'autorità di certificazione di emettere un certificato firmato.

   - **Ottenere un certificato firmato ufficialmente da un provider CA (Certificate Authority).**

     Inviare la richiesta di firma certificato (`<foo>.csr`) a un provider CA di certificati SSL. La maggior parte dei provider CA richiedono che l'utente tagli e incolli l'output CSR in una schermata dell'applicazione Web. La ricezione del certificato firmato può in genere richiedere fino a sette giorni lavorativi.

5. **Caricare il nuovo certificato e la nuova chiave privata SSL in Oracle ILOM.**

   Vedere le seguenti istruzioni: Caricamento di un certificato e di una chiave privata SSL personalizzati in Oracle ILOM [40].

▼ Caricamento di un certificato e di una chiave privata SSL personalizzati in Oracle ILOM

Informazioni preliminari

- Per modificare le proprietà del server Web in Oracle ILOM è richiesto il ruolo Admin (a).

- Ottenere il nuovo certificato (autofirmato temporaneo o firmato dall'autorità di certificazione) e la nuova chiave privata HTTPS. Per istruzioni sull'uso del toolkit OpenSSL, vedere Ottenere un certificato e una chiave privata SSL mediante OpenSSL [39].
- Verificare di poter accedere al nuovo certificato e alla nuova chiave privata HTTPS tramite la rete o il file system locale.

1. **Passare alla pagina SSL Certificate nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Configuration -> System Management Access -> SSL Certificate;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> -> SSL Certificate.**

2. **Nella pagina del server SSL eseguire le operazioni riportate di seguito.**

   a. **Fare clic sul pulsante Load Certificate per caricare il file Custom Certificate designato nelle proprietà File Transfer Method.**

   b. **Fare clic sul pulsante Load Custom Private Key per caricare il file Custom Private Key designato nelle proprietà File Transfer Method.**

   c. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Proprietà di configurazione di certificati e chiavi private SSL nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione di certificati e chiavi private SSL nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Caricamento di un certificato SSL nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Caricamento di un certificato SSL nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

▼ Abilitazione delle proprietà di cifratura SSL e TLS più efficaci

Oracle ILOM supporta i protocolli di cifratura Secure Socket Layer (SSLv3 e TLS v1.0, v1.1 e v1.2) più efficaci con le cifrature più forti. Tuttavia, in alcuni casi potrebbe essere necessario abilitare il protocollo SSLv2 o cifrature deboli per supportare i browser Web meno recenti.

Attenersi a questa procedura per impostare le proprietà SSL e TLS in Oracle ILOM per soddisfare i requisiti dei criteri di sicurezza.

Nota - Il supporto dei protocolli SSL e TLSv1.0 è diventato disponibile a partire dalla release firmware 3.1.0. Il supporto dei protocolli TLS v1.1e v1.2 è diventato disponibile in Oracle ILOM a partire dalla release firmware 3.2.4.

Informazioni preliminari

- Per modificare le proprietà del server Web in Oracle ILOM è richiesto il ruolo Admin (a).
- L'impostazione predefinita per la proprietà TLS in Oracle ILOM dipende dalla versione del firmware attualmente installata sul server.

Firmware	Impostazione predefinita di TLS
3.1.x, 3.2.1.x, 3.2.2.x e 3.2.3.x	TLS v1.0 abilitata
3.2.4 e versioni successive	TLS v1.0, v1.1 e v1.2 abilitate

- Per le release del firmware di Oracle ILOM *precedenti* la 3.2.4, la proprietà SSLv3 viene abilitata per impostazione predefinita.

Nota - A causa di una vulnerabilità della sicurezza rilevata con SSLv3, è opportuno disabilitare SSLv3 finché il problema non verrà risolto. Per maggiori dettagli, consultare il documento di Oracle: MOS SSLv3 Vulnerability Article.

- Per la release 3.2.4.x e successive del firmware di Oracle ILOM, l'impostazione predefinita di SSLv3 dipende dal modello del server e dalla versione del firmware 3.2.4.x installata.

Modello del server	Firmware	Impostazione predefinita di SSLv3
SPARC T3, T4, T5, M5, M6	3.2.4.1	SSLv 3 disabilitata
X4-2 X4-2L X4-2B	3.2.4.20 (x4-2) 3.2.4.22 (x4-2L) 3.2.24.24 (X4-2B)	SSLv3 abilitata Per maggiori dettagli, consultare MOS SSLv3 Vulnerability Article.
X4-4 X4-8	3.2.4.18	SSLv3 abilitata Per maggiori dettagli, consultare MOS SSLv3 Vulnerability Article.
X5-2 X5-2L	3.2.4.10 (x5-2) 3.2.4.12 (x5-2L)	SSLv3 disabilitata

- In Oracle ILOM le proprietà relative ai protocolli SSLv2 e alle cifrature deboli sono disabilitate per impostazione predefinita.

Per visualizzare o modificare le proprietà di sicurezza del server Web SSL o TLS in Oracle ILOM, fare riferimento alle istruzioni basate sul Web riportate di seguito.

1. **Nell'interfaccia Web di Oracle ILOM fare clic su ILOM Administration -> Management Access ->Web Server.**
2. **Nella pagina Web Server visualizzare o modificare le proprietà di sicurezza Web per i protocolli SSL, TLS o le cifrature deboli.**
3. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Proprietà di configurazione del server Web nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione del server Web nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*

▼ Impostare un intervallo di timeout per le sessioni Web inattive

Gli intervalli di timeout sessione Web di Oracle ILOM garantiscono la sicurezza degli utenti con accesso al Web che dimenticano di eseguire il logout. Gli intervalli di timeout sessione Web determinano i minuti che devono trascorrere prima del logout automatico di una sessione Web HTTP o HTTPS inattiva. Tale funzionalità consente di ridurre il rischio che un utente non autorizzato abbia accesso a un computer non presidiato con una sessione Web autenticata e attiva in Oracle ILOM.

Per visualizzare o modificare gli intervalli di timeout sessione Web impostati per le sessioni HTTP e HTTPS, vedere le istruzioni basate sul Web riportate di seguito.

Informazioni preliminari

- L'intervallo di timeout sessione Web predefinito impostato per le connessioni HTTP e HTTPS è di 15 minuti.

Nota - La riduzione del timeout della sessione potrebbe costringere l'utente a reimmettere il nome utente e la password più spesso, alla scadenza delle sessioni. Tuttavia, la riduzione del timeout abbrevia il periodo di tempo durante il quale sessioni Web autenticate, ma non presidiate, rimangono attive.

- Per modificare le proprietà del server Web è richiesto il ruolo Admin (a).

- Le proprietà dell'intervallo di timeout sessioni HTTP e HTTPS sono configurabili in Oracle ILOM solo per i processori SP server con release firmware 3.0.4 o versioni successive.

1. **Passare alla pagina Web Server.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Configuration -> System Management Access -> Web Server;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> Web Server.**

2. **Nella pagina Web Server eseguire le operazioni riportate di seguito.**

   a. **Passare alla proprietà di timeout sessione HTTP o HTTPS.**

   b. **Immettere un numero compreso tra 1 e 720 minuti per specificare i minuti che possono trascorrere prima del logout automatico di una sessione Web inattiva.**

   c. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Proprietà di configurazione del server Web nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione del server Web nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Impostazione del timeout della sessione nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Configurazione dell'interfaccia CLI per una maggiore sicurezza

Consultare gli argomenti riportati di seguito relativi a come configurare al meglio l'interfaccia della riga di comando (CLI) di Oracle ILOM per una maggiore sicurezza.

È possibile configurare le proprietà di gestione CLI in Oracle ILOM utilizzando usando l'interfaccia della riga di comando (CLI, Command-Line Interface) o l'interfaccia Web. Le procedure descritte in questa sezione forniscono istruzioni per la navigazione Web relative a tutte le release firmware di Oracle ILOM. Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà di configurazione, consultare la documentazione appropriata riportata nella sezione Informazioni correlate che segue ciascuna procedura.

▼ Gestione dello stato del server SSH e delle crittografie meno avanzate (3.2.5 e versioni successive)

A partire dalla release firmware 3.2.5, le proprietà SSH Server State e Weak Ciphers sono configurabili nell'interfaccia Web e CLI di Oracle ILOM. Per una maggiore sicurezza, la proprietà SSH Server State è abilitata e la proprietà Weak Ciphers disabilitata. Per modificare queste proprietà di accesso alla gestione del server SSH, vedere le istruzioni basate sul Web riportate di seguito.

1. **Nell'interfaccia Web di Oracle ILOM fare clic su ILOM Administration -> Management Access ->SSH Server.**
2. **Nella pagina SSH Server fare clic sul collegamento** *More Details...* **per ulteriori istruzioni.**
3. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Gestione dello stato del server SSH e delle crittografie meno avanzate nel manuale *Oracle ILOM Administrator's Guide for Configuration and Maintenance (Firmware 3.2.x)*

▼ Impostare un intervallo di timeout per le sessioni CLI inattive

L'interfaccia della riga di comando (CLI) di Oracle ILOM, accessibile mediante connessione a Oracle ILOM sul protocollo Secure Shell (SSH) o tramite una connessione seriale, supporta un intervallo di timeout sessione configurabile per la chiusura delle sessioni CLI inattive. Questa funzionalità, quando è configurata, riduce il rischio che un utente non autorizzato abbia accesso a un computer incustodito con una sessione CLI autenticata a Oracle ILOM.

Per una maggiore sicurezza, configurare un timeout di sessione CLI in qualsiasi ambiente in cui l'interfaccia CLI di Oracle ILOM sia utilizzata in una console condivisa. È consigliabile impostare l'intervallo di timeout sessione CLI al massimo su 15 minuti.

Per visualizzare o modificare la proprietà dell'intervallo di timeout impostato per le sessioni CLI di Oracle ILOM, vedere le istruzioni basate sul Web riportate di seguito.

Prima di cominciare

- Per modificare le proprietà CLI è richiesto il ruolo Admin (a).

- L'intervallo di timeout sessione CLI predefinito impostato per le connessioni SSH è disabilitato e impostato su 0 (zero) minuti.

Nota - Quando l'intervallo di timeout CLI è impostato su 0 (zero), Oracle ILOM non chiuderà le sessioni CLI inattive indipendentemente dal tempo di inattività di una sessione.

- La proprietà dell'intervallo di timeout sessione CLI è configurabile in Oracle ILOM solo per i processori SP server con release firmware 3.0.4 o versioni successive.

1. **Passare alla pagina CLI nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Configuration -> System Management Access -> CLI;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> CLI.**

2. **Nella pagina CLI impostare un intervallo di timeout sessione CLI eseguendo le operazioni riportate di seguito.**

   a. **Selezionare la casella di controllo Enable.**

   b. **Immettere un numero compreso tra 1 e 1440 minuti per specificare i minuti che possono trascorrere prima del logout automatico di una sessione della riga di comando inattiva.**

   c. **Fare clic su Save per applicare le modifiche.**

Informazioni correlate

- Proprietà di configurazione del timeout sessione CLI nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione del timeout sessione CLI nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Impostazione di un timeout sessione CLI nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

▼ Utilizzare chiavi lato server per cifrare le connessioni SSH

Oracle ILOM fornisce una capacità server SSH (Secure Shell) che consente ai client remoti di connettersi e gestire in modo sicuro Oracle ILOM mediante un'interfaccia della riga di comando. Il protocollo SSH utilizza chiavi lato server per cifrare il canale di gestione e

proteggere tutte le comunicazioni. I client SSH utilizzano inoltre tali chiavi per verificare l'autenticità del server SSH.

Oracle ILOM consente di generare un insieme di chiavi SSH univoche al primo boot di un sistema predefinito. Qualora siano necessarie nuove chiavi lato server, Oracle ILOM consente di generare manualmente ulteriori chiavi lato server SSH.

Per visualizzare o generare manualmente chiavi di cifratura lato server SSH, vedere le istruzioni basate sul Web riportate di seguito.

Informazioni preliminari

- Per modificare le proprietà del server SSH è richiesto il ruolo Admin (a).

1. **Passare alla pagina SSL Server nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:
   - **nell'interfaccia Web 3.0.x fare clic su System Management -> SSH Server;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> SSH Server.**
2. **Nella pagina SSH Server esaminare le informazioni sulle chiavi RSA e DSA generate oppure eseguire le operazioni riportate di seguito.**
   a. **Fare clic su Generate RSA Key per generare una nuova chiave.**
   b. **Fare clic su Generate DSA Key per generare una nuova chiave.**

Informazioni correlate

- Proprietà di configurazione del server SSH nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione del server SSH nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Generazione di una nuova chiave SSH nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- Generazione di una nuova chiave SSH nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

▼ Aggiungere chiavi SSH agli account utente per l'autenticazione CLI automatizzata

È possibile utilizzare coppie di chiavi SSH (DSA o RSA) generate e personalizzate per singoli account utente, in cui la chiave pubblica viene caricata su Oracle ILOM. Questa operazione

è molto vantaggiosa quando si utilizzano script eseguiti senza intervento manuale e che non includono password con testo in chiaro incorporate. Gli utenti possono scrivere script che eseguono automaticamente o regolarmente comandi del processore di servizio su una connessione SSH basata sulla rete da un sistema remoto.

Per caricare e aggiungere un account Oracle ILOM con una chiave SSH pubblica generata, vedere le istruzioni basate sul Web riportate di seguito.

Informazioni preliminari

- Generare le chiavi SSH private e pubbliche mediante uno strumento di connettività SSH quale ssh-keygen, quindi memorizzare i file delle chiavi SSH generati su un sistema SSH remoto.
- Per aggiungere chiavi pubbliche SSH ad altri account utente è richiesto il ruolo User Management (u).
- Per aggiungere una chiave pubblica SSH al proprio account utente è richiesto il ruolo Read Only (o).

1. **Passare alla pagina User Account nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su User Management -> User Accounts;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> User Management -> User Accounts.**

2. **Nella pagina User Account eseguire le operazioni riportate di seguito.**

   a. **Scorrere l'elenco fino a visualizzare la sezione SSH Keys, quindi fare clic su Add.**

   b. **Selezionare un account utente dall'elenco User.**

   c. **Selezionare un metodo di trasferimento dall'elenco, quindi specificare le proprietà del metodo di trasferimento necessarie per il caricamento della chiave SSH pubblica.**

3. **Fare clic su Load per caricare la chiave SSH pubblica e aggiungerla all'account utente selezionato.**

Informazioni correlate

- Autenticazione CLI mediante chiave SSH locale nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Autenticazione CLI mediante chiave SSH locale nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*

- Gestione degli account utente nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*
- Gestione degli account utente nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*

Configurare l'accesso alla gestione del protocollo SNMP per una maggiore sicurezza

SNMP è un protocollo standard utilizzato per monitorare o gestire un sistema. Oracle ILOM fornisce una soluzione SNMP per il monitoraggio e la gestione, ma è necessario eseguirne la configurazione prima dell'utilizzo. È importante tenere a mente le implicazioni relative alla sicurezza delle diverse opzioni SNMP configurabili dall'utente prima di eseguire la configurazione di questo servizio. Per ulteriori informazioni, consultare i seguenti argomenti:

- Usare la cifratura SNMPv3 e l'autenticazione utente [49]
- sezione chiamata «MIB Sun SNMP che supportano oggetti configurabili» [50]

▼ Usare la cifratura SNMPv3 e l'autenticazione utente

SNMPv1 e SNMPv2c non forniscono alcuna cifratura e utilizzano stringhe comunità come forma di autenticazione. Le stringhe community vengono inviate con testo in chiaro sulla rete e generalmente condivise da un gruppo di singoli individui, senza quindi essere limitate a un solo utente. Al contrario, SNMPv3 utilizza la cifratura per fornire un canale sicuro, nonché password e nomi utente singoli. Le password utente SNMPv3 sono localizzate in modo da poter essere archiviate in maniera sicura nelle stazioni di gestione.

SNMPv1, SNMPv2c e SNMPv3 sono tutti supportati da Oracle ILOM e possono essere attivati o disattivati separatamente. Inoltre, è possibile attivare o disattivare impostazioni per fornire un livello aggiuntivo di sicurezza. Questa opzione configurabile determina se il servizio SNMP consentirà l'impostazione delle proprietà MIB SNMP configurabili. Disattivando le impostazioni sarà possibile utilizzare il servizio SNMP solo per il monitoraggio.

Per impostazione predefinita, SNMPv1 e SNMPv2c sono disattivati. SNMPv3 è attivato per impostazione predefinita, ma è necessario creare uno o più utenti SNMP prima dell'utilizzo. Non sono disponibili utenti SNMPv3 preconfigurati.

Per configurare la gestione SNMP in Oracle ILOM, vedere le istruzioni basate sul Web riportate di seguito.

Informazioni preliminari

- Per una maggiore sicurezza SNMP, utilizzare SNMPv1 e SNMPv2c solo per il monitoraggio e non attivare le impostazioni quando i protocolli meno sicuri sono attivati.

- La proprietà SNMP sets deve essere abilitata solo per la gestione del protocollo SNMPv3. La proprietà SNMP Set è disabilitata per impostazione predefinita.
- Le proprietà sets di SNMPv3 richiedono la configurazione di account utente SNMPv3. Non vengono forniti account utente SNMPv3 preconfigurati.
- La proprietà di stato configurazione del servizio SNMP è abilitata per impostazione predefinita.
- Per modificare le proprietà SNMP sono richiesti i privilegi del ruolo Admin (a).
- Per aggiungere o modificare account utente SNMPv3 sono richiesti i privilegi User Management (u).

1. **Passare alla pagina SNMP nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su System Management Access -> SNMP;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> SNMP.**

2. **Nella pagina SNMP visualizzare o modificare le proprietà SNMP, quindi fare clic su Save per applicare le modifiche.**

   Per ulteriori istruzioni, consultare la documentazione riportata nella sezione Informazioni correlate di questa procedura. Per gli utenti di versioni firmware 3.2 o successive, fare clic sul collegamento `More details` nella pagina SNMP per ulteriori informazioni.

Informazioni correlate

- Configurazione delle impostazioni SNMP nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Configurazione delle impostazioni SNMP nel manuale *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)*
- Configurazione delle impostazioni SNMP nel manuale *Oracle ILOM 3.1 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference*
- Configurazione delle impostazioni SNMP nel manuale *Oracle ILOM 3.0 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference*

MIB Sun SNMP che supportano oggetti configurabili

Di seguito sono riportati i MIB Sun di Oracle che supportano oggetti configurabili e in cui sono applicabili le impostazioni.

- `SUN-HW-CTRL-MIB`: questo MIB viene utilizzato per configurare i criteri hardware, come ad esempio i criteri di gestione dell'alimentazione.

- `SUN-ILOM-CONTROL-MIB`: questo MIB è utilizzato per configurare le funzionalità di Oracle ILOM, quali creazione di utenti e configurazione di servizi.

Nota - È possibile impostare un oggetto MIB nei seguenti casi: 1) l'oggetto MIB supporta la modifica; 2) l'elemento `MAX-ACCESS` per l'oggetto MIB è impostato su `read-write`; e 3) l'utente che tenta di eseguire l'impostazione dispone dell'autorizzazione appropriata.

Configurare l'accesso alla gestione del protocollo IPMI per una maggiore sicurezza

Consultare gli argomenti riportati di seguito relativi a come configurare al meglio l'accesso alla gestione del protocollo IPMI di Oracle ILOM per una maggiore sicurezza.

- Usare IPMI v2.0 per autenticazione avanzata e cifratura dei pacchetti [51]
- sezione chiamata «Linee guida e pratiche consigliate sulla sicurezza di IPMI» [53]
- sezione chiamata «Supporto della suite di cifratura per l'autenticazione IPMI 2.0» [53]

▼ Usare IPMI v2.0 per autenticazione avanzata e cifratura dei pacchetti

Sebbene Oracle ILOM supporti IPMI v1.5 e v2.0 per la gestione remota, gli amministratori di sistema devono sempre utilizzare l'interfaccia -I lanplus IPMI v2.0 per gestire i server Oracle in modo sicuro. A partire da IPMI versione 2.0, l'interfaccia -I lanplus offre autenticazione avanzata e controlli di integrazione dati.

A partire dalla release firmware 3.2.4, Oracle ILOM offre una proprietà configurabile per l'abilitazione o la disabilitazione di sessioni IPMI v1.5. Per una maggiore sicurezza, la proprietà IPMI v1.5 è disabilitata per impostazione predefinita. Quando tale proprietà è disabilitata, tutte le connessioni delle sessioni IPMI v1.5 a Oracle ILOM sono bloccate.

Attenersi alla procedura riportata di seguito per visualizzare o modificare la proprietà di stato configurazione del servizio IPMI o la proprietà IPMI v1.5 configurabile, disponibile a partire dalla release firmware 3.2.4.

Informazioni preliminari

- Per modificare le proprietà del IPMI in Oracle ILOM è richiesto il ruolo Admin (a).
- La proprietà di stato configurazione del servizio IPMI è abilitata per impostazione predefinita. Prima dell'uso, gli account utente devono essere configurati in Oracle ILOM con privilegi basati sul ruolo appropriato (Administrator, Operator) per eseguire funzioni di gestione IPMI.

- Per i processori SP con firmware Oracle ILOM 3.2.4 o versioni successive sono supportate sessioni di gestione IPMI v2.0, mentre le sessioni IPMI v1.5 non lo sono per impostazione predefinita. La proprietà IPMI v1.5 è configurabile in Oracle ILOM.

Nota - Quando le sessioni IPMI v1.5 sono disabilitate in Oracle ILOM, gli utenti di IPMItool devono utilizzare l'opzione IPMI 2.0 -I lanplus.

- Per i processori SP con firmware Oracle ILOM 3.2.3 o versioni precedenti, le sessioni di gestione IPMI v2.0 e v1.5 sono supportate da Oracle ILOM. La proprietà IPMI v1.5 non è configurabile in Oracle ILOM.

Nota - Le sessioni IPMI v1.5 non supportano autenticazione avanzata e cifratura dei pacchetti. Per l'autenticazione avanzata e la cifratura dei pacchetti IPMI è necessario utilizzare IPMI v2.0.

---

1. **Passare alla pagina IPMI nell'interfaccia Web di Oracle ILOM.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Configuration -> System Management Access -> IPMI;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Management Access -> IPMI.**

2. **Nella pagina IPMI visualizzare o configurare le proprietà IPMI appropriate, quindi fare clic su Save per applicare le modifiche.**

   Per ulteriori istruzioni sulla configurazione IPMI, consultare la documentazione appropriata riportata nella sezione Informazioni correlate di seguito.

Informazioni correlate

- Gestione del server mediante IPMI nel manuale *Oracle ILOM Protocol Management Reference for SNMP and IPMI (Firmware 3.2.x)*
- Gestione del server mediante IPMI nel manuale *Oracle ILOM 3.1 SNMP, IPMI, CIM, and WS-Man Protocol Management Reference*
- Gestione del server mediante IPMI nel manuale *Oracle ILOM 3.0 SNMP, IPMI, CIM, WS-MAN Protocol Management Reference*
- sezione chiamata «Linee guida e pratiche consigliate sulla sicurezza di IPMI» [53]
- sezione chiamata «Supporto della suite di cifratura per l'autenticazione IPMI 2.0» [53]

Linee guida e pratiche consigliate sulla sicurezza di IPMI

Per garantire che le sessioni di gestione del sistema IPMI definite siano sicure e non vulnerabili ad attacchi cibernetici, gli amministratori di sistema devono attenersi a quanto riportato di seguito.

- Non devono stabilire mai sessioni di gestione remota IPMI utilizzando IPMI versione 1.5 (interfaccia IPMItool `-I lan`). Usare in modo esplicito IPMI versione 2.0 quando utilizzano utility della riga di comando quali IPMItool (interfaccia IPMItool `-I lanplus`).
- Devono modificare regolarmente tutte le password di Oracle ILOM e assicurarsi che il ciclo di vita degli account utente Oracle ILOM venga gestito in modo appropriato.

  Per ulteriori informazioni, vedere sezione chiamata «Protezione dell'accesso utente in Oracle ILOM» [25].
- Devono limitare l'accesso alla rete dall'esterno e Devono utilizzare il canale di gestione Ethernet dedicato per comunicare con Oracle ILOM.

  Per ulteriori informazioni, vedere sezione chiamata «Protezione della connessione di gestione fisica» [15].
- Collaborare con il responsabile della sicurezza IT per creare un insieme di procedure consigliate e criteri sulla gestione del server e la sicurezza di IPMI.

Supporto della suite di cifratura per l'autenticazione IPMI 2.0

I controlli di autenticazione, riservatezza e integrità in IPMI versione 2.0 sono supportati in tutte le suite di cifratura. Queste suite di cifratura utilizzano il protocollo di scambio chiavi autenticato RMCP+, descritto nelle specifiche di IPMI 2.0.

Oracle ILOM supporta i seguenti algoritmi di chiavi delle suite di cifratura per stabilire sessioni IPMI 2.0 sicure tra il client e il server.

- **Suite di cifratura 2**: utilizza entrambi gli algoritmi di autenticazione e di integrità.
- **Suite di cifratura 3**: utilizza tutti e tre gli algoritmi per l'autenticazione, la riservatezza e l'integrità.

Nota - Per garantire che tutto il traffico IPMI 2.0 sia cifrato, Oracle ILOM non implementa il supporto per la modalità operativa (senza cifratura) Tipo di cifratura 0 di IPMI 2.0.

Configurare l'accesso WS-Management per una maggiore sicurezza

A partire dalla release firmware 3.0.8 fino alla release firmware 3.1.2, Oracle ILOM fornisce un'interfaccia standard di servizi Web per il monitoraggio dell'integrità del server e la

distribuzione di informazioni di inventario mediante un protocollo definito Ws-Management (Ws-Man).

L'interfaccia Ws-Man di Oracle ILOM consente inoltre di eseguire il controllo peer dell'host e la reimpostazione del processore SP di Oracle ILOM. Ws-Man è un protocollo basato su SOAP (Simple Object Access Protocol) che sfrutta i protocolli HTTP(S). È possibile utilizzare l'interfaccia Ws-Man di Oracle ILOM con HTTP o HTTPS come trasporto. Se viene utilizzato HTTPS, la cifratura del canale avviene mediante certificato SSL. Per informazioni sui vantaggi relativi alla sicurezza derivanti dall'utilizzo di certificati SSL, nonché sulla differenza tra certificati autofirmati e certificati trusted, consultare sezione chiamata «Migliorare la sicurezza mediante un certificato e una chiave privata SSL trusted» [38].

Utilizzare questa interfaccia di servizi Web solo se vengono utilizzati i certificati SSL. Per una maggiore sicurezza, utilizzare HTTPS come sistema di trasporto. Per ulteriori informazioni sulla configurazione delle proprietà del server Web, vedere sezione chiamata «Configurare l'interfaccia Web per una maggiore sicurezza» [38].

Procedure di sicurezza consigliate successive alla distribuzione di Oracle ILOM

Gli argomenti riportati di seguito consentono di decidere quali siano le procedure di sicurezza migliori per Oracle ILOM da implementare dopo la distribuzione del server.

Informazioni correlate

- Procedure di sicurezza consigliate per la distribuzione di Oracle ILOM
- Elenchi di controllo delle procedure consigliate per la sicurezza di Oracle ILOM

Come mantenere una connessione di gestione sicura

Prendere in considerazione le informazioni riportate di seguito per mantenere una connessione di gestione sicura a Oracle ILOM.

Evitare l'accesso al dispositivo KCS host non autenticato

I server Oracle supportano una connessione standard a bassa velocità tra l'host e Oracle ILOM definita interfaccia KCS (Keyboard Controller Style). Questa interfaccia KCS supportata è completamente conforme alle specifiche dell'interfaccia IPMI (Intelligent Platform Management Interface) versione 2.0 e pertanto non può essere disabilitata.

L'accesso al dispositivo KCS, pur essendo un metodo pratico per configurare Oracle ILOM dall'host, può anche presentare dei rischi per la sicurezza in quanto qualsiasi utente del sistema operativo con accesso kernel o driver al dispositivo KCS fisico è in grado di modificare le impostazioni di Oracle ILOM senza autenticazione. Solitamente, solo gli utenti `root` o con diritti di amministratore possono accedere al dispositivo KCS. Tuttavia, è possibile configurare la maggior parte dei sistemi operativi in modo che consentano più ampio accesso al dispositivo KCS.

Ad esempio, un utente del sistema operativo con accesso KCS può eseguire le operazioni riportate di seguito.

- Aggiungere o creare utenti di Oracle ILOM.
- Modificare le password utente.
- Accedere all'interfaccia a riga di comando di Oracle ILOM come amministratore ILOM.
- Accedere a informazioni hardware e log.

Solitamente, il dispositivo è definito `/dev/kcs0` o `/dev/bmc` su Linux o Oracle Solaris e `ipmidrv.sys` o `imbdrv.sys` su Microsoft Windows. L'accesso a questo dispositivo, definito anche come driver Baseboard Management Controller (BMC) o driver IPMI, deve essere accuratamente controllato mediante il meccanismo di controllo degli accessi appropriato che è parte del sistema operativo host.

Per configurare le impostazioni di Oracle ILOM, provare a utilizzare l'interfaccia Oracle ILOM Interconnect come alternativa all'uso del dispositivo KCS IPMI host. Per ulteriori informazioni, vedere sezione chiamata «Accesso di interconnessione host autenticata preferenziale» [56].

Per ulteriori informazioni sulla modalità di controllo o protezione dell'accesso a dispositivi hardware come il dispositivo KCS, consultare la documentazione fornita con il sistema operativo host.

Accesso di interconnessione host autenticata preferenziale

Come alternativa più rapida all'interfaccia KCS, i client nel sistema operativo possono comunicare con Oracle ILOM tramite un'interconnessione ad alta velocità interna. L'interconnessione viene implementata mediante una connessione Ethernet tramite USB

interna, in cui è eseguito uno stack IP. In Oracle ILOM è disponibile un indirizzo IP interno non routable che può essere utilizzato per la connessione da parte di un client nell'host.

A differenza dell'interfaccia KCS, basata su un accesso protetto a un dispositivo hardware, l'interconnessione LAN è disponibile per tutti i sistemi operativi per impostazione predefinita. Per questo motivo, la connessione a Oracle ILOM mediante l'interconnessione LAN richiede un'autenticazione, come se la connessione provenisse dalla rete e fosse diretta a una porta di gestione Oracle ILOM.

Inoltre, tutti i servizi o i protocolli visibili sulla rete di gestione sono disponibili mediante l'interconnessione LAN sull'host. È possibile utilizzare un browser Web sull'host per accedere all'interfaccia Web di Oracle ILOM o utilizzare un client SSH (Secure Shell) per eseguire la connessione all'interfaccia della riga di comando di Oracle ILOM. In ogni caso, è necessario fornire un nome utente e una password validi per utilizzare l'interconnessione LAN.

L'interconnessione LAN viene disattivata per impostazione predefinita. Quando è disattivata, non è visibile alcun dispositivo Ethernet sul sistema operativo host e il canale non esiste. Oracle Hardware Management Pack consente di eseguire il provisioning e configurare l'interconnessione LAN.

Per informazioni sulla gestione di Oracle ILOM tramite una connessione di interconnessione host dedicata e sicura, consultare uno degli argomenti riportati di seguito.

- Per le release firmware 3.2 o versioni successive, vedere l'argomento relativo alla connessione di gestione SP di interconnessione dedicata nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (Firmware 3.2x)*
- Per le release firmware 3.1.x, vedere l'argomento relativo alla connessione di gestione SP di interconnessione dedicata nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Per le release firmware da 3.0.12 a 3.0.16, vedere l'argomento relativo alla configurazione di un'interconnessione host locale nella guida *Oracle ILOM 3.0 Web Procedures Guide*.

Usare la cifratura IPMI 2.0 per proteggere il canale

Intelligent Platform Management Interface (IPMI) versione 2.0 supporta un protocollo di rete cifrato definito Remote Management and Control Protocol+ (RMCP+). In questo protocollo viene utilizzato un sistema di risposte di verifica basato su chiavi simmetriche per la cifratura del canale. In questo modo viene impedito che i dati sensibili vengano inviati alla rete senza cifratura ed è necessaria una password utente per cifrare e decifrare il traffico. Per garantire che tutto il traffico di IPMI 2.0 sia cifrato, Oracle ILOM non implementa alcun supporto per la modalità operativa (senza cifratura) Tipo di cifratura 0 di IPMI 2.0.

Nel caso di IPMItool, utilizzare il flag `-I lanplus` per indicare che è necessario stabilire una sessione RMCP+ cifrata.

Per ulteriori informazioni, consultare la documentazione di `ipmitool`.

Nota - A partire dalla release firmware 3.2.4, Oracle ILOM offre una proprietà configurabile per IPMI v1.5. Per impostazione predefinita, la proprietà IPMI 1.5 è disabilitata. Per ulteriori informazioni, vedere Usare IPMI v2.0 per autenticazione avanzata e cifratura dei pacchetti [51].

Utilizzare protocolli sicuri per la gestione remota

Oracle ILOM supporta diversi protocolli di gestione remota. In alcuni casi, sono supportate versioni cifrate e non cifrate dello stesso protocollo. Per motivi di sicurezza utilizzare sempre, se possibile, il protocollo più sicuro disponibile. Per un elenco di protocolli cifrati e non cifrati, vedere la tabella riportata di seguito.

TABELLA 9 Protocolli sicuri supportati

Categoria	Sicuro/Cifrato	Non cifrato
Accesso browser Web	HTTPS	HTTP
Accesso riga di comando	SSH	Nessun protocollo supportato
Accesso IPMI	IPMI v2.0	IPMI v1.5
Accesso protocollo	SNMPv3	SNMPv1/v2c

Stabilire una connessione di gestione di rete trusted sicura

Tutti i server Oracle di Oracle ILOM dispongono di una porta di gestione dedicata utilizzata per la connessione a Oracle ILOM tramite una rete. L'utilizzo della porta di gestione dedicata fornisce una rete privata e sicura per la gestione. Alcuni sistemi supportano inoltre la gestione della banda laterale che consente di accedere sia all'host che a Oracle ILOM tramite le porte di dati server standard. L'utilizzo della gestione della banda laterale semplifica la gestione dei cavi e la configurazione di rete evitando di dover predisporre due connessioni di rete separate. Tuttavia, in questo caso il traffico di Oracle ILOM potrebbe essere inviato tramite una rete non trusted se la porta di gestione dedicata o della banda laterale non è connessa a una rete trusted.

Per garantire la massima affidabilità e sicurezza dell'ambiente per Oracle ILOM, la porta di gestione di rete dedicata o la porta di gestione della banda laterale sul server deve essere sempre connessa a una rete interna trusted o a una rete di gestione/privata sicura dedicata.

Stabilire una connessione di gestione seriale locale sicura

È possibile connettere in locale un server di terminale o un terminale dump a Oracle ILOM mediante la porta di gestione seriale fisica presente sul server. Per mantenere una connessione

di gestione locale sicura a Oracle ILOM, evitare di connettere un dispositivo terminale alla porta di gestione seriale locale se tale dispositivo è connesso anche a una rete interna o privata.

Utilizzo sicuro del sistema KVMS remoto

Oracle ILOM consente di reindirizzare in maniera remota tastiera, video e mouse del server host verso un client remoto, nonché di attivare l'archiviazione remota. Tali funzionalità sono definite KVMS remoto. Il sistema KVMS remoto consente di visualizzare la console grafica del sistema operativo host sul server, eseguendo applicazioni Java definite Remote Console (Console remota), Remote Console Plus (Console remota plus) e Storage Redirection CLI (Interfaccia a riga di comando di reindirizzamento memorizzazione) di Oracle ILOM su un computer client.

Per assicurarsi che le sessioni KVMS remote e le sessioni seriali basate su testo vengano avviate in modo sicuro da Oracle ILOM, consultare gli argomenti riportati di seguito.

- sezione chiamata «Comunicazione KVMS remota e cifratura» [59]
- sezione chiamata «Protezione dall'accesso condiviso del servizio KVMS remoto» [60]
- sezione chiamata «Proteggersi dall'accesso condiviso della console seriale host» [60]

Comunicazione KVMS remota e cifratura

Le applicazioni Oracle ILOM Remote System Console, Remote System Console Plus e CLI Storage Redirection utilizzano una serie di protocolli di rete per comunicare in remoto con Oracle ILOM. Mediante queste applicazioni Java è possibile controllare tastiera e mouse host e attivare un dispositivo di storage locale (ad esempio un'unità CD o DVD) sul server remoto.

Nella seguente tabella viene descritta, più dettagliatamente, la modalità di trasmissione delle informazioni del sistema KVMS remoto su una rete.

TABELLA 10 Funzionalità e cifratura KVMS

Funzionalità KVMS	Cifrato o non cifrato	Descrizione
Reindirizzamento mouse	Cifrato	Le coordinate del mouse sono inviate in maniera sicura tramite rete a Oracle ILOM.
Reindirizzamento tastiera	Cifrato	Qualsiasi carattere digitato sul computer client viene trasmesso a Oracle ILOM mediante protocollo cifrato.
Reindirizzamento video	Cifrato	I dati del video vengono trasmessi mediante un protocollo cifrato tra il client Java e Oracle ILOM.
Reindirizzamento archiviazione	Non cifrato	I dati letti e scritti in un dispositivo di memorizzazione vengono trasmessi sulla rete a Oracle ILOM senza cifratura.

Per un elenco delle porte di rete abilitate dal servizio KVMS remoto, vedere Tabella 4, «Servizi e porte abilitati per impostazione predefinita».

Protezione dall'accesso condiviso del servizio KVMS remoto

Una console video del servizio KVMS remoto esegue il reindirizzamento del contenuto visualizzato se si stesse guardando un monitor fisicamente connesso al server. Benché sia possibile la presenza di più client remoti con sessioni KVMS in Oracle ILOM, in ciascuna sessione verrà visualizzato lo stesso video, in quanto è disponibile solitamente una sola uscita video per un singolo server.

Allo stesso modo, tutto ciò che viene digitato sullo schermo di una sessione del sistema KVMS remoto sarà visualizzato dall'altro utente KVMS connesso allo stesso computer. Ancora più importante, se un utente esegue il login al sistema operativo host all'interno dell'applicazione Remote Console (Console remota), Remote Console Plus (Console remota Plus) e Storage Redirection CLI (Interfaccia a riga di comando di reindirizzamento memorizzazione) di Oracle ILOM come utente con privilegi, tutti gli altri utenti KVMS avranno la possibilità di condividere tale sessione autenticata. Per questo motivo, è fondamentale sapere che la funzionalità KVMS remoto consente connessioni condivise.

Per proteggersi da sessioni del sistema operativo autenticate che rimangono inattive dopo aver terminato una sessione di reindirizzamento del servizio KVMS remoto, è necessario eseguire le operazioni riportate di seguito.

- Configurare Oracle ILOM in modo che blocchi automaticamente il sistema operativo host al termine di una sessione di reindirizzamento del servizio KVMS remoto.

  Per istruzioni, vedere Bloccare l'accesso host all'uscita da una sessione KVMS [34].
- Impostare un intervallo di timeout nel sistema operativo host per chiudere automaticamente le sessioni utente autenticate non presidiate.

  Per istruzioni, consultare la documentazione utente relativa al sistema operativo host in uso.

Per gli utenti di Oracle ILOM Remote System Console Plus che devono limitare il numero di sessioni KVMS visualizzabili avviate da Oracle ILOM, vedere Limitazione delle sessioni KVMS visualizzabili per Remote System Console Plus (3.2.4 o versioni successive) [35].

Proteggersi dall'accesso condiviso della console seriale host

La console host per la maggior parte dei sistemi operativi è disponibile anche mediante una console seriale basata su testo. Questa console è disponibile eseguendo il comando

`start /HOST/console` nella riga di comando dell'interfaccia a riga di comando di Oracle ILOM. Come accade per la console grafica, è disponibile una sola singola console seriale per tutti gli utenti Oracle ILOM. Questa risorsa è pertanto considerata condivisa. Se un utente esegue il login al sistema operativo host dalla console seriale e chiude il reindirizzamento della console senza disconnettersi, un secondo utente della console seriale potrebbe accedere alla sessione del sistema operativo precedentemente autenticata.

Oracle ILOM invia un segnale DTR (Data Transfer Request) al sistema operativo host quando viene terminata una sessione di reindirizzamento console. Molti sistemi operativi eseguono automaticamente la disconnessione di un utente quando viene ricevuto questo segnale. Tuttavia, non tutti i sistemi operativi supportano questa funzionalità:

- Oracle Linux 5 dispone di un supporto per il segnale DTR eseguito per impostazione predefinita.
- Oracle Linux 6 dispone di un supporto DTR, ma è necessario attivarlo manualmente.
- Oracle Solaris non dispone di alcun supporto per il segnale DTR. Per ridurre i rischi relativi alla sicurezza, gli utenti possono configurare il timeout di una sessione nel sistema operativo host.

Per le linee guida su come proteggersi da sessioni del sistema operativo autenticate che rimangono inattive dopo aver terminato una sessione di reindirizzamento seriale host, tenere presente quanto riportato di seguito.

- Stabilire se la funzionalità di segnale DTR nel sistema operativo host è supportata e, qualora lo sia, verificare che sia abilitata per impostazione predefinita.

  Per informazioni sul segnale DTR, consultare la documentazione utente relativa al sistema operativo host in uso.
- Configurare un intervallo di timeout sessione nel sistema operativo host.

  Per informazioni su come impostare un intervallo di timeout sessione nel sistema operativo host, consultare la documentazione utente per il sistema operativo host in uso.
- Implementare un criterio di sicurezza per accertarsi che gli utenti non lascino mai incustodita una console host seriale remota. Gli utenti devono sempre eseguire il logout di tutte le sessioni della console host quando le sessioni non sono in uso.

Considerazioni successive alla distribuzione per la protezione dell'accesso utente

Per garantire il mantenimento dell'accesso utente sicuro, consultare gli argomenti riportati di seguito.

- sezione chiamata «Applicazione della gestione delle password» [62]
- sezione chiamata «Presenza di sicurezza fisica per la reimpostazione della password predefinita dell'account `root`» [63]

- sezione chiamata «Monitorare gli eventi di controllo per individuare accessi non autorizzati» [64]

Applicazione della gestione delle password

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

In genere, gli utenti modificano le proprie password, tuttavia, gli amministratori di sistema con privilegi di gestione utente possono modificare le password associate ad altri account utente.

Per modificare la password associata a un account utente di Oracle ILOM, vedere le istruzioni basate sul Web riportate di seguito.

Nota - Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà di configurazione di gestione utente, consultare la documentazione riportata nella sezione Informazioni correlate presente nella procedura riportata di seguito.

▼ Modificare la password dell'account utente locale

Informazioni preliminari

- Esaminare le sezione chiamata «Linee guida di sicurezza per la gestione di account utente e password» [27].
- Per modificare password o privilegi associati ad altri account utente è richiesto il ruolo User Management (u).
- Il ruolo Operator (o) consente agli utenti di modificare la password per il proprio account.

1. **Passare alla pagina User Account nell'interfaccia Web di Oracle ILOM.**
   Ad esempio:
   - **nell'interfaccia Web 3.0.x fare clic su User Management -> User Accounts;**
   - **nell'interfaccia Web 3.1 e versioni successive fare clic su User Management -> User Accounts.**
2. **Nella pagina User Account fare clic su Edit per l'account che si desidera modificare.**
   Viene visualizzata la finestra di dialogo Edit: User Name.
3. **Nella finestra di dialogo Edit: User Name eseguire le operazioni riportate di seguito.**

- **Immettere una password univoca nella casella di testo New Password, quindi reimmettere la stessa password nella casella di testo Confirm New Password.**

- **Fare clic su Save per applicare la modifica.**

Informazioni correlate

- Impostazione di limitazioni per il criterio della password per tutti gli utenti locali (3.2.5 e versioni successive) [30]
- Configurazione di un account utente locale nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Configurazione di un account utente locale nel manuale *Configuration and Maintenance Guide* di Oracle ILOM 3.1
- Modifica di un account utente nel manuale *Oracle ILOM 3.0 Daily Management - CLI Procedures Guide*
- Modifica di un account utente nel manuale *Oracle ILOM 3.0 Daily Management - Web Procedures Guide*

Presenza di sicurezza fisica per la reimpostazione della password predefinita dell'account `root`

Nel caso in cui venga smarrita la password utente `root` per Oracle ILOM, è possibile reimpostarla. Per reimpostare la password `root`, eseguire la connessione a Oracle ILOM mediante la porta seriale. Benché in molti casi la connessione alla porta seriale di Oracle ILOM richieda accesso fisico al sistema, è possibile collegare la console seriale a un server di terminale. Questo server consente un accesso di rete alla porta seriale fisica.

Per impedire la reimpostazione della password `root` mediante la rete quando il server di terminale è in uso, è disponibile per la maggior parte dei server una funzionalità di verifica della presenza fisica. In questo caso è necessario premere un pulsante sul server come prova dell'esecuzione di un accesso fisico allo stesso. Per una maggiore sicurezza, verificare che la funzionalità di verifica della presenza sia attivata quando la porta seriale di Oracle ILOM è collegata a un server di terminale.

Per visualizzare o modificare la funzionalità di controllo della presenza fisica, vedere le istruzioni basate sul Web riportate di seguito.

Nota - Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sulle proprietà dell'account `root`, consultare la documentazione riportata nella sezione Informazioni correlate presente nella procedura riportata di seguito.

▼ Impostare il controllo della presenza fisica

Informazioni preliminari

- In Oracle ILOM la modalità di controllo della presenza fisica è abilitata per impostazione predefinita.
- Per usare la modalità di controllo della presenza fisica in Oracle ILOM è richiesto il firmware 3.1 o versione successiva.

1. **Nell'interfaccia Web di Oracle ILOM fare clic su ILOM Administration -> Identification.**
2. **Nella pagina Identification passare alla proprietà Physical Presence Check, quindi eseguire una delle operazioni riportate di seguito.**

   - **Selezionare la casella di controllo Physical Presence per abilitarla. Quando è abilitata, è necessario premere il pulsante Locator sul sistema fisico per poter recuperare la password Oracle ILOM predefinita.**
     - Oppure -
   - **Deselezionare la casella di controllo Physical Presence per disabilitarla. Quando è disabilitata, è possibile reimpostare la password root predefinita dell'amministratore di Oracle ILOM senza premere il pulsante Locator sul sistema fisico.**

3. **Fare clic su Save per applicare la modifica.**

Informazioni correlate

- Proprietà di configurazione per l'identificazione del dispositivo nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Proprietà di configurazione per l'identificazione del dispositivo nella *guida relativa a configurazione e gestione di Oracle ILOM 3.1*
- Recupero della password per l'account `root` nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (firmware 3.2.x)*
- Recupero della password per l'account `root` nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM 3.1*

Monitorare gli eventi di controllo per individuare accessi non autorizzati

Il log di controllo di Oracle ILOM consente di registrare tutte le modifiche a login e configurazione. Ciascuna voce del log di controllo indica utente e data/ora associati all'evento.

Gli eventi di controllo possono rivelarsi un utile strumento per rilevare le modifiche e per determinare se sono state applicate modifiche non autorizzate ed eseguiti accessi non autorizzati a Oracle ILOM.

Per visualizzare gli eventi nel log di controllo di Oracle ILOM, vedere le istruzioni basate sul Web riportate di seguito.

Nota - Per istruzioni sull'interfaccia CLI o per ulteriori informazioni sul log di controllo, consultare la documentazione riportata nella sezione Informazioni correlate della procedura riportata di seguito.

▼ Visualizzare il log di controllo

Informazioni preliminari

- Il log di controllo è diventato disponibile in Oracle ILOM a partire dalla release firmware 3.1. Prima della release firmware release 3.1, gli eventi di controllo venivano acquisiti nel log degli eventi di Oracle ILOM.
- Per cancellare le voci contenute nel log di controllo sono richiesti i privilegi del ruolo Admin (a).

1. **Nell'interfaccia Web fare clic su ILOM Administration -> Logs -> Audit.**
2. **Nella pagina Audit log usare i controlli per filtrare le voci del log o per cancellare gli eventi presenti.**

   Per gli utenti di versioni firmware 3.2 o successive, fare clic sul collegamento `More details` nella pagina Audit per ulteriori informazioni.

Informazioni correlate

- Gestione delle voci del log di Oracle ILOM nel manuale *Oracle ILOM User's Guide for System Monitoring and Diagnostics (Firmware 3.2.x)*
- Gestione delle voci del log di Oracle ILOM nel manuale *Oracle ILOM 3.1 User Guide*

Azioni successive alla distribuzione per la modifica della modalità FIPS

A partire dalla release firmware 3.2.4, Oracle ILOM offre una proprietà configurabile per la conformità al Livello 1 degli standard FIPS. Per impostazione predefinita, questa proprietà è disabilitata. Quando si modifica lo stato operativo della conformità agli standard FIPS in Oracle ILOM, vengono ripristinate le impostazioni predefinite di tutte le proprietà delle configurazioni definite dall'utente. Per evitare la perdita delle impostazioni di configurazione definite

dall'utente in Oracle ILOM, è necessario modificare la conformità agli standard FIPS prima di configurare qualsiasi altra impostazione di Oracle ILOM. Nel caso in cui sia necessario modificare la conformità agli standard FIPS dopo la distribuzione della configurazione di Oracle ILOM, vedere le istruzioni riportate di seguito per evitare la perdita delle impostazioni definite dall'utente.

Nota - Oracle utilizza algoritmi crittografici in conformità agli standard di sicurezza FIPS 140-2 per proteggere dati sensibili o preziosi del sistema.

▼ Modifica della modalità FIPS dopo la distribuzione

Attenersi a questa procedura se è necessario modificare lo stato operativo della modalità FIPS dopo aver eseguito un aggiornamento firmware o aver specificato le proprietà di configurazione definite dall'utente in Oracle ILOM.

Nota - La modalità di conformità agli standard FIPS in Oracle ILOM è rappresentata dalle proprietà di stato configurazione e di stato operativo. La proprietà di stato configurazione e la proprietà di stato operativo rappresentano rispettivamente la modalità configurata e la modalità operativa in Oracle ILOM. Quando viene modificata la proprietà di stato configurazione di FIPS, la modifica non ha effetto sulla modalità operativa (proprietà di stato operativo di FIPS) fino al successivo reboot di Oracle ILOM.

Informazioni preliminari

- La proprietà configurabile per la conformità al Livello 1 degli standard FIPS è disponibile in Oracle ILOM a partire dal firmware 3.2.4 o versioni successive. Prima della release firmware 3.2.4, Oracle ILOM non offriva una proprietà configurabile per la conformità al Livello 1 degli standard FIPS.
- Quando FIPS è abilitato (in modalità configurata e operativa), alcune funzionalità in Oracle ILOM non sono supportate. Per un elenco di funzionalità non supportate quando FIPS è abilitato, vedere sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19].
- Per eseguire questa procedura è richiesto il ruolo Admin (a).

1. **Nell'interfaccia Web di Oracle ILOM eseguire il backup della configurazione di Oracle ILOM.**
   Ad esempio:

   a. **Fare clic su ILOM Administration -> Configuration Management -> Backup/ Restore.**

   b. **Nella pagina Backup/Restore fare clic sul collegamento More details... per ulteriori istruzioni.**

Nota - Per semplificare la riconnessione a Oracle ILOM dopo l'aggiornamento firmware, è necessario abilitare le opzioni di aggiornamento firmware per conservare la configurazione.

Nota - Se si esegue il passo 2 prima del passo 1, sarà necessario modificare il file di configurazione XML di cui è stato eseguito il backup e rimuovere l'impostazione FIPS. In caso contrario, si avrà una configurazione incoerente tra il file XML di Oracle ILOM di cui è stato eseguito il backup e lo stato configurazione della modalità FIPS operativa in esecuzione sul server. Questa configurazione non è consentita.

2. **Se è necessario eseguire un aggiornamento firmware, attenersi alla procedura riportata di seguito.**

   a. **Fare clic su ILOM Administration -> Maintenance -> Firmware Update.**

   b. **Nella pagina Firmware Update fare clic sul collegamento More details... per ulteriori istruzioni.**

3. **Modificare la modalità di conformità agli standard FIPS in Oracle ILOM come riportato di seguito.**

   a. **Fare clic su ILOM Administration -> Management Access -> FIPS.**

   b. **Nella pagina FIPS fare clic sul collegamento `More details` per istruzioni su come eseguire le operazioni riportate di seguito.**

      - **Modificare la configurazione dello stato configurazione di FIPS.**
      - **Aggiornare lo stato operativo di FIPS sul sistema reimpostando il processore SP.**

4. **Ripristinare la configurazione di Oracle ILOM di cui è stato eseguito il backup come riportato di seguito.**

   a. **Fare clic su ILOM Administration -> Configuration Management -> Backup/ Restore.**

   b. **Nella pagina Backup/Restore fare clic sul collegamento `More details` per ulteriori istruzioni.**

Informazioni correlate

- sezione chiamata «Come scegliere se configurare la modalità FIPS al momento della distribuzione» [16]

- sezione chiamata «Funzionalità non supportate quando la modalità FIPS è abilitata» [19]
- Configurare le proprietà della modalità FIPS nella *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM (Firmware 3.2.x)*

Aggiornamento alle versioni software e firmware più recenti

Mantenere sempre aggiornate le versioni del software e del firmware sul server.

- Verificare regolarmente la presenza di aggiornamenti pubblicati su My Oracle Support.
- Utilizzare le correzioni dei bug e i miglioramenti installando sempre la versione del software o del firmware più recente disponibile per il server in uso.
- Installare tutte le patch di sicurezza necessarie per tutto il software installato.

Per aggiornare il firmware di Oracle ILOM sul server, vedere le istruzioni riportate di seguito.

▼ Aggiornare il firmware di Oracle ILOM

Informazioni preliminari

- Per aggiornare il firmware di Oracle ILOM è richiesto il ruolo Admin (a) in Oracle ILOM.
- Comunicare a tutti gli utenti di Oracle ILOM l'aggiornamento firmware pianificato e chiedere loro di chiudere tutte le sessioni client fino al completamento di tale aggiornamento.
- Il completamento del processo di aggiornamento firmware richiede diversi minuti durante i quali non devono essere eseguiti altri task di Oracle ILOM.

1. **Scaricare l'aggiornamento software più recente disponibile per il server in uso dal sito Web My Oracle Support (MOS).**

   Se necessario, consultare la documentazione fornita con il server per istruzioni relative a come ottenere gli aggiornamenti software da MOS.

   Nota - La versione più recente del firmware di Oracle ILOM disponibile per il server è inclusa nella patch software più recente pubblicata su MOS per il server in uso.

2. **Inserire l'immagine firmware su un'unità locale o di rete condivisa.**

3. **Passare alla pagina Firmware Update nell'interfaccia Web.**

   Ad esempio:

   - **nell'interfaccia Web 3.0.x fare clic su Maintenance -> Firmware;**

- **nell'interfaccia Web 3.1 e versioni successive fare clic su ILOM Administration -> Maintenance -> Firmware Upgrade;**

4. **nella pagina Firmware Update fare clic sulla modalità Enter Firmware Upgrade, quindi seguire i prompt visualizzati.**

   Per gli utenti di versioni firmware 3.2 o successive di Oracle ILOM, fare clic sul collegamento `More details` nella pagina Firmware Upgrade.