Guida per la sicurezza di Oracle MiniCluster S7-2

N. di parte: E78273-02
Ottobre 2016

N. di parte: E78273-02

Copyright © 2016, Oracle e/o relative consociate. Tutti i diritti riservati.

Il software e la relativa documentazione vengono distribuiti sulla base di specifiche condizioni di licenza che prevedono restrizioni relative all'uso e alla divulgazione e sono inoltre protetti dalle leggi vigenti sulla proprietà intellettuale. Ad eccezione di quanto espressamente consentito dal contratto di licenza o dalle disposizioni di legge, nessuna parte può essere utilizzata, copiata, riprodotta, tradotta, diffusa, modificata, concessa in licenza, trasmessa, distribuita, presentata, eseguita, pubblicata o visualizzata in alcuna forma o con alcun mezzo. La decodificazione, il disassemblaggio o la decompilazione del software sono vietati, salvo che per garantire l'interoperabilità nei casi espressamente previsti dalla legge.

Le informazioni contenute nella presente documentazione potranno essere soggette a modifiche senza preavviso. Non si garantisce che la presente documentazione sia priva di errori. Qualora l'utente riscontrasse dei problemi, è pregato di segnalarli per iscritto a Oracle.

Qualora il software o la relativa documentazione vengano forniti al Governo degli Stati Uniti o a chiunque li abbia in licenza per conto del Governo degli Stati Uniti, sarà applicabile la clausola riportata di seguito.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Il presente software o hardware è stato sviluppato per un uso generico in varie applicazioni di gestione delle informazioni. Non è stato sviluppato né concepito per l'uso in campi intrinsecamente pericolosi, incluse le applicazioni che implicano un rischio di lesioni personali. Qualora il software o l'hardware venga utilizzato per impieghi pericolosi, è responsabilità dell'utente adottare tutte le necessarie misure di emergenza, backup e di altro tipo per garantirne la massima sicurezza di utilizzo. Oracle Corporation e le sue consociate declinano ogni responsabilità per eventuali danni causati dall'uso del software o dell'hardware per impieghi pericolosi.

Oracle e Java sono marchi registrati di Oracle e/o delle relative consociate. Altri nomi possono essere marchi dei rispettivi proprietari.

Intel e Intel Xeon sono marchi o marchi registrati di Intel Corporation. Tutti i marchi SPARC sono utilizzati in base alla relativa licenza e sono marchi o marchi registrati di SPARC International, Inc. AMD, Opteron, il logo AMD e il logo AMD Opteron sono marchi o marchi registrati di Advanced Micro Devices. UNIX è un marchio registrato di The Open Group.

Il software o l'hardware e la documentazione possono includere informazioni su contenuti, prodotti e servizi di terze parti o collegamenti agli stessi. Oracle Corporation e le sue consociate declinano ogni responsabilità ed escludono espressamente qualsiasi tipo di garanzia relativa a contenuti, prodotti e servizi di terze parti se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle. Oracle Corporation e le sue consociate non potranno quindi essere ritenute responsabili per qualsiasi perdita, costo o danno causato dall'accesso a contenuti, prodotti o servizi di terze parti o dall'utilizzo degli stessi se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle.

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 sulla pianificazione, sulla configurazione e sulla gestione di un ambiente sicuro per i sistemi Oracle MiniCluster S7-2.
- **Destinatari**: tecnici, amministratori di sistema e provider di servizi autorizzati.
- **Competenze richieste**: esperienza avanzata nell'amministrazione di UNIX e dei database.

Libreria della documentazione del prodotto

La documentazione e le risorse per questo prodotto e per i prodotti correlati sono disponibili all'indirizzo http://www.oracle.com/goto/minicluster-s7-2/docs

Feedback

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

Informazioni sui principi di sicurezza

Nella presente Guida vengono fornite informazioni sulla pianificazione, sulla configurazione e sulla gestione di un ambiente sicuro per i sistemi Oracle MiniCluster S7-2.

In questa sezione vengono trattati gli argomenti seguenti:

Task di sicurezza obbligatori minimi

Il sistema ingegnerizzato MiniCluster è configurato per impostazione predefinita come sistema ad alta sicurezza ed è dotato delle funzioni e delle caratteristiche di sicurezza riportate di seguito.

- Il sistema è preconfigurato con controlli di sicurezza completamente automatici per tutte le virtual machine (VM).
- La cifratura è abilitata per impostazione predefinita e garantisce la sicurezza dei dati archiviati e in transito.
- Le VM vengono configurate in modo automatico con un sistema operativo protetto ed essenziale dotato di firewall basati su host.
- Il controllo dell'accesso richiede l'accesso basato su ruolo con privilegi minimi.
- Tutte le VM usano lo storage ZFS cifrato.
- Sono disponibili una funzione di gestione delle chiavi centralizzata, che utilizza PKCS#11, e il supporto per FIPS.
- Il sistema include un criterio di controllo completo con log di controllo centralizzati.
- Il sistema e tutte le VM sono configurati con un profilo di sicurezza PCI-DSS, equivalente a CIS o DISA-STIG. Nota: l'ultimo profilo è attualmente in fase di revisione. Utilizzare il profilo DISA-STIG solo per uso sperimentale in ambienti non di produzione.

- È disponibile un dashboard di conformità di facile visualizzazione che supporta benchmark di conformità di facile esecuzione.

Al termine dell'installazione di MiniCluster, l'amministratore della sicurezza deve eseguire i due task obbligatori riportati di seguito.

- Modifica della password root di ILOM Vedere Modifica delle password `root` Oracle ILOM predefinite [27]

È importante inoltre rivedere le informazioni di sicurezza fornite nella presente Guida per comprendere e verificare le funzioni di sicurezza di MiniCluster.

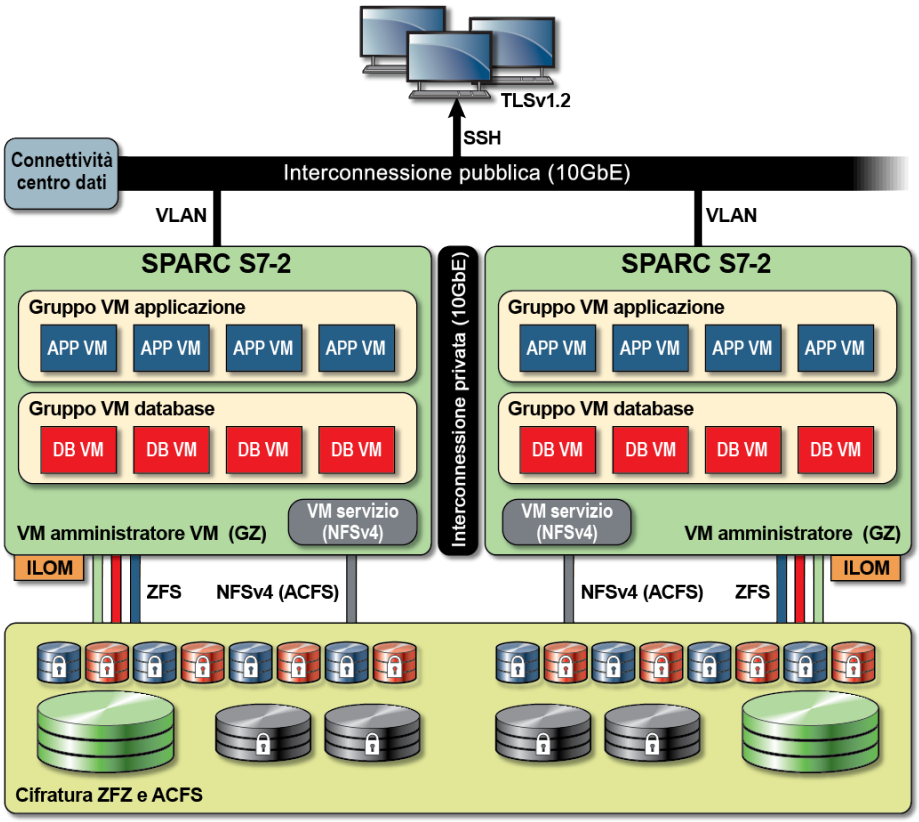
Principi di sicurezza di base

MiniCluster è una piattaforma di infrastruttura cloud sicura per il consolidamento delle applicazioni e dei database, in grado di offrire servizi cloud di calcolo dedicati basati sulla funzionalità IaaS (Infrastructure as a Service). Creato come sistema ingegnerizzato multifunzione, MiniCluster riunisce in sé la potenza di elaborazione del processore SPARC S7 Oracle, le efficienti capacità di virtualizzazione di SPARC Solaris e le prestazioni di database ottimizzate del database Oracle con storage dedicato integrato. Viene inoltre utilizzata una rete 10 GbE che consente ai client di accedere ai servizi in esecuzione in MiniCluster. Infine, un'altra rete 10 GbE fornisce il canale di intercomunicazione tra l'ambiente delle virtual machine nei server SPARC S7 e le applicazioni hosted.

Il processore SPARC S7 si caratterizza per una funzionalità di crittografia assistita da hardware sempre attiva che consente alle entità configurate in MiniCluster di proteggere le proprie informazioni mediante un sistema dalle elevate prestazioni in grado di proteggere i dati archiviati, utilizzati e in transito. Il processore è dotato anche della funzione Silicon Secured Memory, che individua e previene gli attacchi che hanno come obiettivo il danneggiamento dei dati in memoria e lo scraping della memoria, salvaguardando in questo modo l'integrità dei dati delle applicazioni.

Per impostazione predefinita, MiniCluster viene distribuito già configurato con oltre 250 controlli di sicurezza integrati che riducono la superficie di attacco del sistema mediante la disabilitazione dei servizi, delle porte e dei protocolli non assolutamente necessari e la configurazione dei servizi esposti per l'accettazione delle sole connessioni sicure.

Il sistema supporta numerose opzioni di configurazione e distribuzione. Questa figura illustra una distribuzione standard che consolida i carichi di lavoro del database e delle applicazioni Oracle.



Virtual machine sicure

La sicurezza all'interno dei nodi di calcolo MiniCluster si basa su vari livelli. Il primo livello è costituito dalla funzione Boot verificato dei nodi di calcolo, un sistema operativo protetto ed essenziale eseguito in ambienti virtual machine isolati per prevenire l'accesso ai carichi di lavoro e ai dati da parte di utenti e sistemi non autorizzati. La tecnologia Oracle Solaris Zones viene utilizzata sotto forma di virtual machine in MiniCluster per adattare ambienti di calcolo isolati e offrire un ambiente sicuro ed efficace per le varie applicazioni in esecuzione nello stesso sistema operativo, proteggendole dalle attività non intenzionali o non autorizzate svolte nelle altre virtual machine. Pur essendo eseguita nello stesso kernel delle altre zone, ogni zona Solaris è caratterizzata da identità, risorse, spazio di nomi e isolamento dei processi propri. Rispetto alle virtual machine tradizionali in esecuzione negli Hypervisor Type 1, le zone Solaris forniscono funzioni di virtualizzazione integrata basata su forte isolamento e controlli flessibili delle risorse mediante unità CPU e footprint di memoria di dimensioni inferiori. Ogni virtual machine è configurata con un profilo di sicurezza che definisce il set completo di controlli e di criteri di sicurezza applicati in modo automatico durante il processo di installazione. L'uso dei

pool e dei data set ZFS consente di suddividere e isolare ulteriormente lo storage in unità con maggiore granularità per le virtual machine, che possono disporre di criteri di sicurezza propri.

Controllo dell'accesso

Per proteggere i dati di applicazione, i carichi di lavoro e l'infrastruttura di esecuzione di base, in MiniCluster sono disponibili funzioni di controllo dell'accesso complete e al contempo flessibili, sia per gli utenti finali che per gli amministratori. MiniCluster si basa su Oracle Solaris per numerosi metodi di controllo dell'accesso per gli utenti e per le applicazioni che accedono ai servizi del sistema. Sebbene le tradizionali coppie nome utente-password siano ancora utilizzate su larga scala, è possibile integrare con facilità metodi di autenticazione più potenti grazie all'architettura PAM (Moduli di autenticazione collegabili, Pluggable Authentication Modules) Oracle Solaris, che consente di usare l'autenticazione LDAP, Kerberos e con chiave pubblica. L'ambiente computazionale di MiniCluster è basato sulla funzione RBAC (Controllo dell'accesso basato su ruoli, Role Based Access Control), che consente alle organizzazioni di delegare l'accesso amministrativo e degli utenti in base alle esigenze. Eliminando la nozione di utente privilegiato con pieni poteri, la funzione RBAC di Oracle Solaris consente di separare i compiti e supporta la nozione di ruoli amministrativi, autorizzazioni, privilegi con filtro e profili utilizzati collettivamente per assegnare i diritti agli utenti e agli amministratori. La funzione RBAC è integrata ad altri servizi di base Oracle Solaris, comprese la funzione SMF (Funzione di gestione dei servizi, Service Management Facility) e le virtual machine, per garantire un'architettura coerente a supporto di tutte le esigenze di controllo dell'accesso a livello di sistema. MiniCluster utilizza la funzione RBAC di Oracle Solaris come elemento di base dell'architettura di controllo dell'accesso, consentendo in questo modo alle organizzazioni di gestire, controllare e sottoporre a controllo l'accesso di gestione del sistema operativo e della virtualizzazione da un'autorità centralizzata. Tutte le operazioni critiche vengono effettuate sulla base del principio di separazione dei compiti supportato da un workflow di autorizzazioni per più persone. Il sistema esige che ogni operazione inerente alla sicurezza venga approvata da due o più persone. Insieme, queste funzioni possono essere utilizzate per offrire un elevato livello di garanzia per l'identità degli utenti e per la gestione delle operazioni business critiche.

Tutti i dispositivi del sistema MiniCluster sono in grado di limitare l'accesso in rete ai servizi mediante metodi architetturali (ad esempio l'isolamento della rete) o l'utilizzo di filtri per i pacchetti e/o delle liste di controllo dell'accesso al fine di limitare la comunicazione verso, da e tra i dispositivi fisici e virtuali, nonché verso i servizi esposti dal sistema. MiniCluster implementa impostazioni di sicurezza predefinite in base alle quali nessun servizio di rete, ad eccezione di Secure Shell (SSH), è abilitato per l'accettazione del traffico di rete in entrata. Gli altri servizi di rete abilitati ascoltano internamente le richieste nell'ambito del sistema operativo (virtual machine o zona) di Oracle Solaris. Ciò garantisce che tutti i servizi di rete siano disabilitati per impostazione predefinita oppure siano impostati per l'ascolto delle sole comunicazioni di sistema locali. Le organizzazioni possono naturalmente personalizzare questa configurazione in base a esigenze specifiche. MiniCluster è preconfigurato con il filtraggio dei pacchetti dei layer di rete e di trasporto (con conservazione dello stato) che utilizza la funzione

IP Filter di Oracle Solaris. IP Filter offre numerose funzioni di rete basate su host, tra le quali il filtraggio dei pacchetti con conservazione dello stato, la conversione degli indirizzi di rete e la conversione degli indirizzi di porta.

Protezione dei dati

Il processore SPARC S7 di MiniCluster facilita la cifratura assistita da hardware, ad alte prestazioni per la protezione dei dati negli ambienti IT che rivolgono particolare attenzione alla sicurezza. Il processore SPARC S7 utilizza inoltre la tecnologia Silicon Secured Memory che garantisce la prevenzione da attacchi non autorizzati a livello di applicazione, come scraping della memoria, danneggiamento della memoria in background, dati in eccesso nel buffer e attacchi correlati.

Il processore SPARC supporta l'accelerazione crittografica assistita da hardware per più di 16 algoritmi di cifratura standard del settore. Questi algoritmi supportano le esigenze di cifratura più moderne, quali la cifratura a chiave pubblica, la cifratura a chiave simmetrica, la generazione di numeri casuali, nonché il calcolo e la verifica delle firme digitali e dei digest di messaggio. Inoltre, a livello di sistema operativo, l'accelerazione hardware crittografica è abilitata per impostazione predefinita per la maggior parte dei servizi principali, inclusi Secure Shell, IPSec/IKE e data set ZFS cifrati.

Oracle Database e Oracle Fusion Middleware identificano automaticamente il sistema operativo Oracle Solaris e il processore SPARC utilizzato da MiniCluster. Ciò consente a Oracle Database e a Oracle Middleware di utilizzare automaticamente le funzionalità di accelerazione crittografica della piattaforma per le operazioni di cifratura di TLS, WS-Security e delle tablespace. Consente inoltre a questi prodotti di utilizzare la funzione Silicon Secured Memory per garantire la protezione della memoria e assicurare l'integrità dei dati dell'applicazione senza che l'utente finale debba eseguire la configurazione. MiniCluster supporta l'uso di IPsec (IP Security) e IKE (Internet Key Exchange) per proteggere la confidenzialità e l'integrità delle comunicazioni specifiche delle VM e tra VM diverse che utilizzano le reti pubbliche e private.

In MiniCluster la cifratura dei data set ZFS si basa su un keystore PKCS#11 Oracle Solaris centralizzato per proteggere in modo sicuro le chiavi di wrapping. Utilizzando il keystore PKCS#11 Oracle Solaris si attiva in modo automatico l'accelerazione crittografica SPARC assistita da hardware per tutte le operazioni di cifratura. Ciò consente a Oracle di migliorare in modo significativo le prestazioni relative alle operazioni di cifratura e decifrazione associate ai data set ZFS, alla TDE (Cifratura dati trasparente, Transparent Data Encryption) del database Oracle, alla cifratura delle tablespace, ai backup dei database cifrati (mediante Oracle Recovery Manager [Oracle RMAN]), alle esportazioni dei database cifrati (mediante la funzione Data Pump del database Oracle) e ai redo log (mediante Oracle Active Data Guard). Le virtual machine di database possono utilizzare un approccio con wallet condiviso sfruttando il keystore PKCS#11 Oracle Solaris oppure creare una directory nello storage di condivisione ACFS in modo che il wallet possa essere condiviso tra i database residenti nelle virtual machine. L'uso di un keystore condiviso e centralizzato in ogni nodo di calcolo consente al sistema di gestire,

conservare e ruotare meglio le chiavi della cifratura Oracle TDE nelle architetture di database in cluster basate su Oracle Grid Infrastructure, poiché le chiavi vengono sincronizzate in ogni nodo del cluster. In MiniCluster è inoltre disponibile una funzione di eliminazione sicura delle virtual machine e dei data set ZFS associati che prevede la gestione dei criteri e delle chiavi di cifratura a livello di data set ZFS (file system/ZVOL) in modo da garantire l'eliminazione tramite la distruzione delle chiavi.

Controllo e conformità

MiniCluster si basa sull'uso del sottosistema di controllo di Oracle Solaris per raccogliere, memorizzare ed elaborare le informazioni degli eventi di controllo. Ogni virtual machine (zona non globale) genera record di controllo che vengono memorizzati localmente in ogni area di memorizzazione di controllo di MiniCluster (zona globale). Questo approccio impedisce alle singole virtual machine di modificare i criteri di controllo, le configurazioni o i dati registrati poiché il provider di servizi cloud è responsabile di queste attività.

La funzionalità di controllo di Oracle Solaris monitora tutte le azioni amministrative, i richiami dei comandi e anche le singole chiamate del sistema a livello di kernel nelle virtual machine. Questa funzionalità è altamente configurabile e offre criteri di controllo globali, per zona e anche per utente. Quando è configurata per l'uso delle virtual machine, i record di controllo relativi a ogni virtual machine possono essere memorizzati nella zona globale per proteggerli dalla manomissione. La zona globale sfrutta inoltre la funzionalità di controllo nativa di Oracle Solaris per registrare azioni ed eventi associati agli eventi di virtualizzazione e all'amministrazione di MiniCluster.

In MiniCluster sono disponibili strumenti in grado di valutare la conformità dell'ambiente runtime Oracle Solaris residente nelle virtual machine e di creare report specifici. Le utility di conformità sono basate sull'implementazione del protocollo SCAP (Protocollo di automazione del contenuto di sicurezza, Security Content Automation Protocol). MiniCluster supporta i due profili di benchmark di conformità alla sicurezza riportati di seguito.

- **Profilo di sicurezza predefinito**: profilo equivalente a CIS (basato sul benchmark Center of Internet Security), più allineato ai requisiti di conformità di sicurezza previsti da una regolamentazione, ad esempio HIPAA, FISMA, SOX e così via.
- **Profilo PCI-DSS**: lo standard PCI-DSS (Payment Card Industry Data Security Standard).
- **Profilo DISA-STIG**: acronimo di Defense Information System Agency-Security Technical Implementation Guidance Standard. Questo profilo si basa sul profilo di sicurezza predefinito e presenta 75 controlli di sicurezza aggiuntivi, la crittografia FIPS-140-2 e il supporto per l'impostazione di una password S. *Nota*: questo profilo è attualmente in fase di revisione. Utilizzare questo profilo solo per uso sperimentale in ambienti non di produzione.

L'amministratore di MiniCluster può eseguire il benchmark di conformità su richiesta e verificare l'ambiente per determinarne la conformità e le anomalie. Gli strumenti di profilo mappano i controlli di sicurezza ai requisiti di conformità definiti dagli standard di settore. I

report di conformità associati contribuiscono a ridurre in modo significativo i tempi e i costi di controllo.

A partire da MiniCluster v.1.1.18, il sistema include le funzioni di controllo riportate di seguito.

- **Ruolo Auditor**: quando si specifica questo ruolo per un utente MCMU, l'utente può accedere alla pagina di revisione dell'auditor nell'interfaccia BUI MCMU. L'utente non può visualizzare né eseguire nessun altro task amministrativo di MiniCluster.
- **Pagina di revisione dell'auditor**: è una pagina speciale dell'interfaccia BUI MCMU che può essere visualizzata solo dagli utenti con il ruolo Auditor. Questa pagina consente di accedere allo stato dei pool di controllo e offre la possibilità di generare record di controllo per tutte le attività utente per zona. Vedere Generazione dei report di controllo [41].

Informazioni sulla configurazione della sicurezza

Gli argomenti riportati di seguito descrivono i controlli di sicurezza di MiniCluster.

Profili di sicurezza integrati

Per inizializzare MiniCluster si utilizza l'interfaccia BUI o CLI della utility MCMU. Durante l'inizializzazione, la utility MCMU richiede alla persona che esegue l'installazione di scegliere uno di questi profili di sicurezza:

- **Profilo di sicurezza predefinito**: soddisfa i requisiti comparabili ed equivalenti ai benchmark preimpostati in base alle valutazioni CIS (Center for Internet Security) e STIG (Security Technical Implementation Guidelines).
- **Profilo PCI-DSS**: è conforme allo standard PCI DSS (Payment Card Industry Data Security Standard) definito dal Payment Card Industry Security Standards Council.
- **Profilo DISA-STIG**: acronimo di Defense Information System Agency-Security Technical Implementation Guidance Standard. Questo profilo si basa sul profilo di sicurezza predefinito e presenta 75 controlli di sicurezza aggiuntivi, la crittografia FIPS-140-2 e il supporto per l'impostazione di una password eeprom. *Nota*: questo profilo è attualmente in fase di revisione. Utilizzare questo profilo solo per uso sperimentale in ambienti non di produzione.

A seconda del criterio selezionato, la utility MCMU configura la zona globale e le zone non globali con oltre 250 controlli di sicurezza.

Al termine dell'inizializzazione, durante la creazione delle virtual machine, la utility MCMU richiede la selezione di uno dei profili di sicurezza per ogni virtual machine. A seconda delle esigenze di sicurezza del proprio ambiente, è possibile disporre di una combinazione di profili di sicurezza nelle virtual machine.

▼ Verifica del profilo di sicurezza VM (CLI)

Usare questa procedura per verificare o identificare il profilo di sicurezza configurato per le zone e le virtual machine.

Nota - Per eseguirla, è necessario accedere al sistema con un account utente che disponga del ruolo `root`.

Nota - Per identificare il profilo di sicurezza assegnato alla zona globale, visualizzare Impostazioni del sistema -> Riepilogo input utente nell'interfaccia BUI MCMU. Il profilo di sicurezza è visualizzato nella parte inferiore della pagina.

---

1. **Eseguire il login alla zona globale come utente `mcinstall`.**

   Per istruzioni su come accedere al sistema, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

2. **Assumere il ruolo `root`.**

   Esempio:

   ```
   # su root
   ```

3. **Determinare il nome del file di log per la VM interessata.**

   In questo esempio esiste un file di log per ogni VM:

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **Visualizzare i file di log di verifica.**

   Osservare le ultime righe del file di log. Se è visualizzata la dicitura `(PCI-DSS)`, il profilo di sicurezza della VM è PCI-DSS. Se invece non viene indicato alcun profilo, il profilo di sicurezza della VM è equivalente a CIS.

   - Esempio delle ultime 22 righe di una VM con profilo PCI-DSS:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured

     (PCI-DSS) Checking audit configuration (user audit flags):
     Passed/Configured
     ```

```
(PCI-DSS) Checking audit configuration (non-attributable audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (audit_binfile plugin):
Passed/Configured

(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- Esempio delle ultime 22 righe di una VM con profilo equivalente a CIS:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

Protezione dei dati

Gli argomenti riportati di seguito descrivono le tecnologie di protezione dei dati di MiniCluster.

Protezione dei dati con la cifratura dei data set ZFS

In MiniCluster la protezione dei dati archiviati viene configurata in modo automatico mediante la cifratura dei data set ZFS. La cifratura è configurata come riportato di seguito.

- Tutti i data set ZFS, compresi i file system radice e di swap, vengono cifrati nelle virtual machine.
- Tutti i data set ZFS, ad eccezione dei file system radice e di swap, vengono cifrati nella zona globale.

Per verificare la configurazione della cifratura, è possibile visualizzare le chiavi di cifratura. Vedere Visualizzazione delle chiavi di cifratura dei data set ZFS (BUI) [21].

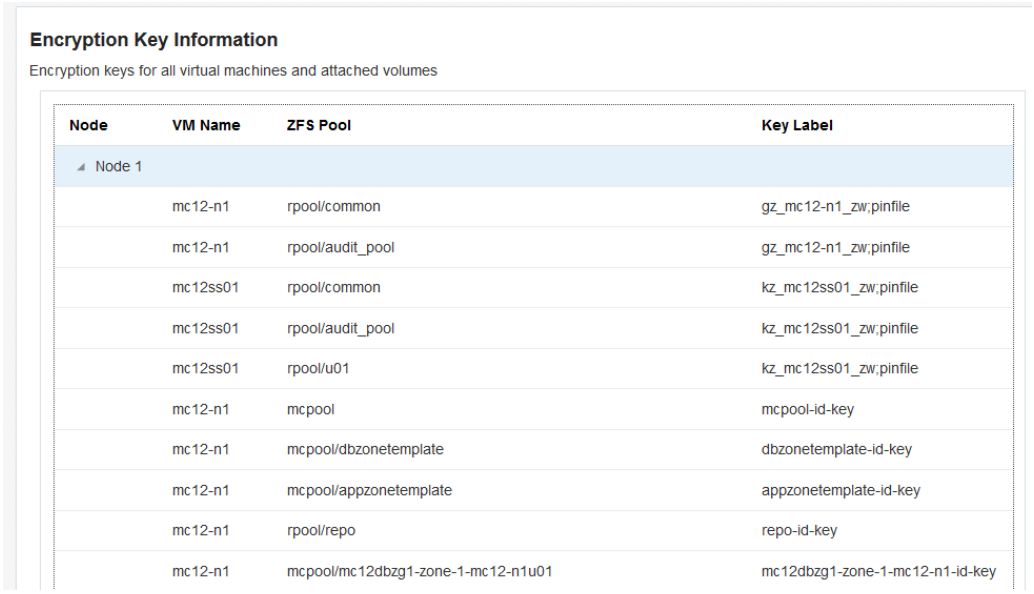
▼ Visualizzazione delle chiavi di cifratura dei data set ZFS (BUI)

Usare questa procedura per visualizzare i dettagli delle chiavi di cifratura.

1. **Accedere all'interfaccia BUI MCMU.**

   Per informazioni dettagliate sulle modalità di accesso all'interfaccia BUI MCMU, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

2. **Selezionare Impostazioni del sistema -> Sicurezza nel pannello di navigazione.**
   Fare clic su un nodo per visualizzare i dettagli.



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
◢ Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

Servizio Secure Shell

MiniCluster richiede l'uso de protocollo di rete SSH per garantire che l'utente possa eseguire il login, in tutta sicurezza, ai nodi di calcolo (zone globali) e alle istanze delle virtual machine (zone non globali) MiniCluster.

Quando un utente esegue il login per la prima volta utilizzando il protocollo SSH, il sistema genera in modo automatico una nuova coppia di chiavi SSH.

▼ Modifica delle chiavi SSH (BUI)

Usare questa procedura per modificare le chiavi SSH per una zona o una VM mediante una delle configurazioni seguenti.

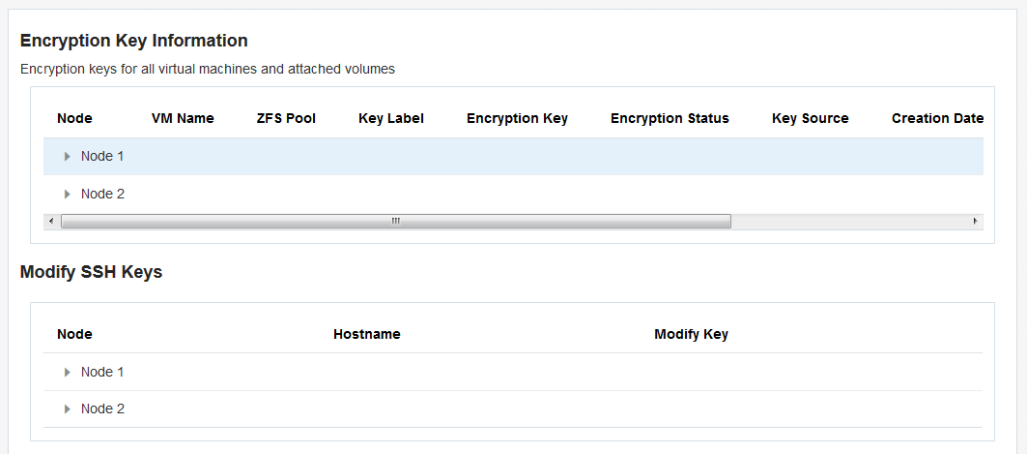
- Inserimento di una nuova chiave per autorizzare il protocollo SSH senza password: richiede l'immissione del nome utente della VM e del nome del computer VM, nonché della chiave pubblica RSA.

- Generazione automatica di nuove chiavi per le VM.

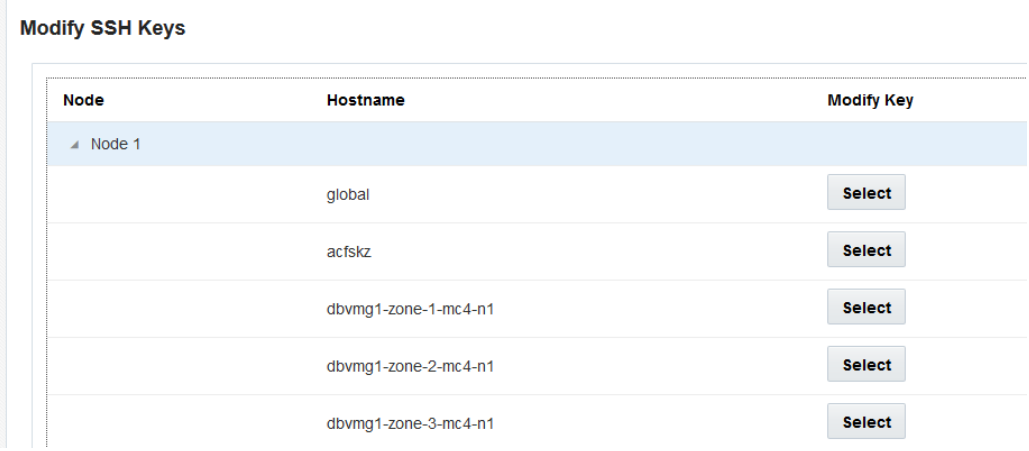
Nota - Per eseguire questa procedura mediante l'interfaccia CLI MCMU, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

---

1. **Accedere all'interfaccia BUI MCMU.**
2. **Selezionare Impostazioni del sistema -> Sicurezza nel pannello di navigazione.**



3. **Nel pannello Modifica chiavi SSH, fare clic su un nodo per espandere la visualizzazione.**



4. **Fare clic su Seleziona per la VM che si desidera modificare.**
5. **Selezionare un'opzione nell'elenco a discesa e fare clic su Successivo.**

   Sono disponibili le scelte seguenti:

   - Inserisci nuova chiave per autorizzare SSH senza password
   - Genera automaticamente nuove chiavi per le VM
6. **Fare clic su Successivo.**
7. **Se si scelto di autorizzare SSH senza password, immettere le informazioni seguenti, quindi fare clic su Successivo:**

   - Nome utente del computer
   - Nome host del computer
   - Chiave pubblica RSA del computer
8. **Fare clic su Imposta SSH.**

   La modifica viene applicata.

Comunicazione sicura con IPsec

Per proteggere la confidenzialità e l'integrità delle comunicazioni basate su IP tra le zone e il traffico NFS nella rete, si consiglia l'uso di IPsec (IP Security) e IKE (Internet Key Exchange). IPsec è consigliato perché supporta l'autenticazione peer a livello di rete, l'autenticazione dell'origine dei dati, la confidenzialità e l'integrità dei dati e la protezione della replica. Quando vengono utilizzati nella piattaforma Oracle MiniCluster, IPsec e IKE sono in grado di sfruttare automaticamente l'accelerazione crittografica assistita da hardware, riducendo al minimo l'impatto che l'uso della crittografia per proteggere le informazioni riservate che fluiscono nel canale di rete può avere sulle prestazioni.

▼ Configurazione di IPsec e IKE

Per poter configurare IPsec, è necessario definire i nomi host e/o gli indirizzi IP specifici utilizzati tra i peer comunicanti.

Per l'esempio di questa procedura vengono utilizzati gli indirizzi 10.1.1.1 e 10.1.1.2 per indicare due zone non globali Solaris gestite da un unico tenant. La comunicazione tra i due indirizzi verrà protetta con IPsec. L'esempio si basa sulla prospettiva della zona non globale associata all'indirizzo IP 10.1.1.1.

Per configurare e usare IPsec e IKE in una coppia di zone non globali (virtual machine) designate, attenersi alla procedura riportata di seguito.

1. **Definire il criterio di sicurezza IPsec.**

   Definire il criterio di sicurezza che verrà applicato per la coppia di zone comunicanti.

   In questo esempio, tutte le comunicazioni di rete tra gli indirizzi 10.1.1.1 e 10.1.1.2 verranno cifrate:

   ```
   {laddr 10.1.1.1 raddr 10.1.1.2}
   ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
   ```

2. **Memorizzare il criterio nel file `/etc/inet/ipsecinit.conf`.**

3. **Verificare che il criterio IPsec sia corretto dal punto di vista sintattico.**

   Esempio:

   ```
   # ipsecconf –c –f ipsecinit.conf
   ```

4. **Configurare il servizio IKE (Internet Key Exchange).**

   Configurare il servizio in conformità con le impostazioni di host e algoritmo presenti nel file `/etc/inet/ike/config`.

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5

   auth_alg sha256 encr_alg aes } }
   ```

5. **Configurare la chiave precondivisa.**

   Per poter abilitare IPsec, è necessario che il materiale chiave venga condiviso per entrambi i nodi peer in modo che possano autenticarsi reciprocamente.

   L'implementazione IKE di Oracle Solaris supporta numerosi tipi di chiavi, tra i quali le chiavi precondivise e i certificati. Per praticità, in questo esempio vengono utilizzate le chiavi precondivise memorizzate nel file `/etc/inet/secret/ike.preshared`. Possono essere tuttavia adottate forme di autenticazione più rigorose da parte delle organizzazioni che le ritengono necessarie.

   Modificare il file /etc/inet/secret/ike.preshared e immettere le informazioni della chiave precondivisa. Ad esempio:

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **Abilitare i servizi IPsec e IKE in entrambi i peer.**

   Affinché la comunicazione cifrata sia possibile, i servizi devono essere abilitati in entrambi i peer in comunicazione.

   Esempio:

```
# svcadm enable svc:/network/ipsec/policy:default
# svcadm enable svc:/network/ipsec/ike:default
```

Controllo dell'accesso

Gli argomenti riportati di seguito descrivono le funzioni di controllo dell'accesso disponibili in MiniCluster.

▼ Modifica delle password `root` Oracle ILOM predefinite

Il sistema viene distribuito con password predefinite assegnate agli account root di Oracle ILOM su entrambi i nodi. Ciò consente di eseguire il processo di installazione con un account di accesso iniziale previsibile. Si consiglia di modificare le password predefinite subito dopo l'installazione per garantire la massima sicurezza possibile.

1. **Eseguire il login a Oracle ILOM nel nodo 1 come `root`.**

   Usare il comando `ssh` per connettersi a Oracle ILOM.

   Per ottenere i nomi host di Oracle ILOM, selezionare Impostazioni del sistema -> Informazioni di sistema. I nomi host vengono elencati nella colonna ILOM.

   Sintassi:

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

   Immettere la password root Oracle ILOM predefinita: welcome1

2. **Modificare la password `root` Oracle ILOM.**

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: ***********
```

3. **Ripetere la procedura per modificare la password `root` Oracle ILOM anche nel nodo 2.**

4. **Aggiornare Oracle Engineered Systems Hardware Manager con le nuove password.**

   Vedere «Update Component Passwords» in *Oracle MiniCluster S7-2 Administration Guide*.

▼ Configurazione delle password EEPROM

Ogni nodo MiniCluster dispone di un EEPROM, a cui a volte viene fatto riferimento come OpenBoot PROM, ovvero un firmware di basso livello contenente alcuni parametri di configurazione e driver che agevolano il boot del sistema. Per impostazione predefinita, la funzione della password EEPROM è disabilitata.

In ambienti sicuri, usare la procedura descritta di seguito per abilitare la funzione della password e impostare una password. La password viene abilitata e applicata automaticamente a entrambi i nodi.

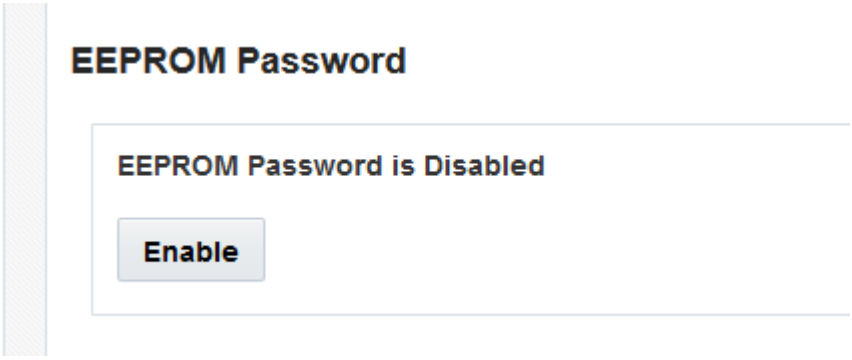
Questa procedura sostituisce i metodi precedenti in cui la password veniva impostata al prompt `ok` di OpenBoot o in Oracle Solaris con il comando `eeprom`.

Attenzione - È importante ricordare la password. Se si dimentica la password, sarà necessario rivolgersi ai servizi di assistenza per poter effettuare di nuovo il boot del sistema.

Nota - La procedura riportata di seguito descrive come impostare le password tramite l'interfaccia BUI MCMU. In alternativa, è possibile usare il comando `mcmu security -e`.

1. **Eseguire il login a MCMU come amministratore principale, ad esempio `mcinstall`.**

2. **Selezionare Impostazioni del sistema -> Sicurezza nel pannello di navigazione**



3. **Effettuare una delle operazioni riportate di seguito.**

   - Per abilitare e impostare la password: fare clic su Enable, immettere due volte la password, quindi fare clic su Set Password.
   - Per disabilitare la funzione: fare clic su Disable, quindi su Confirm.
   - Per modificare una password esistente: Change Password, immettere due volte la nuova password, quindi fare clic su Update.

Provisioning utente

Durante l'installazione di MiniCluster, il processo di installazione richiede di creare e registrare il primo utente MCMU denominato `mcinstall`. Vengono raccolte le informazioni demografiche dell'utente, che comprendono l'indirizzo di posta elettronica e il numero di telefono. L'utente `mcinstall` è il primo account amministratore primario. Alla prima esecuzione del login come `mcinstall`, la utility richiede all'utente `mcinstall` di creare una nuova password conforme ai criteri password di Oracle Solaris associati al profilo di sicurezza.

Durante la registrazione dell'utente `mcinstall`, viene richiesto di specificare la persona che fungerà da supervisore MCMU. Il supervisore viene identificato solo mediante un nome e un indirizzo di posta elettronica. Il supervisore non è un utente della utility MCMU e non dispone di credenziali di login.

Gli utenti supervisore e mcinstall vengono associati entrambi a nomi di persone reali e a indirizzi di posta elettronica validi.

A provisioning degli utenti MCMU effettuato, a ogni account utente viene assegnato un ruolo di amministratore primario o di amministratore secondario (vedere sezione chiamata «Controllo

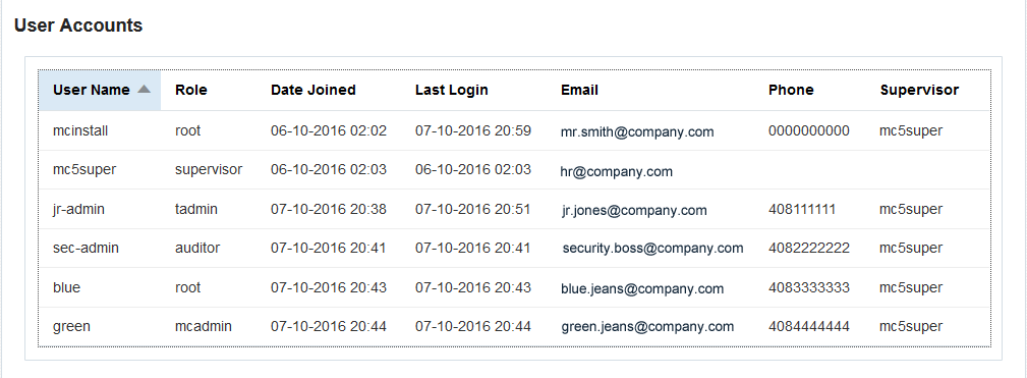
dell'accesso basato su ruoli » [31]). Per abilitare il nuovo account, è necessario che l'utente `mcinstall` e il supervisore approvino il nuovo account utente utilizzando l'URL ricevuto in un messaggio di posta elettronica (vedere sezione chiamata «Processo di approvazione degli utenti MCMU» [30]). Al primo login l'utente deve impostare una password conforme ai criteri password MCMU. Vedere sezione chiamata «Criteri di autenticazione utente e password» [33].

Processo di approvazione degli utenti MCMU

Per tutti gli account utente MCMU è richiesta l'approvazione di due persone, ovvero il supervisore e l'amministratore primario della utility MCMU. Il processo viene descritto di seguito.

1. L'utente potenziale (o l'amministratore MCMU che agisce per conto dell'utente) accede alla pagina di registrazione MCMU e fornisce i dettagli obbligatori seguenti:
   - nome utente MCMU;
   - indirizzo di posta elettronica;
   - nome e cognome;
   - numero di telefono;
   - ruolo MCMU.
2. Il supervisore e l'amministratore primario ricevono dalla utility MCMU un messaggio di posta elettronica in cui viene richiesto di approvare o rifiutare l'account. Il messaggio di posta elettronica contiene un URL per la funzione di approvazione/negazione della utility MCMU e include un identificativo di chiave univoca.
3. Dopo l'approvazione da parte del supervisore e dell'amministratore primario, l'account utente viene abilitato e il nuovo utente riceve dalla utility MCMU un messaggio di conferma dell'attivazione dell'account. L'utente riceve un account MCMU a cui è possibile accedere mediante l'interfaccia BUI o CLI MCMU. L'utente riceve anche un account utente di Oracle Solaris. Se l'utente esiste in un protocollo LDAP aziendale e MiniCluster è configurato con un client LDAP, l'utente potrà utilizzare solo LDAP per l'account Oracle Solaris.

Tutti gli utenti registrati vengono memorizzati nel repository MCMU. Un amministratore MCMU può verificare gli utenti, compresi i relativi ruoli, e il supervisore selezionando Impostazioni del sistema -> Account utente. Esempio:



User Accounts

User Name	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	408111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

Le modalità di esecuzione di questi task vengono descritte negli argomenti successivi di questa sezione.

Controllo dell'accesso basato su ruoli

Non esiste un utente `root` in MiniCluster. In effetti, root è un ruolo assegnato agli utenti MCMU registrati come amministratori primari.

Durante la procedura di creazione, all'utente MCMU viene assegnato uno dei ruoli riportati di seguito.

- **Amministratore primario (ruolo `root`)**: il ruolo `root` definisce i diritti e i privilegi degli amministratori primari del sistema MiniCluster, compresi tutti i nodi di calcolo, le reti, il database e lo storage. Gli utenti che dispongono del ruolo `root` possono eseguire qualsiasi operazione di installazione e tutte le operazioni di amministrazione critiche senza alcuna limitazione. Gli amministratori primari possono delegare le operazioni e approvare l'aggiunta e l'eliminazione degli utenti, compresi i nuovi amministratori primari e secondari. L'utente deve eseguire il login con le proprie credenziali. Tutte le azioni e le operazioni effettuate vengono registrate e sottoposte a controllo in base all'identificativo dell'utente e non all'identificativo del ruolo.
- **Amministratore secondario (ruolo `mcadmin`)** : questo ruolo definisce i diritti e i privilegi degli amministratori secondari dei domini e delle zone non globali MiniCluster. Per impostazione predefinita, questo ruolo consente solamente l'accesso in sola lettura a MCMU. Tutte le azioni e le operazioni effettuate vengono registrate e sottoposte a controllo in base all'identificativo dell'utente e non all'identificativo del ruolo.
- **Amministratore tenant (ruolo `tadmin`)**: questo ruolo definisce i diritti e i privilegi dell'amministratore di una VM MiniCluster. Il ruolo definisce i diritti e i privilegi di un amministratore VM che svolge le operazioni amministrative quotidiane a supporto delle installazioni e della distribuzione delle applicazioni. Tutte le azioni vengono sottoposte a controllo in base all'identificativo dell'utente e non all'identificativo del ruolo.

- **Auditor (ruolo `auditor`)**: gli utenti con questo ruolo possono accedere alla pagina di revisione del controllo dell'interfaccia BUI MCMU, in cui possono visualizzare lo stato dei pool di controllo e generare report per le attività utente. Solo gli utenti con questo ruolo possono accedere alla pagina di revisione del controllo. Gli auditor non possono accedere a MCMU (tranne che per la pagina di controllo) né effettuare il login alle zone del kernel o alle VM.

Account utente

In MiniCluster sono disponibili gli account utente elencati in questa tabella.

Utente	Password	Ruolo	Descrizione
`mcinstall`	La password viene configurata durante l'installazione. Può essere reimpostata e modificata mediante la utility MCMU.	`root`	Il processo di installazione richiede la creazione di `mcinstall` come amministratore principale di MCMU e la creazione di una password. Questo account è destinato ad essere l'amministratore principale di MCMU. Questo account utente viene utilizzato per le attività seguenti: ■ inizializzazione del sistema durante l'installazione mediante l'esecuzione di `installmc`; ■ amministrazione del sistema, incluse le VM che utilizzano l'interfaccia BUI e CLI `mcmu` MCMU; ■ assunzione del ruolo `root` (`su` impostato su root) nelle VM delle applicazioni, nella zona globale e nelle zone kernel per i privilegi di superutente.
Supervisore MCMU: nome account determinato durante l'installazione.	N/D	N/D	Nel software MiniCluster, l'utente supervisore è identificato unicamente da un nome utente e un indirizzo di posta elettronica. Non costituisce una credenziale di login. È possibile usare questo account per fornire un secondo livello nel processo di approvazione degli utenti MCMU. Questo utente riceve un messaggio di posta elettronica a ogni creazione di un nuovo utente MCMU. Il nuovo utente deve essere approvato dal supervisore e dall'amministratore primario affinché l'account utente sia abilitato. È possibile usare questo account per fornire un secondo livello nel processo di approvazione degli utenti MCMU mediante l'assegnazione come supervisore di una persona diversa dall'amministratore primario.
(Facoltativo) *Amministratore tenant*: nome account determinato al momento della registrazione dell'utente.	Determinato al momento del login iniziale.	`tadmin`	Questo utente può eseguire tutte le attività successive all'installazione solo sulle VM. Questo utente non può accedere alle zone globali o kernel e non può eseguire l'interfaccia BUI o CLI MCMU.
(Facoltativo) *Amministratore secondario*: nome account	Determinato al momento del login iniziale.	`mcadmin`	Quando un utente MCMU viene creato e assegnato come amministratore secondario e dispone dell'accesso in sola lettura alle zone non globali.

Utente	Password	Ruolo	Descrizione
determinato al momento della registrazione dell'utente.			
`oracle`	La password è uguale alla password dell'utente `mcinstall`.	`root`	Questo account utente viene utilizzato per le attività seguenti: ■ login iniziale alle VM di database per configurare le VM di database con un database, dati, e altri account in base alle esigenze; ■ assunzione del ruolo root (`su` impostato su root) nelle VM di database per i privilegi di superutente.

La password MCMU predefinita utilizzata durante il primo login è `welcome1`. Dopo l'immissione della password `welcome1`, la utility obbliga l'utente a creare una nuova password conforme ai criteri password definiti. Vedere sezione chiamata «Criteri di autenticazione utente e password» [33].

Tutte le azioni eseguite da tutti gli utenti della utility MCMU vengono registrate in base all'identificativo dell'utente. Per informazioni sui report di controllo, vedere Report di controllo e conformità [39].

Nota - Gli account utente MCMU non vengono utilizzati per l'uso di routine del sistema, ad esempio per l'utilizzo delle applicazioni e dei database. Gli account utente vengono gestiti mediante Oracle Solaris, l'applicazione e il database presente nelle VM, nonché tramite i servizi di denominazione del sito.

Criteri di autenticazione utente e password

A tutti gli utenti di cui è stato eseguito il provisioning in MiniCluster viene assegnato un ruolo con criteri password rigorosi e la cifratura applicata dal profilo di sicurezza.

Il criterio di sicurezza predefinito stabilisce i requisiti seguenti per la password MCMU:

- deve contenere almeno 14 caratteri;
- deve contenere almeno un carattere numerico;
- deve contenere almeno un carattere alfanumerico maiuscolo;
- deve differire da una password precedente per almeno tre caratteri;
- non deve corrispondere alle 10 password precedenti.

Tutti gli utenti eseguono il login al proprio account Oracle Solaris utilizzando esclusivamente la password utente personale.

▼ Verifica dei ruoli utente Oracle Solaris

1. **Eseguire il login alla zona globale MiniCluster e assumere il ruolo root.**

   Per ulteriori dettagli, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

2. **Verificare l'elenco dei ruoli disponibili.**

   ```
   # logins -r
   ```

3. **Verificare il ruolo e la password utente richiesti per l'autenticazione:**

   ```
   # grep root /etc/user_attr
   root::::audit_flags=lo\:no;type=role;roleauth=user
   mcinstall::::auths=solaris.system.maintenance;roles=root
   ```

Eliminazione sicura delle VM

L'eliminazione delle VM e dei gruppi di VM è una prerogativa esclusiva dell'amministratore primario MCMU. Quando un componente VM viene eliminato, le chiavi corrispondenti vengono eliminate in modo automatico e viene inviato un messaggio di posta elettronica all'amministratore primario.

Per verificare questa funzione, prima di eliminare un componente VM eseguire il login all'interfaccia BUI MCMU come amministratore primario e osservare le chiavi di cifratura (Impostazioni del sistema -> Sicurezza). Eliminare il componente VM, quindi osservare di nuovo le chiavi. La VM e l'etichetta di chiave associata al componente eliminato non sono più visualizzate.

▼ Verifica delle regole di firewall basate su host

Tutti gli ambienti computazionali, comprese le zone globali, le zone kernel e le zone non globali, vengono configurate in modo automatico con firewall IPFilter. Non è necessario alcun intervento manuale.

Per verificare i componenti IPFilter in uso, effettuare le operazioni riportate di seguito.

1. **Eseguire il login alla zona globale nel nodo 1 come utente `mcinstall` e assumere il ruolo `root`.**

   Per le istruzioni di login Oracle ILOM, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. Controllare la configurazione IPFilter.

Assicurarsi che le regole contenute nel file `/etc/ipf/ipf.conf` corrispondano all'output della schermata riportata di seguito.

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. Verificare che i servizi IPF siano online.

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
```

```
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **Assicurarsi inoltre che i database e le applicazioni siano accessibili senza dover modificare le regole dei firewall.**

Verifica dell'ambiente della funzione Boot verificato

Boot verificato di Oracle Solaris è una funzione anti-malware e di controllo dell'integrità che riduce il rischio di introdurre componenti critici di boot e kernel potenzialmente dannosi o modificati per errore. Questa funzione controlla le firme crittografiche predefinite del firmware, del sistema di boot e del kernel.

Le zone globali di MiniCluster sono configurate per impostazione predefinita con la funzione Boot verificato di Oracle Solaris. Se si desidera verificare se il sistema è configurato con la funzione Boot verificato, effettuare le operazioni riportate di seguito.

1. **Eseguire il login a Oracle ILOM in uno dei nodi.**
   Per le istruzioni di login Oracle ILOM, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

2. **Controllare la configurazione della funzione Boot verificato in Oracle ILOM.**
   Assicurarsi che `boot_policy` sia impostato su `warning`.

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **Controllare l'impostazione dei criteri di Boot verificato.**
   Assicurarsi che `module_policy` sia impostato su `enforce`.

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **Avviare la console host per accedere alla zona globale.**
   Eseguire il login come utente `mcinstall`.

```
-> start /HOST/console
```

```
Are you sure you want to start /HOST/console (y/n)? y

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **Cercare nella zona globale la prova che il sistema si sia avviato con una configurazione Boot verificato.**

   Controllare nel file `messages` la presenza della stringa `NOTICE: Verified boot enabled; policy=warning`.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

Limitazione dell'accesso allo storage condiviso

MiniCluster include un array di storage con una combinazione di unità SSD e HDD. Le unità HDD possono essere configurate per fornire lo storage condiviso alle VM.

MiniCluster include una funzione di isolamento dello storage condiviso, ovvero una funzione di attivazione e disattivazione che agevola l'isolamento dello storage condiviso applicato solo alle zone globali e kernel. Ciò consente di isolare un ambiente gruppo di VM di sicurezza e abilitato alla conformità dalla condivisione di file con le zone globali e kernel. Ciò assicura che i gruppi di VM non siano più collegati agli accessi NFS e che i servizi NFS siano disabilitati.

Per garantire un livello di sicurezza elevato per gli ambienti, non abilitare lo storage condiviso per le VM di database e le VM delle applicazioni. Quando la funzione di storage condiviso è abilitata, il file system deve essere accessibile per le VM in modalità di sola lettura. Per istruzioni su come abilitare o disabilitare lo storage condiviso, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*, disponibile all'indirizzo: `http://docs.oracle.com/cd/E69469_01`.

La directory `/sharedstore` è il punto di accesso per lo storage condiviso.

- **Basandosi sulle esigenze di sicurezza del proprio ambiente di lavoro, configurare lo storage condiviso tenendo presenti i suggerimenti riportati di seguito.**

  - Assicurarsi che lo storage condiviso non sia disponibile per le VM di database e le VM delle applicazioni oppure che sia accessibile in modalità di sola lettura.
  - Nelle distribuzioni di produzione, assicurarsi che le zone kernel non siano accessibili tramite reti pubbliche o direttamente accessibili all'accesso client. È necessario interrompere

ogni accesso e uso diretto dei servizi di storage condiviso da parte delle reti pubbliche o dell'accesso client. Se le VM richiedono l'accesso al file system `/sharedstore` tramite NFS, assicurarsi che tale operazione sia agevolata tramite i canali IPSEc/IKE.

Report di controllo e conformità

Gli argomenti riportati di seguito descrivono le funzionalità di creazione dei report di controllo e conformità disponibili in MiniCluster.

▼ Verifica dei criteri di controllo

Il criterio di controllo viene configurato durante l'installazione delle zone globali e non globali in fase di selezione di un profilo di conformità (equivalente a CIS (impostazione predefinita) o PCI-DSS).

Per verificare che i criteri di controllo siano abilitati, effettuare le operazioni riportate di seguito.

1. **Eseguire il login alla zona globale come utente `mcinstall` e assumere il ruolo `root`.**

   Per le istruzioni di login Oracle ILOM, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **Verificare che il servizio di controllo sia online.**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **Verificare che il plugin di controllo sia attivo.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **Verificare i criteri di controllo attivi.**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **Verificare che tutti i ruoli vengano acquisiti per il criterio di controllo `cusa`.**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ Revisione dei log di controllo

1. **Eseguire il login alla zona globale come utente `mcinstall` e assumere il ruolo `root`.**

   Per le istruzioni di login Oracle ILOM, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **Usare il comando `auditreduce` come mostrato.**

   Di seguito viene riportata la sintassi per la visualizzazione dei log di controllo.

```
auditreduce -z vm_name audit_file_name | praudit -s
```

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

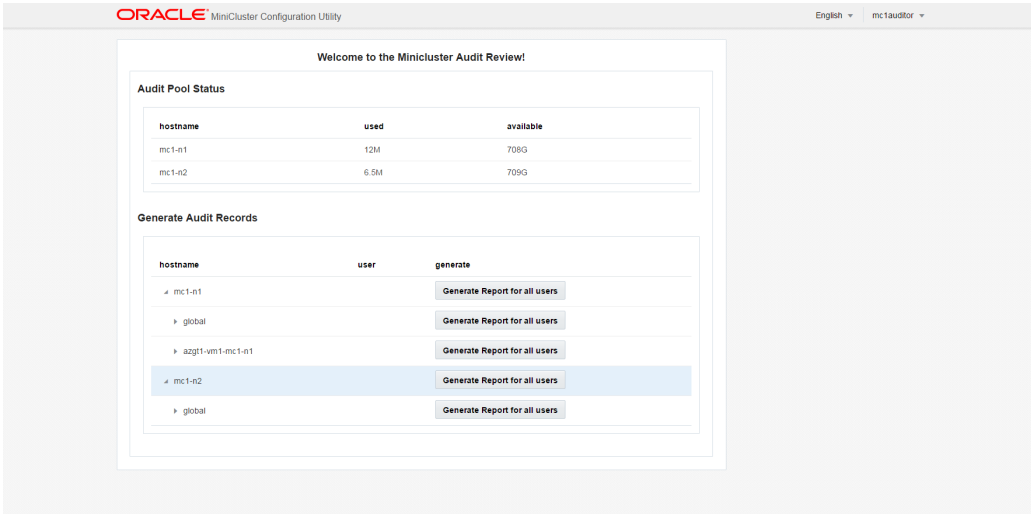
Generazione dei report di controllo

Usare questa procedura per generare i report di controllo per un nodo o per singole VM e zone globali.

1. **Eseguire il login a MCMU come utente a cui è stato assegnato il ruolo Auditor.**
   Per informazioni su utenti e ruoli di MCMU, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*, disponibile all'indirizzo: `http://docs.oracle.com/cd/E69469_01`.

2. **Selezionare Impostazioni del sistema -> Sicurezza nel pannello di navigazione.**
   Viene visualizzata la pagina Audit Review.

Nota - Possono visualizzare questa pagina solo gli utenti di MCMU a cui è stato assegnato il ruolo Auditor.

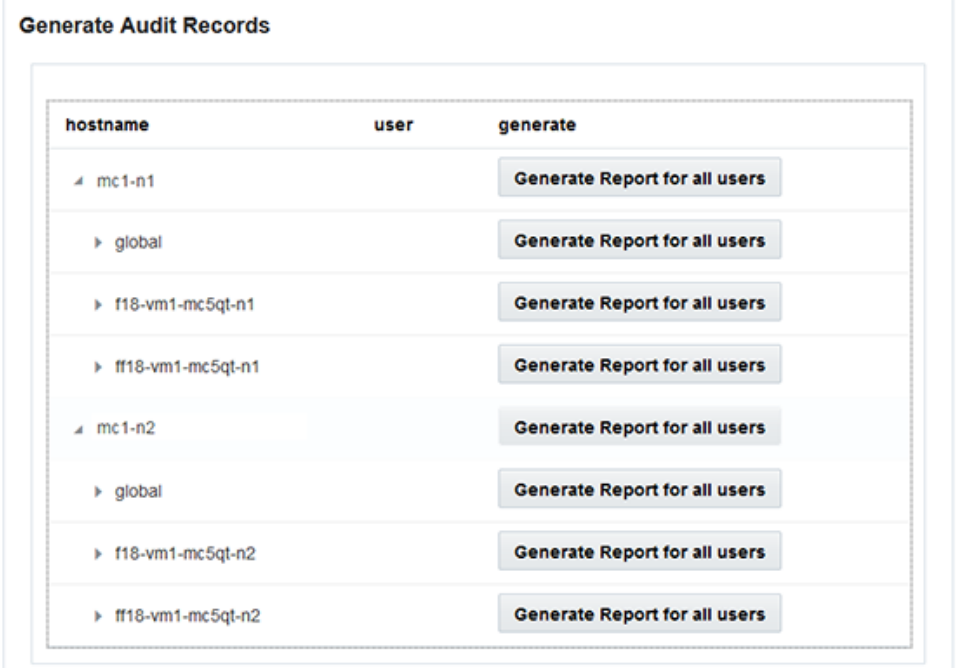


3. **Controllare la sezione Audit Pool Status.**
   In questa sezione viene indicata la quantità di spazio utilizzata e disponibile per i pool di controllo in ogni nodo.

4. **Per generare un report per l'intero nodo, fare clic sul pulsante Generate di uno dei nodi e andare al Passo 6**
   In alternativa, è possibile generare un report per una VM o una zona specifica. Vedere il Passo 5

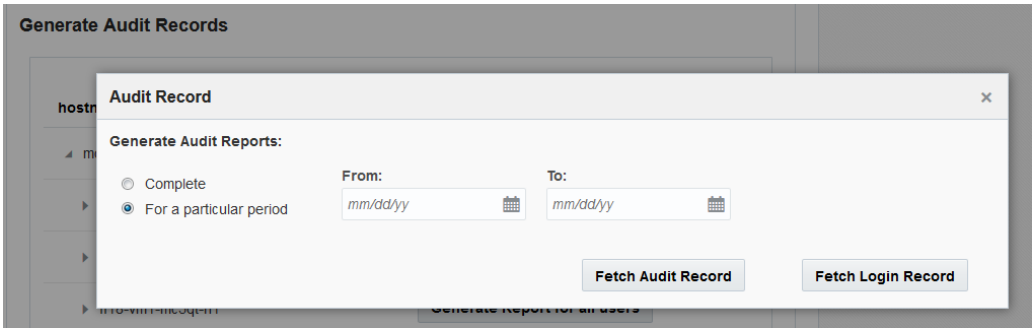
5. **Per generare un report per una VM o una zona globale specifica, effettuare quanto riportato di seguito.**

a. **Fare clic sul triangolo accanto a un nodo per espandere la vista.**



b. **Per la VM o la zona globale, fare clic su Generate Report for all users.**

6. **Nella finestra di dialogo Audit Record, configurare i parametri relativi ai record di controllo.**



Sono disponibili le scelte seguenti:

- **Complete**: selezionare questa opzione se si desidera ottenere un report che includa tutti i record di controllo.
- **For a particular period**: selezionare questa opzione se si desidera specificare un periodo di tempo specifico, quindi immettere le date di inizio e fine periodo.

7. **Fare clic su uno dei pulsanti Fetch.**
   Sono disponibili le scelte seguenti:

   - **Fetch Audit Record**: genera un record di controllo completo.
   - **Fetch Login Record**: genera le attività eseguite dall'utente, come i login, i logout e le azioni dell'utente.

8. **Fare clic sul pulsante Click Here e selezionare il file XML di download.**
   Il file XML può essere importato in applicazioni di analisi del controllo come Oracle Audit Vault.

9. **Fare clic su Close.**

▼ (Se richiesto) Abilitazione del funzionamento conforme a FIPS 140 (Oracle ILOM)

L'uso della crittografia convalidata in base a FIPS 140 è obbligatorio per i clienti del Governo federale degli Stati Uniti.

Per impostazione predefinita, Oracle ILOM non utilizza la crittografia convalidata in base a FIPS 140. È tuttavia possibile abilitare l'uso di questo tipo di crittografia, se necessario.

Alcune funzioni e funzionalità di Oracle ILOM non sono disponibili quando il sistema è configurato per il funzionamento conforme a FIPS 140. L'elenco di tali funzioni e funzionalità è disponibile nella sezione "Funzionalità non supportate quando la modalità FIPS è abilitata" della *Guida per la sicurezza di Oracle ILOM*.

Vedere anche sezione chiamata «Conformità a FIPS-140-2, Livello 1» [44].

Attenzione - Questa procedura richiede la reimpostazione di Oracle ILOM. La reimpostazione implica la perdita di tutte le impostazioni configurate dall'utente. Per questo motivo, prima di apportare ulteriori modifiche specifiche del sito a Oracle ILOM, è necessario abilitare il funzionamento conforme a FIPS 140. Per i sistemi in cui sono state apportate modifiche alla configurazione specifiche del sito, eseguire il backup della configurazione di Oracle ILOM in modo da ripristinarla dopo la reimpostazione di Oracle ILOM, altrimenti le modifiche alla configurazione andranno perse.

1. **Sulla rete di gestione eseguire il login a Oracle ILOM.**

2. **Determinare se Oracle ILOM è configurato per il funzionamento conforme a FIPS 140.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

In Oracle ILOM la modalità di funzionamento conforme a FIPS 140 è rappresentata dalle proprietà `state` e `status`. La proprietà `state` rappresenta la modalità configurata in Oracle ILOM, mentre la proprietà `status` rappresenta la modalità operativa in Oracle ILOM. Quando la proprietà `state` di FIPS viene modificata, la modifica non ha effetto sulla proprietà `status` di FIPS per la modalità operativa fino al successivo reboot di Oracle ILOM.

3. **Abilitare il funzionamento conforme a FIPS 140.**

```
-> set /SP/services/fips state=enabled
```

4. **Riavviare il processore di servizio di Oracle ILOM.**

Per rendere effettiva questa modifica, è necessario riavviare il processore di servizio di Oracle ILOM.

```
-> reset /SP
```

Conformità a FIPS-140-2, Livello 1

Le applicazioni di crittografia presenti in MiniCluster si basano sulla funzione Cryptographic Framework di Oracle Solaris, convalidata per la conformità a FIPS 140-2, Livello1. La funzione Cryptographic Framework di Oracle Solaris rappresenta lo store di crittografia centrale per Oracle Solaris e offre due moduli verificati in base a FIPS 140 che supportano i processi dello spazio utente e a livello kernel. Questi moduli di libreria offrono alle applicazioni funzioni di cifratura, decifrazione, hashing, creazione e verifica di firme, creazione e verifica di certificati, autenticazione dei messaggi. Le applicazioni a livello utente che effettuano chiamate in questi moduli vengono eseguite in modalità FIPS 140.

Oltre alla funzione Cryptographic Framework di Oracle Solaris, anche il modulo oggetto OpenSSL fornito con Oracle Solaris è convalidato per la conformità a FIPS 140-2, Livello 1 e supporta la crittografia per le applicazioni basate sui protocolli Secure Shell e TLS. Il provider di servizi cloud può scegliere di abilitare gli host tenant con modalità conformi a FIPS 140. Quando vengono eseguiti in modalità conformi a FIPS 140, Oracle Solaris e OpenSSL, che sono provider di FIPS 140-2, applicano l'uso degli algoritmi di crittografia convalidati in base a FIPS 140.

Vedere anche (Se richiesto) Abilitazione del funzionamento conforme a FIPS 140 (Oracle ILOM) [43].

Nella tabella riportata di seguito vengono elencati gli algoritmi approvati in base a FIPS che sono supportati da Oracle Solaris in MiniCluster.

Chiave o CSP	Numero di certificato	
	v1.0	**v1.1**
Chiave simmetrica		
AES: modalità ECB, CBC, CFB-128, CCM, GMAC, GCM e CTR per dimensioni di chiave a 128, 192 e 256 bit	#2311	#2574
AES: modalità XTS per dimensioni di chiave a 256 e 512 bit	#2311	#2574
TripleDES: modalità CBC e ECB per l'opzione di cifratura 1	#1458	#1560
Chiave asimmetrica		
Generazione/verifica di firme RSA PKCS#1.5: 1024 bit, 2048 bit (con SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
Generazione/verifica di firme ECDSA: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
SHS (Secure Hashing Standard)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
Autenticazione dei messaggi basata su hash (con chiave)		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Generatori di numeri casuali		
Generatore di numeri casuali swrand FIPS 186-2	#1154	#1222
Generatore di numeri casuali n2rng FIPS 186-2	#1152	#1226

Oracle Solaris offre due provider di algoritmi di crittografia convalidati per FIPS 140-2, Livello 1.

- La funzione Cryptographic Framework di Oracle Solaris rappresenta lo store di crittografia centrale in un sistema Oracle Solaris e fornisce due moduli FIPS 140. Il modulo userland fornisce la crittografia per le applicazioni che vengono eseguite nello spazio utente, mentre il modulo kernel fornisce la crittografia per i processi a livello kernel. Questi moduli di libreria offrono alle applicazioni funzioni di cifratura, decifrazione, hashing, creazione e verifica di firme, creazione e verifica di certificati, autenticazione dei messaggi. Le applicazioni a livello utente che effettuano chiamate in questi moduli vengono eseguite in modalità FIPS 140, ad esempio il comando `passwd` e IKEv2. I consumer a livello Kernel, ad esempio Kerberos e IPsec, utilizzano interfacce API di proprietà per effettuare chiamate nella struttura di crittografia del kernel.
- Il modulo oggetto OpenSSL fornisce la crittografia per SSH e per le applicazioni Web. OpenSSL è il toolkit Open Source per i protocolli SSL (Secure Sockets Layer) e TLS (Transport Layer Security) e fornisce una libreria di crittografia. In Oracle Solaris, SSH e Apache Web Server sono consumer del modulo OpenSSL FIPS 140. Con Oracle Solaris 11.2 viene fornita una versione FIPS 140 di OpenSSL che è disponibile per tutti i consumer, mentre la versione fornita con Oracle Solaris 11.1 è disponibile solo per Solaris SSH.

Poiché utilizzano le risorse della CPU in modo intensivo, i moduli del provider FIPS 140-2 non sono abilitati per impostazione predefinita. L'amministratore è responsabile dell'abilitazione dei provider in modalità FIPS 140 e della configurazione dei consumer.

Per ulteriori informazioni sull'abilitazione dei provider FIPS-140 in Oracle Solaris, consultare il documento *Using a FIPS 140 Enabled System in Oracle Solaris 11.2*, disponibile sotto l'intestazione Protezione del sistema operativo Oracle Solaris 11, all'indirizzo: http://docs.oracle.com/cd/E36784_01.

Valutazione delle conformità alla sicurezza

Gli argomenti riportati di seguito descrivono la funzione Benchmark di sicurezza di MiniCluster.

Benchmark di conformità alla sicurezza

Durante l'installazione del sistema, viene selezionato un profilo di sicurezza (PCI-DSS, equivalente a CIS e DISA-STIG) e il sistema viene configurato in modo automatico per soddisfare il profilo di sicurezza selezionato. Per garantire che il sistema continui a funzionare secondo i profili di sicurezza, la utility MCMU consente di eseguire appositi benchmark di sicurezza e di accedere ai report dei benchmark. Per amministrare i benchmark è possibile utilizzare sia l'interfaccia BUI che l'interfaccia CLI della utility MCMU.

L'esecuzione dei benchmark di sicurezza offre i vantaggi riportati di seguito.

- Possibilità di valutare e vagliare lo stato di sicurezza corrente delle VM di database e delle applicazioni.
- I test di conformità alla sicurezza supportano gli standard PCI-DSS, equivalenti a CIS (impostazione predefinita) e DISA-STIG in base al livello di sicurezza configurato durante l'installazione.
- I test di conformità alla sicurezza vengono eseguiti in modo automatico all'avvio del sistema e possono essere eseguiti su richiesta o in base a intervalli pianificati.
- Disponibili solo per gli amministratori primari della utility MCMU, i livelli e i report di conformità sono facilmente accessibili dall'interfaccia BUI.
- I report di conformità forniscono appropriati suggerimenti di risoluzione delle anomalie.

Nota - Il profilo DISA-STIG è attualmente in fase di revisione. Utilizzare questo profilo solo per uso sperimentale in ambienti non di produzione.

Pianificazione di un benchmark di conformità alla sicurezza (BUI)

Usare questa procedura per pianificare un benchmark di sicurezza utilizzando l'interfaccia BUI della utility MCMU. Per istruzioni sull'uso dell'interfaccia CLI MCMU, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

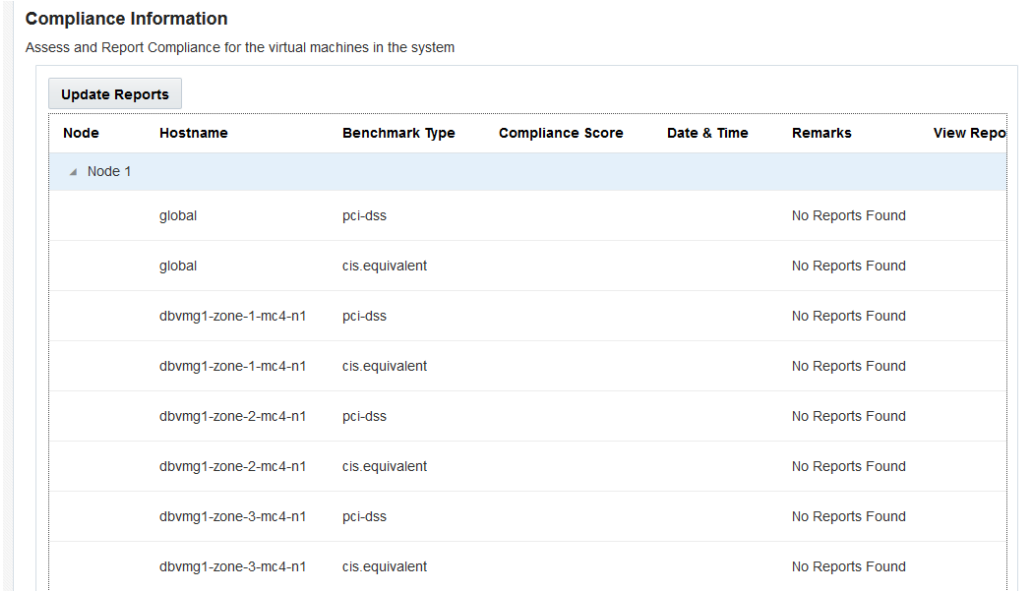
1. **Eseguire il login all'interfaccia BUI MCMU come amministratore primario.**

   Per le necessarie istruzioni, fare riferimento alla *Guida all'amministrazione di Oracle MiniCluster S7-2*.

2. **Nella home page, scorrere fino al pannello Informazioni sulla conformità.**

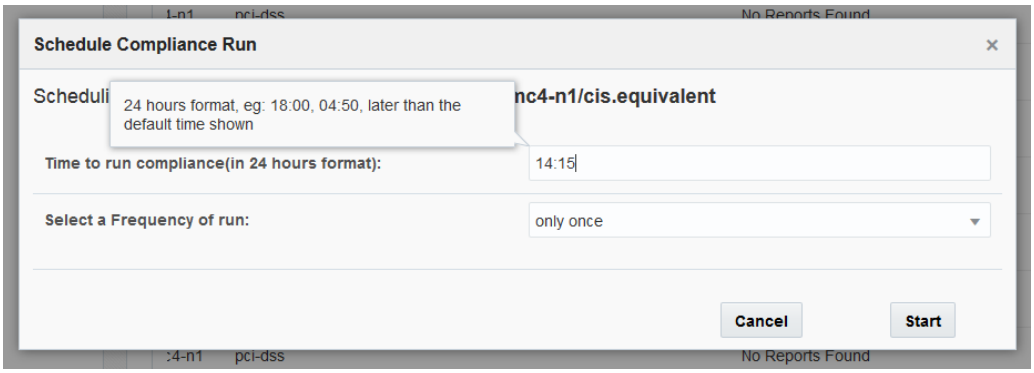
3. **Fare clic su un nodo per espanderne i dettagli.**

   Ogni zona e VM è stata configurata con un profilo di sicurezza (equivalente a CIS o PCI-DSS). Nel pianificare un benchmark è pertanto necessario selezionare un benchmark che corrisponda al profilo di sicurezza del componente.



4. **Scorrere a destra e fare clic sul pulsante Pianifica per una delle VM.**

Viene visualizzata la pagina di pianificazione del test di conformità.



5. **Specificare l'ora e la frequenza, quindi fare clic su Avvia.**

   Dopo che il test di conformità alla sicurezza sarà stato eseguito all'ora pianificata, visualizzare il report. Vedere Visualizzazione dei report dei benchmark (BUI) [49].

▼ Visualizzazione dei report dei benchmark (BUI)

Di seguito sono riportati i risultati di conformità accettabili.

	Equivalente a CIS	PCI-DSS
Zone globali	circa 88%	circa 88%
VM	circa 90%	circa 93%

Di seguito vengono indicati gli errori conosciuti dei test di conformità dovuti a problemi di Oracle Solaris.

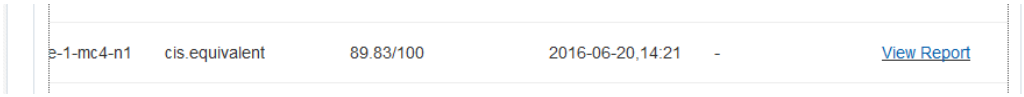
- Integrità del package (CoreOs, Rad-Python)
- GDM
- Daemon di instradamento
- Indirizzi di loopback SSH: la riduzione non risolve il problema.
- Servizi di denominazione che non riconoscono DNS
- Client LDAP

Di seguito vengono indicati gli errori conosciuti dei test di conformità dovuti a problemi di configurazione obbligatoria del cliente MiniCluster.

- Servizi client NFS: selezionare i servizi che devono essere disponibili.
- Impostazione della password eeprom: impostazione facoltativa.

1. **Eseguire il login all'interfaccia BUI MCMU.**
2. **Nella home page, scorrere fino al pannello Informazioni sulla conformità.**
3. **Fare clic su Aggiorna report.**

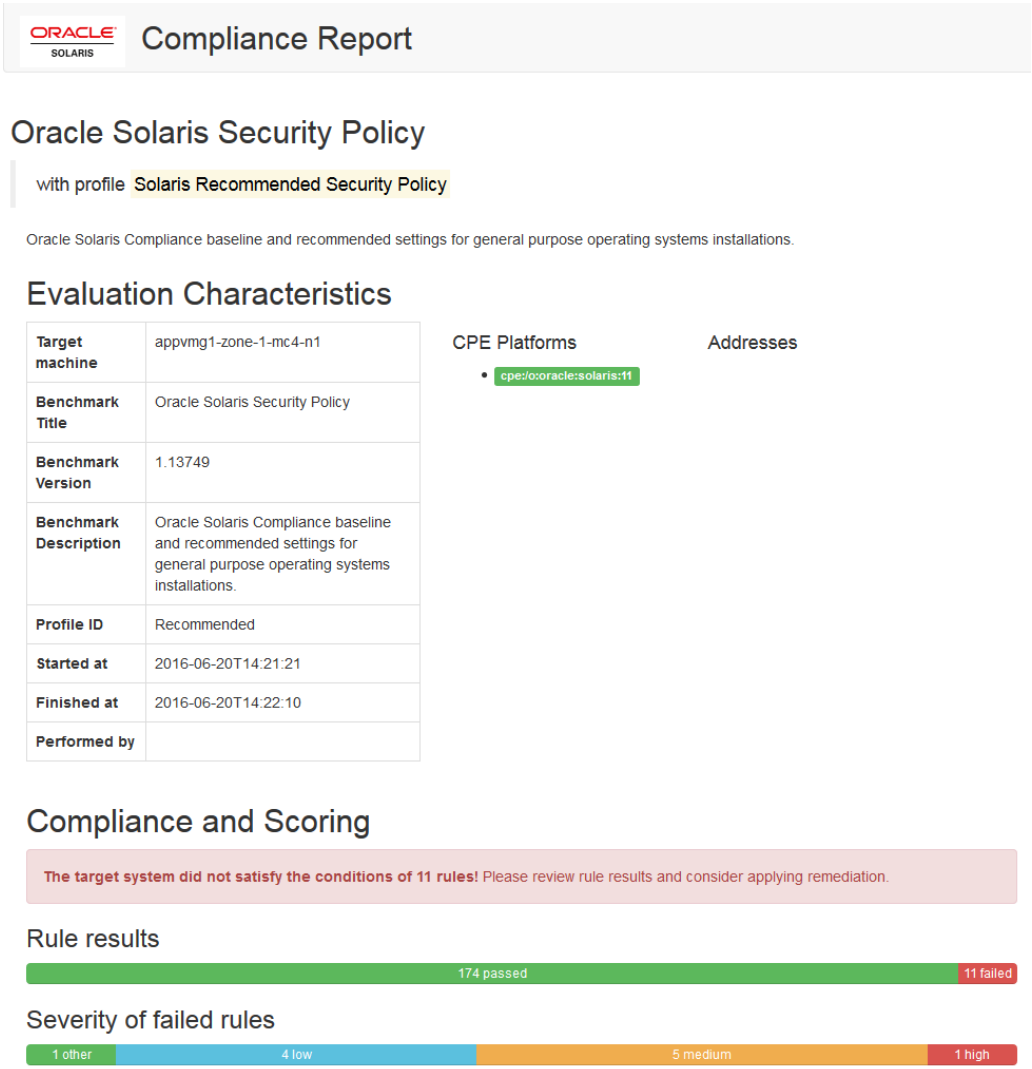
   Il processo di aggiornamento dura un minuto o poco più.
4. **Espandere la visualizzazione del nodo e identificare il report di conformità.**



5. **Scorrere a destra e fare clic su Visualizza report.**

   Viene visualizzato il report del benchmark.

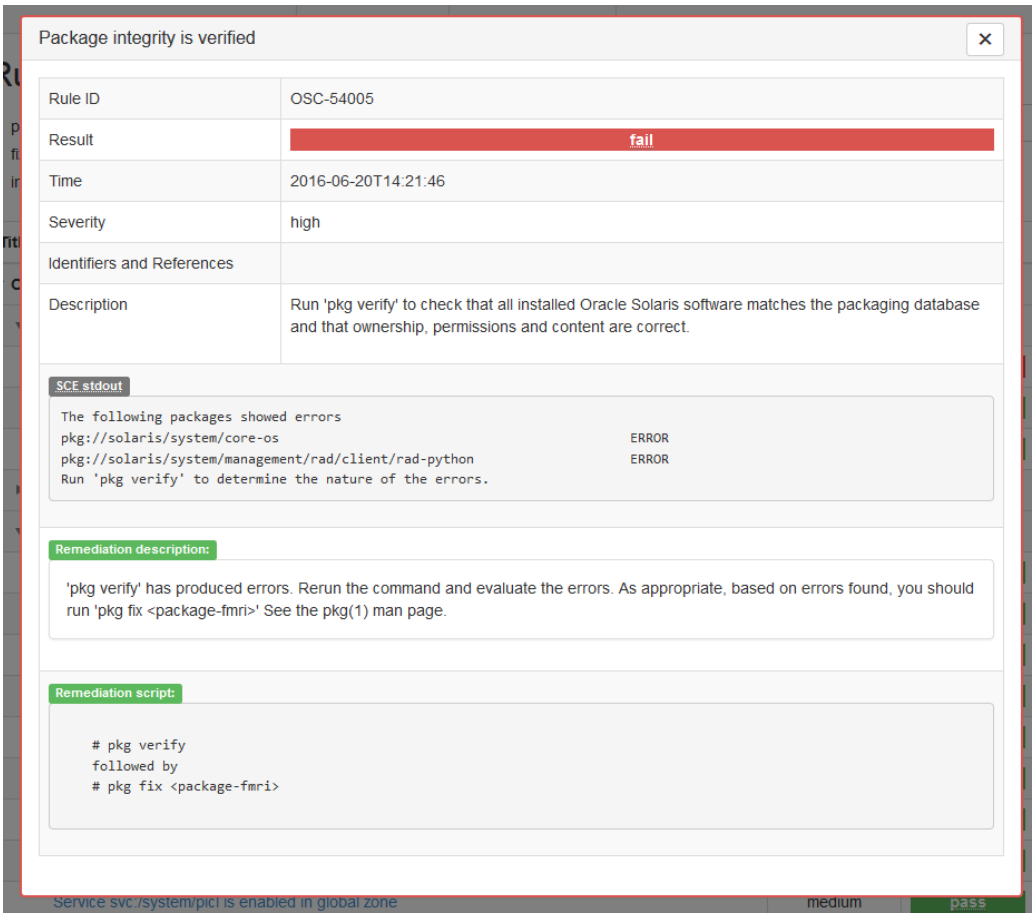
Nella sezione Panoramica regole è possibile selezionare i tipi di test da visualizzare in base ai risultati. È inoltre possibile specificare una stringa di ricerca del campo della ricerca.



6. **Basandosi sul report, è possibile verificare i controlli di sicurezza, i livelli di conformità, le eventuali anomalie e le procedure di risoluzione.**

7. **Fare clic sul nome di un test per ottenere i dettagli e le informazioni relative alla soluzione consigliata.**

Nota - Per visualizzare i dettagli completi di tutti i test, fare clic su Mostra tutti i dettagli dei risultati nella parte inferiore del report.



Informazioni sui controlli di sicurezza del server SPARC S7-2

Gli argomenti riportati di seguito descrivono i controlli di sicurezza per i componenti hardware e per l'ambiente OpenBoot.

Informazioni sulla sicurezza dei componenti hardware

L'isolamento fisico e il controllo dell'accesso costituiscono gli elementi di base per la creazione dell'architettura di sicurezza. L'installazione in un ambiente sicuro protegge il server fisico dagli accessi non autorizzati. In modo analogo, la registrazione di tutti i numeri di serie aiuta a evitare i rischi di furto, rivendita o inerenti alla supply chain (ovvero l'inserimento di componenti falsificati o che non funzionano correttamente nella supply chain dell'organizzazione alla quale si appartiene).

In queste sezioni vengono fornite linee guida generali relative alla sicurezza dei componenti hardware per MiniCluster.

Limitazioni di accesso

- Installare il server e le apparecchiature correlate in una stanza chiusa a chiave con accesso limitato.
- Se le apparecchiature sono installate in un rack dotato di sportello, chiudere sempre lo sportello fino a quando non è necessario effettuare un intervento sui componenti contenuti nel rack. La chiusura degli sportelli limita anche l'accesso ai dispositivi hot plug o hot swap.

- Conservare le unità sostituibili sul campo (FRU, Field Replaceable Unit) o le unità sostituibili dall'utente (CRU, Customer Replaceable Unit) di riserva in un armadio chiuso a chiave. Consentire l'accesso all'armadio chiuso a chiave solo al personale autorizzato.
- Verificare periodicamente lo stato e l'integrità delle serrature nel rack e dell'armadio dei ricambi per evitare o rilevare eventuali tentativi di manomissione o sportelli lasciati inavvertitamente aperti.
- Conservare le chiavi dell'armadio in un luogo sicuro con accesso limitato.
- Limitare l'accesso alle console USB. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU, Power Distribution Unit) e gli switch di rete possono essere dotati di connessioni USB. L'accesso fisico è il metodo di accesso a un componente più sicuro, in quanto non è soggetto ad attacchi che sfruttano la rete.
- Connettere la console a un dispositivo KVM esterno per abilitare l'accesso remoto alla console. I dispositivi KVM supportano spesso l'autenticazione basata su due fattori: il controllo dell'accesso centralizzato e il controllo. Per ulteriori informazioni sulle istruzioni di sicurezza e sulle procedure ottimali per il dispositivo KVM, fare riferimento alla documentazione fornita con il dispositivo KVM in uso.

Numeri di serie

- Tenere traccia dei numeri di serie di tutti i componenti hardware.
- Contrassegnare per la sicurezza tutti gli elementi significativi dell'hardware del computer, ad esempio le parti di ricambio. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.
- Conservare le chiavi e le licenze di attivazione dell'hardware in un luogo sicuro e facilmente accessibile al responsabile del sistema in caso di emergenze relative al sistema. I documenti stampati potrebbero essere la sola prova della proprietà del materiale.

I reader wireless RFID (Radio Frequency Identification) consentono di semplificare ulteriormente la registrazione degli asset. Il white paper Oracle relativo al *tracciamento degli asset del sistema Oracle Sun mediante RFID* è disponibile all'indirizzo:

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

Unità disco rigido

Le unità disco rigido vengono spesso utilizzate per memorizzare informazioni riservate. Per proteggere queste informazioni dalla diffusione non autorizzata, è necessario ripulire le unità disco rigido prima di riutilizzarle, decommissionarle o disfarsene.

- Utilizzare gli strumenti di cancellazione del disco, quale il comando Oracle Solaris `format` (1M), per cancellare completamente tutti i dati dall'unità disco rigido.

- Le organizzazioni sono tenute a fare riferimento ai criteri di protezione dei dati esistenti per determinare il metodo più appropriato per ripulire le unità disco fisso.
- Se necessario, utilizzare il servizio di conservazione di dati e dispositivi dei clienti di Oracle.

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Limitazione dell'accesso a OpenBoot

Gli argomenti riportati di seguito descrivono come limitare l'accesso al prompt OpenBoot.

Per le istruzioni sulla configurazione di una password per OpenBoot, vedere Configurazione delle password EEPROM [28].

- Come ottenere il prompt OpenBoot [55]
- Controllo dei login non riusciti [56]
- Specifica di un banner di accensione [56]

Per informazioni sull'impostazione delle variabili di sicurezza OpenBoot, fare riferimento alla documentazione OpenBoot disponibile all'indirizzo:

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

▼ Come ottenere il prompt OpenBoot

Questa procedura descrive come ottenere il prompt OpenBoot nei nodi di calcolo MiniCluster per configurare i controlli di sicurezza.

Per ottenere il prompt OpenBoot è necessario spegnere il sistema. Attenersi alle procedure appropriate di spegnimento delle VM descritte nella *Guida all'amministrazione di Oracle MiniCluster S7-2*.

1. **Eseguire il login a Oracle ILOM in un nodo ed eseguire questo comando.**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

Eseguire il login alla console host come utente `mcinstall` e con `su` impostato su `root`.

2. **Dopo aver spento tutte le VM, usare il ruolo root per arrestare la zona globale.**

```
# init 0
.
.
.
```

```
{0} ok
```

Controllo dei login non riusciti

1. **Determinare se qualcuno ha tentato di accedere all'ambiente OpenBoot senza riuscirci utilizzando il parametro `security-#badlogins`, come mostrato nell'esempio seguente.**

   ```
   {0} ok printenv security-#badlogins
   ```

   Se questo comando restituisce un valore qualsiasi maggiore di zero, vuol dire che è stato registrato un tentativo di accesso non riuscito all'ambiente OpenBoot.

2. **Reimpostare il parametro digitando questo comando.**

   ```
   {0} ok setenv security-#badlogins 0
   ```

Specifica di un banner di accensione

Sebbene non si tratti di un controllo di prevenzione o rilevamento diretto, è possibile utilizzare un banner per i motivi elencati di seguito.

- Trasferire la proprietà.
- Avvisare gli utenti dell'uso accettabile del server.
- Indicare che l'accesso o le modifiche ai parametri di OpenBoot sono limitati al personale autorizzato.

- **Utilizzare i comandi riportati di seguito per abilitare un messaggio di avvertenza personalizzato.**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  Il messaggio del banner può essere composto da un massimo di 68 caratteri. Sono consentiti tutti i caratteri stampabili.

Indice