Guida per la sicurezza di Oracle Hardware Management Pack

N. di parte: E39914–01
Marzo 2013

130322@25097

Indice

Panoramica

In questa sezione viene fornita una panoramica del prodotto Oracle Hardware Management Pack (HMP), con informazioni sulla Guida per la sicurezza e la spiegazione dei principi generali della sicurezza dell'applicazione.

Vengono trattati gli argomenti seguenti:

Panoramica sul prodotto

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

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

I plugin SNMP di Hardware Management Agent vengono eseguiti sul sistema operativo host dei server Oracle. I plugin SNMP utilizzano le Oracle Hardware Storage Access Library per comunicare con il processore di servizio. Le informazioni sullo stato corrente del server vengono recuperate automaticamente da Hardware Management Agent.

È possibile utilizzare gli strumenti CLI di Oracle Server per configurare i server Oracle. Gli strumenti CLI sono compatibili con Oracle Solaris, Oracle Linux, Oracle VM, altre varianti di Linux e sistemi operativi Windows. Nella seguente tabella vengono descritti i task che possono essere eseguiti tramite gli strumenti CLI.

Task di gestione del sistema dal sistema operativo host	Strumento CLI
Configurare le impostazioni del BIOS, l'ordine di avvio dei dispositivi e alcune impostazioni del processore di servizio.	`ubiosconfig` `biosconfig`
Aggiornare Oracle ILOM e il BIOS.	`fwupdate`
Eseguire query, aggiornare e convalidare le versioni del firmware sui dispositivi di storage SAS supportati, sui controller di storage SAS incorporati, sugli espansori di storage SAS e sulle unità di storage.	
Ripristinare, impostare e visualizzare le impostazioni di configurazione di Oracle ILOM nonché visualizzare e impostare le proprietà di Oracle ILOM associate alla gestione della rete, alla configurazione del clock e alla gestione utente.	`ilomconfig`
Visualizzare o creare volumi RAID sulle unità di storage collegate a controller RAID, inclusi gli array di storage.	`raidconfig`
Monitorare l'integrità del sistema.	`hwmgmt`

Informazioni su questa Guida per la sicurezza

Nel presente documento vengono fornite istruzioni di sicurezza generali per Oracle Hardware Management Pack. Questa Guida è stata concepita per assistere l'utente nella definizione di un ambiente sicuro durante l'utilizzo del software con altri prodotti hardware Oracle, quali gli switch e le schede di interfaccia di rete.

Vengono trattati gli argomenti seguenti:

Principi di sicurezza di base

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

- Accesso

  Eseguire controlli fisici e del software per proteggere l'hardware o i dati da eventuali intrusioni.

  - Per l'hardware, i limiti di accesso sono in genere limiti all'accesso fisico.
  - Per il software, i limiti di accesso comprendono in genere sia mezzi fisici che mezzi virtuali.
  - Il firmware può essere modificato solo tramite il processo di aggiornamento Oracle.

- Autenticazione

  Impostare tutte le funzionalità di autenticazione, come ad esempio un sistema di password, nei sistemi operativi della piattaforma per verificare l'identità degli utenti.

  L'autenticazione fornisce vari livelli di sicurezza tramite misure quali badge e password. Ad esempio, assicurarsi che il personale utilizzi in modo corretto i badge dipendente per accedere a una sala computer.

- Autorizzazione

  L'autorizzazione consente al personale della società di utilizzare l'hardware e il software solo se correttamente formato e qualificato per tale scopo.

  Ad esempio, impostare un sistema di autorizzazioni di lettura, scrittura ed esecuzione per controllare l'accesso utente a comandi, spazio su disco, dispositivi e applicazioni.

- Accounting

  Il personale di IT del cliente può utilizzare le funzioni software e hardware Oracle per monitorare le attività di login e gestire i magazzini hardware.

  - Utilizzare i log di sistema per monitorare i login utente. In particolare, utilizzare i log di sistema per monitorare gli account di amministratore di sistema e di servizio poiché tali account dispongono di privilegi per l'accesso a comandi potenti.
  - Rimuovere periodicamente i file di log quando superano una determinata dimensione nel rispetto dei criteri in uso nella società del cliente. In genere i log rimangono attivi per lunghi periodi di tempo, pertanto è importante garantirne la gestione.
  - Utilizzare i numeri di serie dei componenti per tenere traccia degli asset del sistema a scopo di inventario. I numeri parte Oracle sono registrati elettronicamente su tutte le schede, i moduli e le schede madri.

Riepilogo della sicurezza di Oracle Hardware Management Pack

Di seguito sono riportati degli elementi di sicurezza importanti da tenere presenti durante la configurazione di tutti gli strumenti di gestione del sistema.

- *I prodotti di gestione del sistema possono essere utilizzati per ottenere un ambiente root di boot.*

  Un ambiente root di boot consente di accedere a Oracle ILOM, Oracle System Assistant e ai dischi rigidi.

- *I prodotti di gestione del sistema includono potenti strumenti la cui esecuzione richiede privilegi di amministratore o root.*

  Questo livello di accesso consente di modificare la configurazione hardware e di eliminare i dati.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Operazioni precedenti all'installazione di Oracle Hardware Management Pack

Durante l'installazione e l'impostazione iniziali, utilizzare le funzioni di sicurezza software Oracle per controllare l'hardware e tenere traccia degli asset di sistema.

Vengono trattati gli argomenti seguenti:

Componenti di Oracle Hardware Management Pack

Oracle Hardware Management Pack contiene una raccolta di strumenti della riga di comando di gestione hardware per la configurazione di RAID, BIOS e Oracle ILOM e per l'aggiornamento del firmware. Contiene anche un plugin SNMP per il monitoraggio. Oracle Hardware Management Pack contiene anche un daemon o servizio che comunica con Oracle ILOM su un canale interno per condividere le informazioni di inventario e integrità relative al server.

Questi strumenti e plugin sono installati sul sistema operativo host e pertanto è possibile eseguire i task di gestione del sistema direttamente dall'host. Oracle Hardware Management Pack fornisce funzionalità utili per la gestione di un server Oracle, completamente opzionali.

Per ulteriori informazioni sulle funzionalità di Oracle Hardware Management Pack per determinare l'opportunità di usarlo e installarlo, vedere il manuale Sun Server Hardware Management Pack User's Guide.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)
- Per informazioni generali su Oracle ILOM, vedere: `http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

Impostazioni di sicurezza del plugin SNMP basate su agente

Oracle Hardware Management Pack contiene un modulo del plugin SNMP che estende l'agente SNMP nativo nel sistema operativo host per fornire funzionalità aggiuntive di Oracle MIB. È particolarmente importante tenere presente che Oracle Hardware Management Pack non contiene un agente SNMP. Per Linux, viene aggiunto un modulo all'agente net-snmp, che deve essere stato installato in precedenza. Per Solaris, viene aggiunto un modulo all'agente di gestione Solaris. Per Windows, il plugin estende il servizio SNMP nativo.

Allo stesso modo, tutte le impostazioni di sicurezza relative a SNMP per il plugin SNMP di Oracle Hardware Management Pack vengono determinate dalle impostazioni dell'agente o servizio SNMP nativo e non dal plugin. Per istruzioni su come configurare SNMP in modo sicuro, vedere la documentazione relativa a net-snmp o al servizio SNMP Windows.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Scelta di una versione del protocollo SNMP dell'agente SNMP

SNMP è un protocollo standard utilizzato per monitorare o gestire un sistema. SNMPv1/v2c non fornisce alcuna cifratura e utilizza stringhe comunità come forma di autenticazione. Le stringhe comunità vengono inviate in testo non cifrato sulla rete e sono solitamente condivise da un gruppo di utenti e non limitate a uno solo. Viceversa, SNMPv3 utilizza la cifratura per fornire un canale sicuro e dispone di singoli nomi utente e password. Le password utente SNMPv3 sono localizzate, in modo da poter essere archiviate in maniera sicura nelle stazioni di gestione.

Oracle consiglia di utilizzare SNMPv3 se supportato dall'agente SNMP nativo. Per istruzioni su come configurareSNMPv3, vedere la documentazione relativa a net-snmp o al servizio SNMP Windows.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Installazione di Oracle Hardware Management Pack

Vengono trattati gli argomenti seguenti:

Esecuzione del programma di installazione di Oracle Hardware Management Pack

Oracle Hardware Management Pack consiste di un set di pacchetti di installazione nativi che possono essere installati utilizzando gli strumenti di installazione nativi per un sistema operativo, ad esempio RPM. Inoltre, è possibile utilizzare un programma di installazione basato su procedura guidata per l'operazione. Oltre ad aggiungere i pacchetti nativi, il programma di installazione consente anche di configurare Oracle Hardware Management Pack per l'uso.

Poiché il programma di installazione di Oracle Hardware Management Pack deve installare pacchetti nativi, è necessario eseguirlo come root o amministratore.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Scelta di abilitare l'interconnessione LAN

Come alternativa più rapida all'interfaccia KCS, i client del sistema operativo possono comunicare con Oracle ILOM tramite un'interconnessione ad alta velocità interna. Questa interconnessione viene implementata mediante una connessione Ethernet tramite USB interna, in cui è in esecuzione uno stack IP. In Oracle ILOM e nell'host sono disponibili indirizzi IP interni non routable per la comunicazione su questo canale.

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. Tutti i servizi o i protocolli visibili sulla rete di gestione sono disponibili mediante l'interconnessione LAN all'host. Ad esempio, è possibile utilizzare un browser Web sull'host per

accedere all'interfaccia Web di Oracle ILOM o utilizzare un client shell sicuro 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.

Nel programma di installazione di Oracle Hardware Management Pack è possibile abilitare l'interconnessione LAN. Oracle consiglia di abilitare l'interconnessione LAN solo se l'istruzione di rete supporta RFC 3927 e la possibilità di avere indirizzi IPv4 link-local. Inoltre, è necessario prestare attenzione per assicurarsi che il sistema operativo non agisca da bridge o router. Questo consente di assicurarsi che il traffico di gestione tra l'host e Oracle ILOM rimanga privato.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Scelta di salvare le credenziali in un file

Gli strumenti ilomconfig e fwupdate, che fanno parte di Oracle Hardware Management Pack, possono connettersi a Oracle ILOM tramite l'interconnessione LAN ad alta velocità. L'utilizzo dell'interconnessione LAN al posto dell'interfaccia KCS (più lenta) può migliorare notevolmente le prestazioni di operazioni chiave, ad esempio gli aggiornamenti del firmware di Oracle ILOM.

Poiché l'interconnessione LAN richiede l'autenticazione, è necessario eseguire tale operazione in Oracle ILOM per ogni richiamo di questi strumenti. Pertanto è possibile inserire le credenziali nella cache di un file in modo che possano essere utilizzate automaticamente dagli strumenti. Questo impedisce di dover incorporare password non cifrate in script che utilizzano gli strumenti di Oracle Hardware Management Pack.

Lo strumento ilomconfig può essere utilizzato per memorizzare il nome utente e la password in un file cifrato di sola lettura root. Se questo file viene rilevato quando si utilizza ilomconfig o fwupdate per accedere a Oracle ILOM, vengono utilizzate le credenziali inserite nella cache. In alternativa, è possibile specificare il nome utente e la password sulla riga di comando per ogni richiamo dello strumento.

L'algoritmo di cifratura usato è univoco per ogni sistema. Tuttavia, se viene trovata la chiave, è possibile decifrare il file e visualizzare il nome utente e la password. A tale scopo, Oracle consiglia di creare una password univoca su ciascun Oracle ILOM in modo che non sia possibile utilizzare una password compromessa su altri sistemi Oracle ILOM.

Per istruzioni su come salvare le credenziali in un file, vedere il manuale Sun Server Hardware Management Pack User's Guide.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)

Operazioni successive all'installazione di Oracle Hardware Management Pack

Vengono trattati gli argomenti seguenti:

Disinstallazione di Oracle Hardware Management Pack

I pacchetti di Oracle Hardware Management Pack possono essere disinstallati utilizzando gli strumenti del pacchetto nativo, ad esempio RPM, oppure il programma di disinstallazione basato su procedura guidata fornito con Oracle Hardware Management Pack. Quando viene utilizzato il metodo del pacchetto nativo per rimuovere i pacchetti, il file cifrato, in cui sono memorizzati il nome utente e la password inseriti nella cache per l'utilizzo nella LAN interconnessa, non verrà eliminato. L'eliminazione deve essere eseguita manualmente.

Il programma di disinstallazione basato su procedura guidata rimuove il file delle credenziali. Pertanto, Oracle consiglia di utilizzare il programma di installazione basato su procedura guidata per disinstallare Oracle Hardware Management Pack.

- Libreria della documentazione di Oracle Hardware Management Pack (`http://www.oracle.com/pls/topic/lookup?ctx=ohmp`)