Guida per la sicurezza di Oracle SuperCluster M7 Series

N. di parte: E69654-01
Febbraio 2016

N. di parte: E69654-01

Accessibilità alla documentazione

Per informazioni sull'impegno di Oracle per l'accessibilità, visitare il sito Oracle Accessibility Program all'indirizzo: http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso il portale Oracle My Oracle Support. Per tutte le necessarie informazioni, si prega di visitare il sito http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oppure http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs per clienti non udenti.

Indice

Uso della presente documentazione

- **Panoramica**: fornisce informazioni sulla pianificazione, sulla configurazione e sulla gestione di un ambiente sicuro per i sistemi Oracle SuperCluster serie M7.
- **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/sc-m7/docs.

Commenti

Inviare i commenti sulla presente documentazione all'indirizzo http://www.oracle.com/goto/docfeedback.

Informazioni sui principi di sicurezza

Nella presente guida vengono fornire informazioni sulla pianificazione, sulla configurazione e sulla gestione di un ambiente sicuro per i sistemi Oracle SuperCluster serie M7.

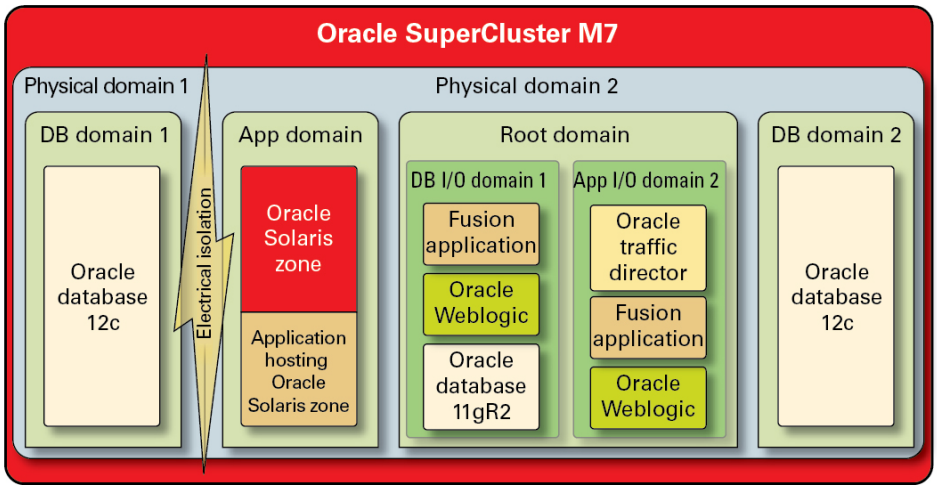
In questa sezione vengono trattati i seguenti argomenti:

Isolamento sicuro

SuperCluster M7 supporta varie strategie di isolamento che i provider di servizi cloud possono selezionare in base alle proprie esigenze di sicurezza. Questa flessibilità consente ai provider di servizi cloud di creare un'architettura multi-tenant personalizzata e sicura, adatta alle loro aziende.

SuperCluster M7 supporta varie strategie di isolamento del carico di lavoro, ciascuna con un set di funzionalità univoche. Sebbene ciascuna strategia di implementazione possa essere utilizzata in modo indipendente, è possibile anche utilizzare le varie strategie insieme in un approccio ibrido per consentire ai provider di servizi cloud di distribuire le architetture che possono bilanciare in modo più efficace le esigenze di sicurezza, di prestazioni, di disponibilità e così via.

FIGURA 1 Isolamento sicuro con una configurazione dinamica dei tenant



I provider di servizi cloud possono utilizzare i domini fisici (denominati anche PDomain) quando sugli host tenant vengono eseguiti applicazioni e database che devono essere isolati fisicamente da altri carichi di lavoro. Per una distribuzione potrebbero essere necessarie risorse fisiche dedicate a causa della criticità che tale distribuzione riveste per l'organizzazione, del livello di riservatezza delle informazioni in essa contenute, dei requisiti di conformità o semplicemente perché il carico di lavoro del database o dell'applicazione utilizza tutte le risorse di un intero sistema fisico.

Per le organizzazioni che richiedono l'isolamento mediato dagli hypervisor, vengono utilizzati i domini Oracle VM Server for SPARC, definiti domini dedicati, per creare ambienti virtuali che isolano le istanze dell'applicazione e/o del database. Su ciascun dominio dedicato, creato durante l'installazione di SuperCluster, viene eseguita un'istanza univoca del sistema operativo Oracle Solaris. L'accesso alle risorse fisiche viene mediato dagli hypervisor assistiti dall'hardware incorporati nei processori SPARC.

Inoltre, SuperCluster consente di creare domini aggiuntivi, definiti domini radice, che utilizzano la tecnologia SR-IOV (Single Root I/O Virtualization). I domini radice dispongono di uno o due HCA IB e NIC da 10 GbE. È possibile scegliere di creare in modo dinamico domini aggiuntivi, definiti domini di I/O, all'inizio dei domini radice. SuperCluster M7 include uno strumento basato sul browser per creare e gestire questi domini.

All'interno di ciascuno di questi domini, i tenant del cliente del cloud possono, tuttavia, utilizzare la tecnologia Oracle Solaris Zones per creare ambienti isolati aggiuntivi. Utilizzando

le zone è possibile distribuire singole istanze di applicazioni o di database oppure gruppi di questo tipo di istanze in uno o più contenitori virtualizzati che vengono eseguiti collettivamente su un singolo kernel del sistema operativo. Questo semplice approccio alla virtualizzazione viene utilizzato per creare un limite di sicurezza più potente per i servizi distribuiti.

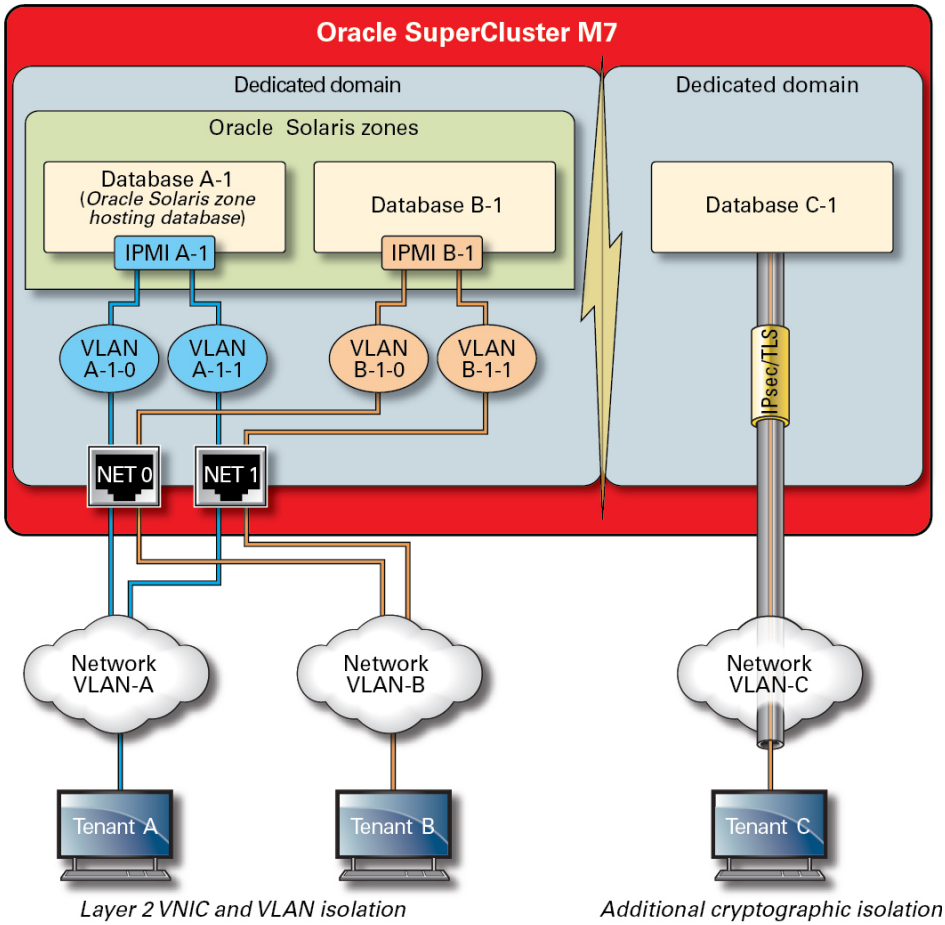
I tenant che ospitano più applicazioni e database su SuperCluster possono anche scegliere di utilizzare un approccio ibrido, che prevede una combinazione di strategie di isolamento basate su Oracle Solaris Zones, sui domini di I/O e sui domini dedicati per creare architetture flessibili ma resilienti che soddisfano le esigenze dell'infrastruttura del cloud in uso. Grazie a una serie di opzioni di virtualizzazione, SuperCluster consente l'isolamento sicuro dei tenant ospitati su cloud a livello di hardware e fornisce la tecnologia Oracle Solaris Zones per garantire un livello avanzato di sicurezza e un maggiore isolamento negli ambienti runtime.

Assicurare l'isolamento corretto delle singole applicazioni e dei singoli database, utenti e processi sui rispettivi sistemi operativi degli host è un ottimo punto di partenza. Tuttavia, è allo stesso modo importante considerare le tre reti principali utilizzate nel sistema SuperCluster e il modo in cui vengono protette le funzionalità di isolamento della rete e le comunicazioni che si verificano sulla rete:

- Rete di accesso ai client da 10 GbE
- Rete di servizio IB privata
- Rete di gestione

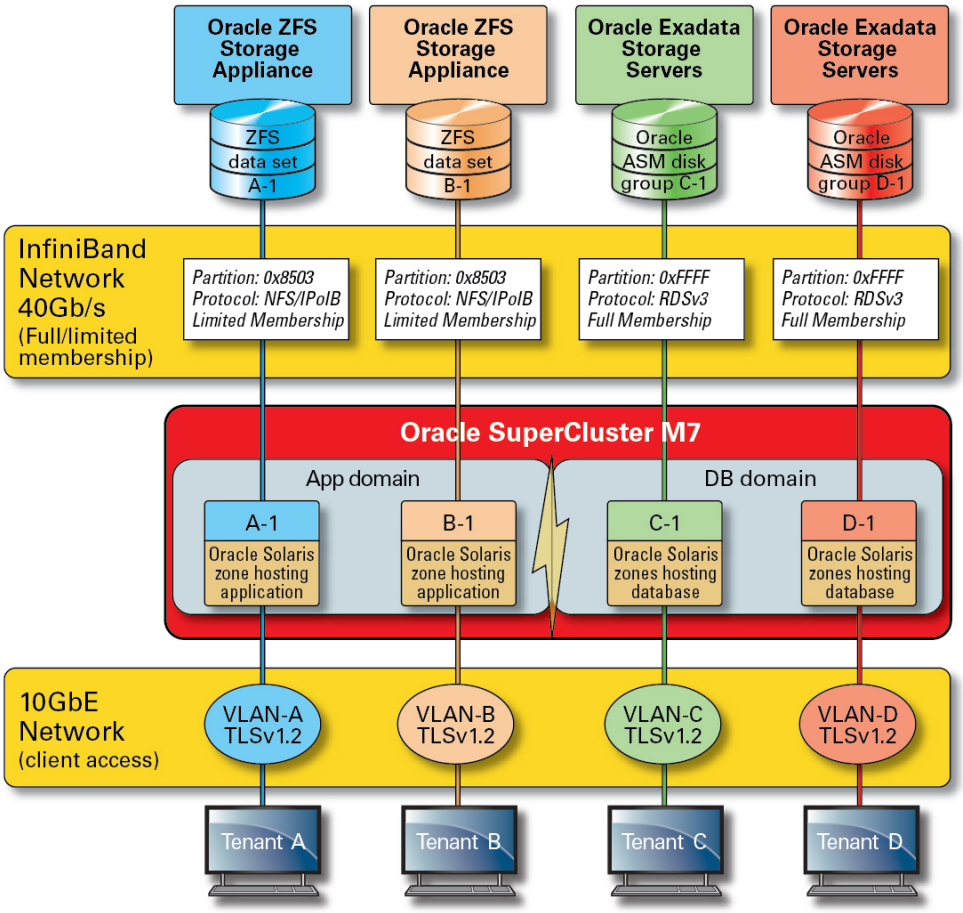
È possibile utilizzare varie tecniche per isolare il traffico sulla rete di accesso al client SuperCluster. In questa figura viene illustrata una possibile configurazione che prevede l'utilizzo di quattro istanze del database su tre LAN virtuali (VLAN) separate. La configurazione delle interfacce di rete di SuperCluster per l'uso delle reti VLAN consente di isolare il traffico di rete tra i domini dedicati di Oracle VM Server for SPARC e Oracle Solaris Zones.

FIGURA 2 Isolamento di rete sicuro sulla rete di accesso ai client



SuperCluster include una rete IB privata utilizzata dalle istanze di database per accedere alle informazioni memorizzate sugli Exadata Storage Server e su ZFS Storage Appliance nonché per stabilire le comunicazioni iniziali necessarie per il clustering e l'alta disponibilità. Questa figura illustra l'isolamento di rete sicuro su SuperCluster M7.

FIGURA 3 Isolamento di rete sicuro sulla rete IB da 40 GB/sec



Per impostazione predefinita, la rete IB di SuperCluster viene suddivisa in sei partizioni distinte durante l'installazione e la configurazione. Sebbene non sia possibile modificare le partizioni predefinite, Oracle supporta la creazione e l'uso di partizioni dedicate aggiuntive nei casi in cui è richiesta un'ulteriore segmentazione della rete IB. Inoltre, la rete IB supporta il concetto di appartenenza limitata o completa delle partizioni. I membri limitati possono comunicare solo con i membri completi, mentre questi ultimi possono comunicare con tutti i nodi sulla partizione. È possibile configurare i domini di I/O dell'applicazione e le zone di Oracle Solaris 11 come membri limitati delle rispettive partizioni IB, garantendo in tale modo che possano comunicare solo con il componente ZFS Storage Appliance, configurato come

membro completo, e non con altri nodi con appartenenza limitata che potrebbero esistere sulla stessa partizione.

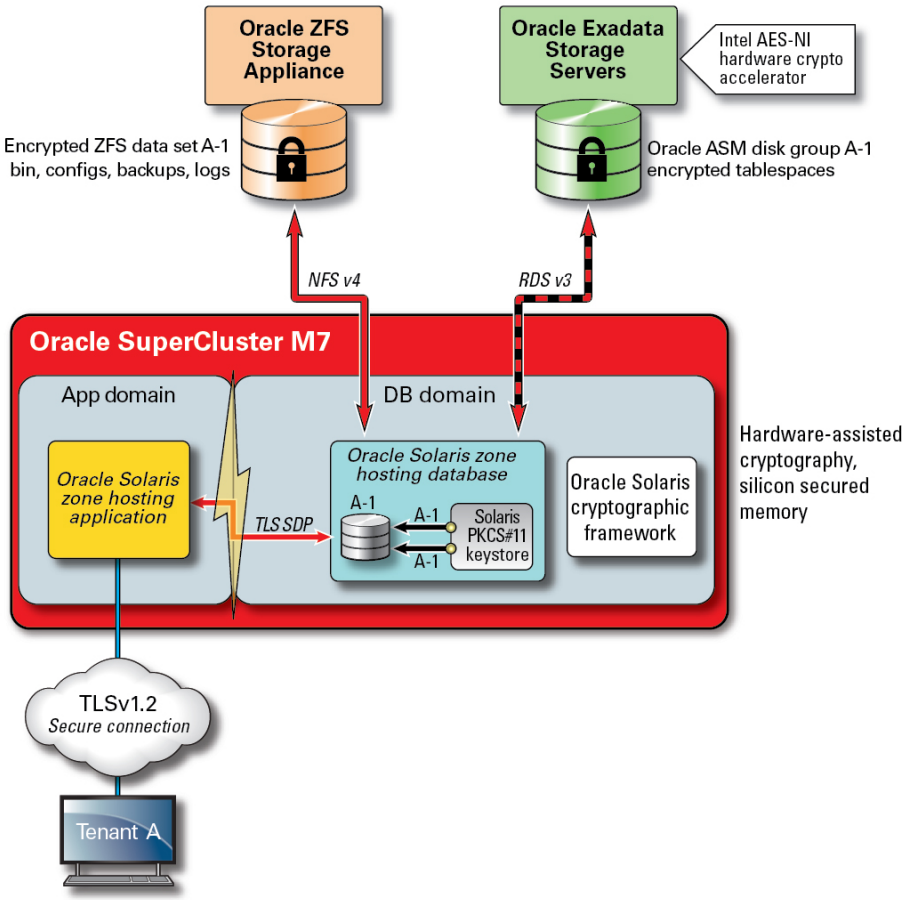
SuperCluster include inoltre una rete di gestione dedicata attraverso la quale è possibile gestire e monitorare i relativi componenti principali. Grazie a questa strategia, le importanti funzioni di gestione e monitoraggio rimangono isolate dai percorsi di rete utilizzati per elaborare le richieste dei client. Mantenendo queste funzioni isolate e accessibili solo da questa rete di gestione, SuperCluster può ridurre ulteriormente l'esposizione della rete agli attacchi provenienti dalle reti IB e di accesso ai client. Si consiglia ai provider di servizi cloud di seguire questa procedura consigliata e di isolare le funzioni di gestione e di monitoraggio nonché le funzioni correlate in modo che siano accessibili solo dalla rete di gestione.

Protezione dei dati

La protezione dei dati rappresenta l'elemento fondamentale della strategia di sicurezza dei provider di servizi cloud. Vista l'importanza dei requisiti di riservatezza e di conformità, le organizzazioni che prendono in considerazione architetture multi-tenant devono valutare la possibilità di utilizzare la cifratura per proteggere le informazioni inviate e ricevute dai database. L'uso dei servizi di cifratura per la protezione dei dati viene applicata in modo sistematico per assicurare la riservatezza e l'integrità delle informazioni trasmesse sulla rete e memorizzate sul disco.

Il processore SPARC M7 incluso in SuperCluster facilita la cifratura assistita dall'hardware, ad alte prestazioni per la protezione dei dati negli ambienti IT che rivolgono particolare attenzione alla sicurezza. Il processore SPARC M7 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.

FIGURA 4 Protezione dei dati fornita dall'accelerazione crittografica assistita dall'hardware e protezione della memoria dalle intrusioni



Per le architetture multi-tenant sicure, in cui la protezione dei dati riguarda quasi tutti gli aspetti dell'architettura, SuperCluster e il software di supporto consente alle organizzazioni di soddisfare i propri obiettivi di sicurezza e conformità senza dover rinunciare alle prestazioni. SuperCluster utilizza istruzioni di cifratura basate sulla memoria e le funzionalità Silicon Secured Memory incorporate nel processore SPARC M7 per accelerare le operazioni di cifratura e assicurare la protezione della memoria dalle intrusioni senza influire sulle prestazioni. Queste funzionalità migliorano le prestazioni di cifratura e forniscono il controllo

delle intrusioni nella memoria, oltre a migliorare le prestazioni globali, poiché è possibile dedicare più risorse di calcolo ai carichi di lavoro dei tenant.

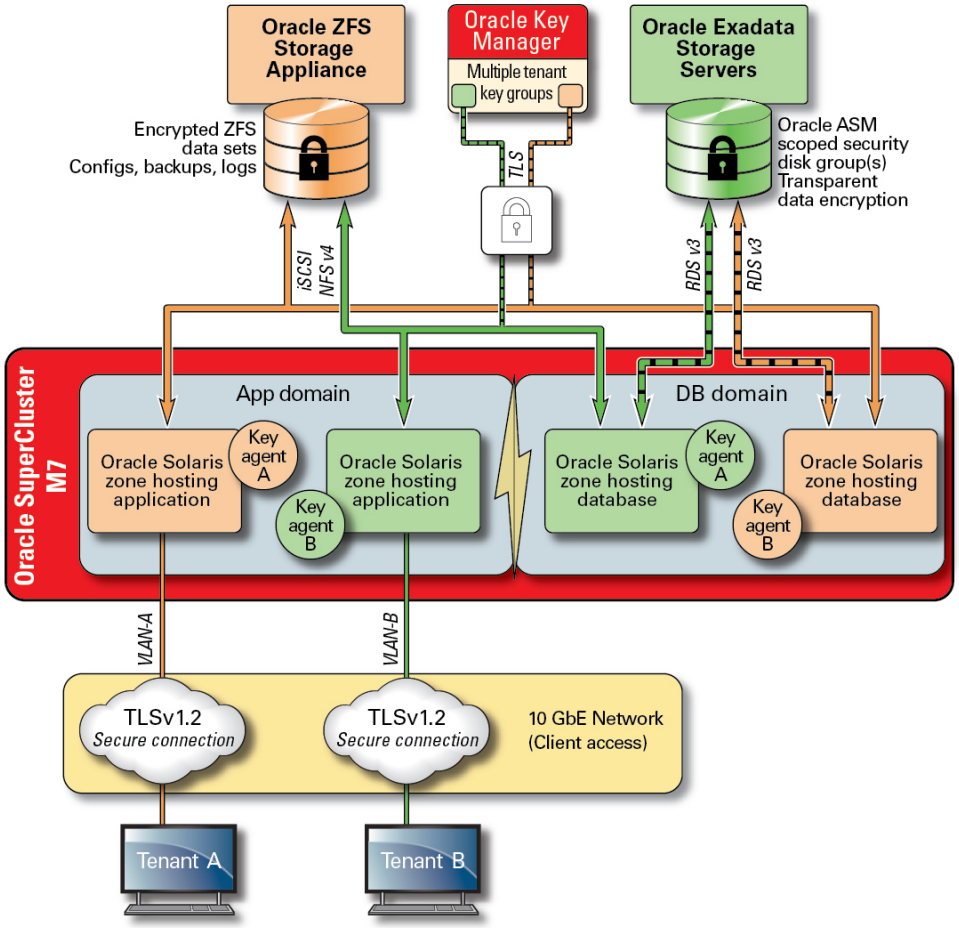
Il processore SPARC supporta l'accelerazione crittografica assistita dall'hardware per più di 16 algoritmi di cifratura standard del settore. Questi algoritmi supportano le esigenze di cifratura più moderne, quali la cifratura a chiave pubblica, la cifratura a chiave simmetrica, la generazione di numeri 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 SuperCluster. 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. Per proteggere la riservatezza e l'integrità delle comunicazioni specifiche dei tenant, interzona e basate su IP che si verificano sulla rete IB, utilizzare IPSec (IP Security) e IKE (Internet Key Exchange).

La descrizione delle modalità di gestione delle chiavi di cifratura è indispensabile per fornire informazioni complete sulla cifratura. La generazione e la gestione delle chiavi di cifratura, in particolare per molti servizi, hanno sempre rappresentato le principali sfide per le organizzazioni e tali sfide diventano sempre più impegnative nel caso di un ambiente multi-tenant basato sul cloud. In SuperCluster la cifratura dei set di dati ZFS e la cifratura dei dati trasparente di Oracle Database possono utilizzare un keystore PKCS#11 di Oracle Solaris per proteggere la chiave master. L'uso del keystore PKCS#11 di Oracle Solaris attiva automaticamente l'accelerazione crittografica assistita dall'hardware SPARC per qualsiasi operazione che utilizza la chiave master. Ciò consente a SuperCluster di migliorare in modo significativo le prestazioni relative alle operazioni di cifratura e decrifratura associate ai set di dati ZFS, alla cifratura delle tablespace di Oracle Database, ai backup dei database cifrati (mediante Oracle Recovery Manager [Oracle RMAN]), alle esportazioni dei database cifrati (mediante la funzione Data Pump di Oracle Database) e ai redo log (mediante Oracle Active Data Guard).

I tenant che utilizzano un approccio wallet condiviso possono utilizzare ZFS Storage Appliance per creare una directory che può essere condivisa in tutti i nodi di un cluster. L'uso di un keystore condiviso e centralizzato consente ai tenant di migliorare la gestione, la manutenzione e la rotazione delle chiavi nelle architetture di database in cluster, come ad esempio Oracle Real Application Clusters (Oracle RAC), poiché le chiavi verranno sincronizzate in ogni nodo del cluster.

FIGURA 5 Protezione dei dati in uno scenario di gestione delle chiavi multi-tenant mediante Oracle Key Manager



Per identificare le problematiche e le complessità della gestione delle chiavi associate a più host e applicazioni in un ambiente multi-tenant basato sul cloud, utilizzare il prodotto facoltativo Oracle Key Manager come appliance integrata nella rete di gestione. Oracle Key Manager autorizza, protegge e gestisce a livello centrale l'accesso alle chiavi di cifratura utilizzate da Oracle Database, dalle applicazioni Oracle Fusion, da Oracle Solaris e da ZFS Storage Appliance. Oracle Key Manager supporta anche le unità nastro per la cifratura StorageTek di Oracle. La possibilità di gestire i criteri e le chiavi di cifratura a livello di set di dati ZFS (file

system) consente di eliminare in modo sicuro i file system dei tenant tramite la distruzione delle chiavi.

Oracle Key Manager è un'appliance di gestione delle chiavi completa che supporta le operazioni di gestione delle chiavi e la memorizzazione delle chiavi sicure. Quando viene configurato con una scheda PCIe Sun Crypto Accelerator 6000 aggiuntiva fornita da Oracle, Oracle Key Manager fornisce la memorizzazione conforme alla certificazione FIPS 140-2 livello 3 delle chiavi di cifratura a 256 bit AES, nonché la generazione di numeri casuali conforme a FIPS 186-2. In SuperCluster è possibile configurare tutti i domini dei database e delle applicazioni, incluse le zone globali e le zone non globali, in modo da utilizzare Oracle Key Manager per gestire le chiavi associate ad applicazioni, database e set di dati ZFS cifrati. Infatti, Oracle Key Manager è in grado di supportare le operazioni di gestione delle chiavi associate a istanze di database singole o multiple, a Oracle RAC, a Oracle Active Data Guard, a Oracle RMAN e alla funzione Data Pump di Oracle Database.

Infine, la separazione dei compiti, applicata da Oracle Key Manager, consente a ciascun tenant di mantenere il controllo completo delle chiavi di cifratura e di avere una visibilità costante delle operazioni di gestione delle chiavi. Vista l'importanza delle chiavi per la protezione delle informazioni, è fondamentale che i tenant implementino i livelli necessari di audit e di controllo dell'accesso basato sui ruoli per garantire la protezione delle chiavi nell'intero ciclo di vita.

Informazioni correlate

- sezione chiamata «Oracle Key Manager» [130]

Controllo dell'accesso

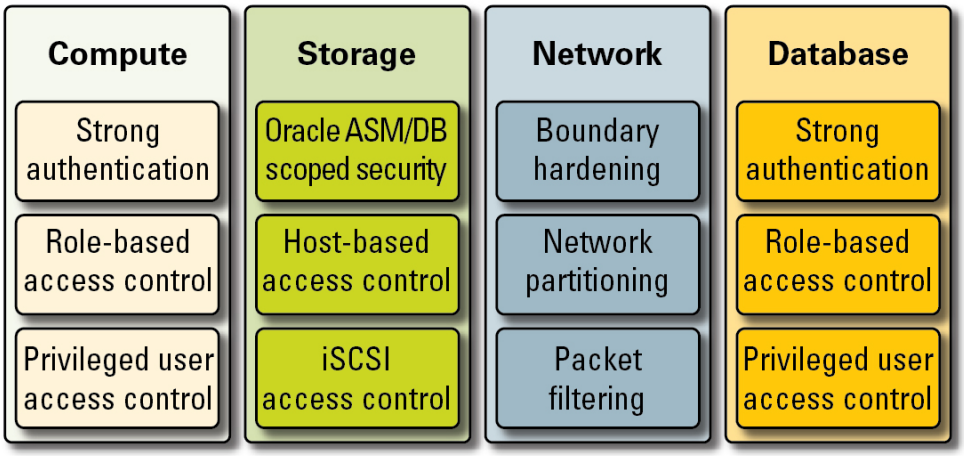
Per le organizzazioni che adottano una strategia basata su un ambiente ospitato su cloud, il controllo dell'accesso è uno dei problemi più importanti da risolvere. I tenant devono avere la certezza che le informazioni memorizzate nell'infrastruttura condivisa siano protette e disponibili solo agli host, ai servizi, agli utenti, ai gruppi e ai ruoli autorizzati. È necessario applicare ulteriori vincoli agli host, agli utenti e ai servizi autorizzati in conformità al principio di privilegio minimo, in base al quale gli host, gli utenti e i servizi devono disporre solo dei diritti e dei privilegi necessari per eseguire una determinata operazione.

SuperCluster semplifica un'architettura di controllo dell'accesso flessibile e strutturata che copre tutti i livelli dello stack e supporta vari ruoli, tra cui gli utenti finali, gli amministratori del database e gli amministratori di sistema. Ciò consente alle organizzazioni di definire i criteri per la protezione di host, applicazioni e database singoli e per proteggere l'infrastruttura di calcolo, di storage e di rete di base sulla quale vengono eseguiti i servizi.

Ai livelli di virtualizzazione e sistema operativo, il controllo dell'accesso inizia con la riduzione del numero di servizi esposti sulla rete. Ciò consente di controllare l'accesso alle console, ai domini e alle zone di Oracle VM Server for SPARC. Grazie alla riduzione del numero di punti di accesso utilizzabili dai sistemi, la quantità dei criteri di controllo dell'accesso può essere ridotta e conservata più facilmente per l'intero ciclo di vita del sistema.

Nel sistema operativo Oracle Solaris i controlli dell'accesso vengono implementati utilizzando una combinazione di autorizzazioni POSIX insieme alla funzione di controllo dell'accesso basato sui ruoli (RBAC) di Oracle Solaris. Molto importante è anche la possibilità di proteggere gli host, le applicazioni, i database e i servizi correlati in esecuzione su SuperCluster dagli attacchi basati sulla rete. A tale scopo, i tenant devono innanzitutto verificare che vengano eseguiti solo i servizi di rete autorizzati e che tali servizi ascoltino le connessioni di rete in entrata. Una volta ridotta al minimo l'esposizione della rete agli attacchi, i tenant configurano i servizi rimanenti in modo che ascoltino le connessioni in entrata solo sulle reti e sulle interfacce approvate. Questo semplice metodo garantirà che i protocolli di gestione, come Secure Shell, siano accessibili solo dalla rete di gestione.

FIGURA 6 Riepilogo del controllo dell'accesso end-to-end



I tenant possono anche scegliere di implementare un firewall basato su host, come il servizio IP Filter di Oracle Solaris. I firewall basati su host sono utili poiché forniscono agli host più funzioni per il controllo dell'accesso ai servizi di rete. Ad esempio, IP Filter supporta funzioni di filtro dei pacchetti con conservazione dello stato e consente di filtrare i pacchetti in base all'indirizzo IP, alla porta, al protocollo, all'interfaccia di rete e alla direzione del traffico.

Queste funzionalità sono importanti per le piattaforme come SuperCluster che utilizzano molte interfacce di rete e supportano una vasta gamma di comunicazioni di rete in entrata e in uscita.

Nel sistema SuperCluster è possibile configurare IP Filter all'interno di un dominio di Oracle VM Server for SPARC o attivarlo da una zona di Oracle Solaris. Ciò consente di applicare i criteri di controllo dell'accesso nello stesso contenitore del sistema operativo in cui vengono forniti i servizi del database. In uno scenario multi-tenant la quantità di attività di rete in uscita probabilmente sarà minima e può essere facilmente suddivisa in categorie, in modo da poter creare un criterio che limita le comunicazioni a specifiche interfacce di rete e destinazioni. Tutto il traffico rimanente verrà rifiutato e registrato in un criterio di "rifiuto predefinito" per bloccare le comunicazioni non autorizzate, sia in entrata che in uscita.

Oracle End User Security consente ai tenant di integrare le applicazioni e i database con i servizi di gestione delle identità esistenti in modo da supportare il Single Sign-On (SSO) e la gestione centralizzata degli utenti e dei ruoli. In modo specifico, Oracle End User Security consente di centralizzare (1) il provisioning e l'annullamento del provisioning degli utenti e degli amministratori del database, (2) la gestione delle password e la reimpostazione delle password self-service e (3) la gestione delle autorizzazioni utilizzando i ruoli di database globali. Le organizzazioni che richiedono i metodi di autenticazione multi-fattore, come Kerberos o PKI, possono utilizzare Oracle Advanced Security.

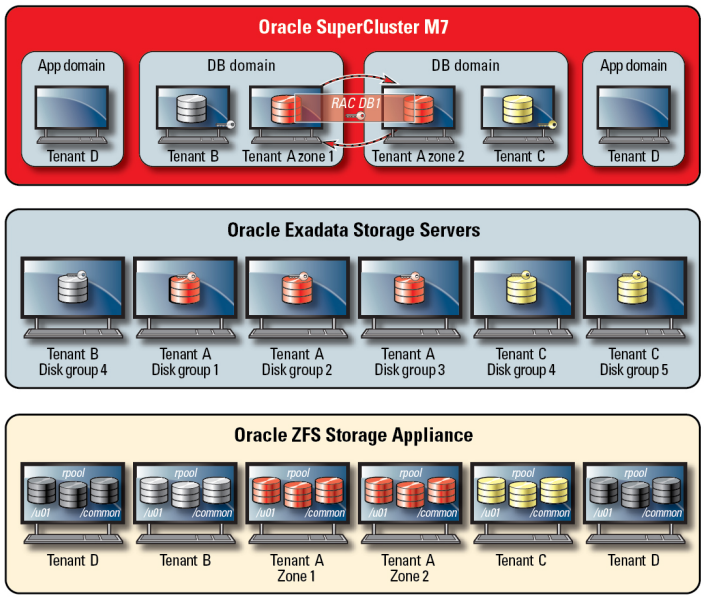
La tecnologia di Oracle Exadata Storage Server supporta un set predefinito di account utente, ciascuno con privilegi distinti. Gli amministratori che gestiscono Oracle Exadata Storage Server devono utilizzare uno di questi ruoli predefiniti per accedere al sistema. Dall'altra parte, ZFS Storage Appliance supporta la creazione di account amministrativi locali e remoti, entrambi in grado di supportare la singola assegnazione di ruoli e privilegi.

Per impostazione predefinita, i domini dei database accedono agli Oracle Exadata Storage Server utilizzati in SuperCluster utilizzando la funzione Oracle Automatic Storage Management. Questa funzione consente ai provider di servizi cloud di creare per ciascun tenant gruppi di dischi separati in grado di soddisfare i requisiti di capacità, prestazioni e disponibilità. Oracle Automatic Storage Management supporta tre modalità di controllo dell'accesso: sicurezza aperta, sicurezza con ambito Oracle Automatic Storage Management e sicurezza con ambito database.

In uno scenario multi-tenant, è consigliata la sicurezza con ambito database poiché offre il livello più capillare di controllo dell'accesso. Quando si utilizza questa modalità, è possibile configurare i gruppi di dischi in modo che solo un singolo database possa accedervi. In particolare, ciò significa che sia gli amministratori che gli utenti del database possono accedere solo ai dischi griglia contenenti informazioni per le quali dispongono dei privilegi di accesso. Negli scenari di consolidamento dei database in cui esiste la possibilità che i singoli database supportino organizzazioni e tenant differenti, è importante che ciascun tenant sia in grado di accedere e manipolare solo il proprio storage. In particolare, quando questo scenario è unito alle strategie di isolamento del carico di lavoro e dei database descritte in precedenza, è possibile impostare per i tenant una suddivisione efficace dell'accesso ai singoli database.

La sicurezza con ambito database è uno strumento efficace per limitare l'accesso ai dischi griglia di Oracle ASM. In questa figura vengono illustrate le strategie di sicurezza con ambito Oracle ASM e di sicurezza ZFS. Nei casi in cui esiste un numero elevato di istanze di Oracle Database da distribuire sulla piattaforma SuperCluster, una strategia di sicurezza con ambito Oracle ASM per ciascun tenant risulta più appropriata poiché riduce notevolmente il numero di chiavi da creare, assegnare e gestire. Inoltre, poiché la strategia di sicurezza con ambito database richiede la creazione di gruppi di dischi separati per ciascun database, questo approccio ridurrà in modo significativo anche il numero di dischi griglia distinti da creare su un Exadata Storage Server.

FIGURA 7 Sicurezza con ambito Oracle ASM per ciascun tenant



SuperCluster utilizza la protezione dei collegamenti dati di Oracle Solaris per prevenire i possibili danni che possono essere causati da computer virtuali tenant non autorizzati sulla rete. Questa funzione integrata di Oracle Solaris fornisce protezione contro le seguenti minacce di base: spoofing di indirizzi IP e MAC e spoofing di frame L2, ad esempio attacchi BPDU (Bridge Protocol Data Unit). La protezione dei collegamenti dati di Oracle Solaris deve essere applicata a tutte le singole zone non globali di Oracle Solaris distribuite all'interno dell'ambiente multi-tenant.

Poiché i singoli tenant non devono mai richiedere l'accesso a livello amministrativo o di host agli Exadata Storage Server, si consiglia di limitare questo tipo di accesso. È necessario configurare gli Exadata Storage Server in modo da impedire l'accesso diretto alle zone non globali dei tenant e ai domini di I/O dei database e consentire, al contempo, l'accesso ai domini di database SuperCluster che vengono attivati dal provider di servizi cloud. Ciò consente di gestire gli Exadata Storage Server solo da posizioni affidabili sulla rete di ricerca.

Una volta definita e implementata la configurazione di sicurezza dei tenant, i provider di servizi possono considerare la possibilità di effettuare un'ulteriore operazione di configurazione, ovvero impostare le zone globali e non globali specifiche dei tenant come immutabili (ambienti di sola lettura). Le zone immutabili creano un ambiente operativo resiliente, ad alta integrità all'interno del quale i tenant possono utilizzare i propri servizi. Grazie alle funzionalità di sicurezza integrate di Oracle Solaris, le zone immutabili impediscono la modifica di tutti i file e di tutte le directory del sistema operativo o parte di essi senza l'intervento del provider di servizi cloud. L'applicazione di questo metodo di sola lettura impedisce di apportare modifiche non autorizzate, promuove procedure più potenti di gestione delle modifiche e impedisce l'introduzione di malware basati sia sul kernel e che sull'utente.

Monitoraggio e controllo della conformità

In un ambiente cloud le operazioni di monitoraggio e registrazione proattive sono molto importanti e, in molti casi, consentono di ridurre gli attacchi causati da falle e vulnerabilità nel sistema di sicurezza. Il monitoraggio e il controllo sia delle attività di generazione di rapporti di conformità che di risposta agli incidenti sono critiche per il provider del cloud e le organizzazioni dei tenant devono applicare criteri di registrazione e di controllo ben definiti per ottenere una maggiore visibilità nei propri ambienti di hosting. Il livello di utilizzo delle operazioni di monitoraggio e di controllo si basa spesso sul rischio o sulla criticità dell'ambiente da proteggere.

L'architettura cloud di SuperCluster si basa sull'uso del sottosistema di controllo di Oracle Solaris per raccogliere, memorizzare ed elaborare le informazioni degli eventi di controllo. Ciascuna zona non globale specifica del tenant genererà record di controllo memorizzati a livello locale in ciascun dominio dedicato di SuperCluster (zona globale). Questo approccio impedisce ai singoli tenant 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, il richiamo dei comandi e anche le singole chiamate del sistema a livello di kernel sia nelle zone che nei domini dei tenant. Questa funzionalità è altamente configurabile e offre criteri di audit globali, per zona e anche per utente. Quando vengono configurati per utilizzare le zone dei tenant, i record di controllo di ciascuna zona possono essere memorizzati nella zona globale in modo da proteggerli da manomissioni. I domini dedicati e quelli di I/O utilizzano anche la funzione di controllo nativa

di Oracle Solaris per registrare le azioni e gli eventi associati agli eventi di virtualizzazione e di amministrazione dei domini.

Exadata Storage Server e ZFS Storage Appliance supportano il controllo dei login, dell'hardware e della configurazione. Ciò consente alle organizzazioni di determinare chi ha avuto accesso a un dispositivo e quali azioni sono state intraprese. Sebbene non sia esposta direttamente all'utente finale, la funzione di controllo di Oracle Solaris fornisce il contenuto di base per le informazioni visualizzate da ZFS Storage Appliance.

Analogamente, la funzione di controllo di Exadata Storage Server è un insieme esteso di eventi di sistema che possono essere utilizzati insieme alle informazioni sugli avvisi hardware e di configurazione fornite dal software Exadata Storage Server. Grazie alla funzionalità IP Filter di Oracle Solaris, il provider del cloud può registrare in modo selettivo le comunicazioni di rete sia in entrata che in uscita e tale funzionalità può essere applicata sia a livello di dominio che a livello di zone non globali. Ciò consente alle organizzazioni di suddividere i criteri di rete e verificare i record di attività. Oracle Audit Vault e l'appliance Database Firewall possono essere distribuite facoltativamente per aggregare e analizzare in modo sicuro le informazioni di audit provenienti da molti database Oracle e non Oracle nonché le informazioni di audit provenienti da Oracle Solaris.

Grazie all'integrazione con Oracle Enterprise Manager, SuperCluster è in grado di supportare una vasta gamma di operazioni self-service per il cloud. I provider del cloud possono definire pool di risorse, assegnare pool e quote ai singoli tenant, identificare e pubblicare cataloghi di servizi e infine supportare il monitoraggio e la registrazione delle risorse dell'applicazione e del database.

Informazioni correlate

- Audit della conformità [123]
- sezione chiamata «Monitoraggio della sicurezza» [133]

Risorse aggiuntive per le procedure consigliate sulla sicurezza di SuperCluster

Per ulteriori informazioni sulla sicurezza, sull'architettura e sulle procedure ottimali di SuperCluster, consultare le seguenti risorse:

- Oracle SuperCluster M7 - Platform Security Principles and Capabilities

  `http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf`

- Oracle SuperCluster M7 - Secure Private Cloud Architecture

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Comprehensive Data Protection on Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Secure Database Consolidation on Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster and PCI Compliance

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - Security Technical Implementation Guide (STIG) Validation and Best Practices

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Developer's Guide to Oracle Solaris 11 Security

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 and PCI Compliance

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 Audit Quick Start

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Oracle Solaris 11 Security Guidelines

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database Security Guide 12c Release 1 (12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

Revisione della configurazione di sicurezza predefinita

In questi argomenti viene descritta la configurazione di sicurezza predefinita per SuperCluster M7.

Impostazioni di sicurezza predefinite

Il software di SuperCluster M7 viene installato con diverse impostazioni di sicurezza predefinite. Quando possibile, usare le impostazioni di sicurezza predefinite.

- I criteri delle password applicano una complessità minima per le password.
- I tentativi di login non riusciti provocano l'attivazione del blocco dopo un determinato numero di tentativi non riusciti.
- Tutti gli account di sistema predefiniti presenti nel sistema operativo vengono bloccati e viene loro impedito di eseguire il login.
- Viene configurata la possibilità limitata di utilizzo del comando `su`.
- I protocolli e i moduli non necessari vengono disabilitati dal kernel del sistema operativo.
- Il boot loader viene protetto da password.
- Tutti i servizi di sistema non necessari vengono disabilitati, incluso `inetd` (daemon dei servizi Internet).
- Il firewall del software viene configurato nelle celle di storage.
- Autorizzazioni di file restrittive vengono impostate per i file chiave di configurazione ed eseguibili correlati alla sicurezza.
- Le porte di ascolto SSH vengono limitate alle reti di gestione e privata.

- SSH viene limitato al protocollo v2.
- I meccanismi di autenticazione SSH non sicuri vengono disabilitati.
- Vengono configurate cifrature di crittografia specifiche.
- Nel sistema gli switch vengono separati dal traffico dati nella rete.

Account utente e password predefiniti

Nella tabella sono elencati gli account utente predefiniti e le password predefinite per SuperCluster M7. Ulteriori istruzioni sulla modifica delle password predefinite vengono fornite nei capitoli successivi relativi a ciascun componente.

Componente	Nome utente	Password	Informazioni su account utente e password
Oracle ILOM su: ■ Server SPARC serie M7 ■ Exadata Storage Server ■ ZFS Storage Appliance	■ `root`	`welcome1`	Consultare “Configuration and Maintenance” nella raccolta delle documentazione di Oracle ILOM all'indirizzo: `http://docs.oracle.com/cd/E24707_01/html/E24528`
Server SPARC serie M7	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55]. inoltre, fare riferimento alle seguenti risorse: ■ **Oracle Solaris 11**: consultare la documentazione sulla sicurezza per Oracle Solaris 11 all'indirizzo: `http://www.oracle.com/goto/Solaris11/docs` ■ **Oracle Solaris 10**: consultare il documento *Oracle Solaris Administration: Basic Administration* all'indirizzo: `http://docs.oracle.com/cd/E26505_01`

Exadata Storage Server	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			Vedere Modifica delle password degli storage server [96].

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	Vedere Modificare la password `root` di ZFS Storage Appliance [85]. Inoltre, consultare la sezione “Users” nel documento *Oracle ZFS Storage Appliance Administration Guide* all'indirizzo: `http://www.oracle.com/goto/ZS3-ES/docs`
Switch InfiniBand	■ `root` ■ `nm2user`	`welcome1` changeme	Vedere Modificare le password `root` e `nm2user` [113].

Componente	Nome utente	Password	Informazioni su account utente e password
			Inoltre, consultare “Controlling the Chassis” nel documento *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* all'indirizzo: `http://docs.oracle.com/cd/E36265_01`
InfiniBand Oracle ILOM	■ `ilom-admin` ■ `ilom-operator`	ilom-admin ilom-operator	Vedere Modificare le password degli switch IB (Oracle ILOM) [114]. Inoltre, consultare la documentazione di InfiniBand all'indirizzo: `http://docs.oracle.com/cd/E36265_01`
Switch di gestione Ethernet	■ `admin`	`welcome1`	Vedere Modificare la password dello switch Ethernet [121]
Strumento Oracle I/O Domain Creation	■ `admin`	welcome1	Consultare il documento *Oracle I/O Domain Administration Guide* disponibile all'indirizzo: `http://www.oracle.com/goto/sc-m7/docs`.
Oracle Engineered Systems Hardware Manager	■ `admin` ■ service	welcome1 welcome1	Consultare il documento *Oracle SuperCluster M7 Series Owner's Guide: Administration* disponibile all'indirizzo: `http://www.oracle.com/goto/sc-m7/docs`.

Nota - Quando si modifica la password `root` o `admin` di questo componente, è necessario modificarla anche in Oracle Engineered Systems Hardware Manager. Per le istruzioni, consultare il documento *Oracle SuperCluster M7 Series Owner's Guide: Administration*. Vedere anche sezione chiamata «Password conosciute da Oracle Engineered Systems Hardware Manager» [31]

Password conosciute da Oracle Engineered Systems Hardware Manager

È necessario configurare Oracle Engineered Systems Hardware Manager con gli account e le password dei componenti elencati nella tabella riportata di seguito.

Nota - Non è necessario che Oracle Engineered Systems Hardware Manager conosca le password dei domini logici o delle zone.

Componente	Account
Tutti gli Oracle ILOM	`root`

Componente	Account
Sistema operativo degli Exadata Storage Server	`root`
Sistema operativo dei controller di storage ZFS	`root`
Switch IB	`root`
Switch di gestione Ethernet	`admin`
PDU	`admin`

Per ulteriori informazioni su Oracle Engineered Systems Hardware Manager, vedere sezione chiamata «Oracle Engineered Systems Hardware Manager» [131] e consultare il documento *Guida all'amministrazione di Oracle SuperCluster serie M7* all'indirizzo `http://www.oracle.com/goto/sc-m7/docs`.

Protezione dell'hardware

In queste sezioni vengono descritte le linee guida relative alla sicurezza dell'hardware.

Limitazioni di accesso

- Installare i sistemi della serie Oracle SuperCluster M7 e le apparecchiature correlate in una stanza chiusa e con accesso limitato.
- Bloccare gli sportelli del rack a meno che i componenti all'interno del rack non debbano essere riparati. In questo modo, si limita l'accesso ai dispositivi hot plug o hot swap, alle porte USB, alle porte di rete e alla console di sistema.
- 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 a tale armadio 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. La limitazione dell'accesso fisico è il metodo di accesso a un componente più sicuro, in quanto non è soggetto ad attacchi che sfruttano la rete.

Numeri di serie

- Registrare i numeri di serie dei componenti dei sistemi della serie SuperCluster M7.
- 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 i record delle chiavi di attivazione dell'hardware e delle licenze in un luogo sicuro che possa essere raggiunto con facilità dal responsabile del sistema in caso di emergenza. I documenti stampati potrebbero essere l'unica prova di proprietà.
- Conservare tutti i fogli informativi forniti con il sistema in un luogo sicuro.

Unità

Le unità disco rigido e le unità SSD (Solid State Drive) vengono spesso utilizzate per memorizzare informazioni riservate. Per proteggere queste informazioni dalla diffusione non autorizzata, è necessario ripulire le unità prima di riutilizzarle, dismetterle o disfarsene.

- Utilizzare gli strumenti di cancellazione del disco, come il comando Oracle Solaris `format(1M)` per cancellare completamente tutti i dati dall'unità.
- 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 rigido.
- Se necessario, usufruire del servizio di conservazione dei dispositivi e dei dati del cliente di Oracle. Fare riferimento al documento: `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Attenzione - Gli strumenti di cancellazione del disco potrebbero non essere in grado di eliminare alcuni dati contenuti nelle unità più recenti, a causa delle modalità di gestione dell'accesso ai dati che le contraddistingue.

OBP

Per impostazione predefinita, il firmware OBP della serie SPARC M7 non è protetto da password. Per aumentare il livello di sicurezza del sistema, è possibile limitare l'accesso all'OBP effettuando le operazioni riportate di seguito.

- Implementare la protezione mediante password.
- Controllare l'eventuale presenta di login all'OBP non riusciti.
- Specificare un banner di accensione OBP.

Risorse hardware aggiuntive

Tutti i principi di sicurezza descritti nella *Guida per la sicurezza dei server SPARC M7 Series* sono validi per i server SPARC M7 nel sistema SuperCluster. La guida per la sicurezza è disponibile all'indirizzo: http://www.oracle.com/goto/M7/docs

Protezione di Oracle ILOM

Oracle ILOM fornisce il software e l'hardware del processore di servizio avanzato utilizzato per gestire e monitorare i componenti di Oracle SuperCluster, inclusi server di calcolo, storage server, ZFS Storage Appliance e switch IB.

Oracle ILOM consente di gestire e monitorare in modo attivo i server e i dispositivi di base indipendentemente dallo stato del sistema operativo, offrendo funzionalità di gestione remota affidabili.

Per garantire la protezione completa di Oracle ILOM su SuperCluster M7, è necessario applicare le impostazioni di configurazione a tutti i singoli componenti abilitati per Oracle ILOM. Oracle ILOM è disponibile nei seguenti componenti:

- Server di calcolo
- Storage server
- ZFS storage appliance
- Switch IB

Per proteggere Oracle ILOM, eseguire le procedure descritte di seguito.

▼ Eseguire il login all'interfaccia CLI di Oracle ILOM

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

In questo esempio, sostituire *ILOM_SP_ipaddress* con l'indirizzo IP di Oracle ILOM per il componente a cui si desidera accedere:

- Server di calcolo
- Storage server
- ZFS storage appliance
- Switch IB

Gli indirizzi IP per la configurazione in uso sono elencati nel Riepilogo di distribuzione fornito dal personale Oracle.

```
% ssh root@ILOM_SP__ipaddress
```

2. **Immettere la password root di Oracle ILOM.**

   Vedere sezione chiamata «Account e password predefiniti (Oracle ILOM)» [40].

▼ Determinare la versione di Oracle ILOM

Per utilizzare le funzioni, le funzionalità e i miglioramenti della sicurezza più recenti, aggiornare il software Oracle ILOM con la versione più recente supportata.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Visualizzare la versione di Oracle ILOM.**

   In questo esempio, la versione del software Oracle ILOM è la 3.2.4.1.b.

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

Nota - Per aggiornare la versione di Oracle ILOM su un componente di SuperCluster, installare la versione più recente di SuperCluster Quarterly Full Stack Download Patch disponibile in My Oracle Support all'indirizzo `https://support.oracle.com`.

Nota - I sistemi di decodifica Oracle, come ad esempio SuperCluster, prevedono limitazioni per le versioni di Oracle ILOM utilizzabili e per le modalità di aggiornamento di tali versioni. Per ulteriori dettagli, contattare il rappresentante Oracle.

(Se richiesto) Abilitare il 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 funziona se si utilizza la crittografia convalidata in base a FIPS 140. Tuttavia, è 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. Per un elenco di queste funzionalità, consultare la sezione relativa alle funzioni non supportate quando la modalità FIPS è abilitata della *Guida sulla sicurezza di Oracle ILOM* (vedere sezione chiamata «Risorse aggiuntive per Oracle ILOM» [52]).

Vedere anche sezione chiamata «Conformità a FIPS-140-2, Livello 1» [126].

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, queste modifiche alla configurazione andranno perse.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

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
```

Account e password predefiniti (Oracle ILOM)

Account	Tipo	Password predefinita	Descrizione
`root`	amministratore	`welcome1`	Questo è l'account predefinito fornito e abilitato per questo componente. Questo account viene utilizzato per eseguire la configurazione iniziale e per consentire la creazione di ulteriori account amministrativi non condivisi. Per motivi di sicurezza, modificare la password predefinita.

Servizi di rete esposti predefiniti (Oracle ILOM)

In questa tabella vengono elencati i servizi di rete predefiniti esposti da Oracle ILOM.

Per ulteriori informazioni su questi servizi, consultare la *Guida sulla sicurezza di Oracle ILOM* (vedere sezione chiamata «Risorse aggiuntive per Oracle ILOM» [52]).

Nome servizio	Protocollo	Porta	Descrizione
SSH	TCP	22	Utilizzato dal servizio Secure Shell integrato per abilitare l'accesso amministrativo a Oracle ILOM utilizzando un'interfaccia CLI.
HTTP (BUI)	TCP	80	Utilizzato dal servizio HTTP integrato per abilitare l'accesso amministrativo a Oracle ILOM utilizzando un'interfaccia del browser. Sebbene TCP/80 venga in genere utilizzato per l'accesso con testo in chiaro, per impostazione predefinita Oracle ILOM reindirizza automaticamente le richieste in entrata alla versione sicura di questo servizio in esecuzione su TCP/443.
NTP	UDP	123	Utilizzato dal servizio NTP (Network Time Protocol) integrato (solo client) che consente di sincronizzare il clock di sistema locale con una o più origini temporali esterne.

Nome servizio	Protocollo	Porta	Descrizione
SNMP	UDP	161	Utilizzato dal servizio SNMP integrato per fornire un'interfaccia di gestione che consente di monitorare lo stato di Oracle ILOM e le notifiche trap ricevute.
HTTPS (BUI)	TCP	443	Utilizzato dal servizio HTTPS integrato per abilitare l'accesso amministrativo a Oracle ILOM su un canale (SSL/TLS) cifrato utilizzando un'interfaccia del browser.
IPMI	TCP	623	Utilizzato dal servizio IPMI (Intelligent Platform Management Interface) integrato per fornire un'interfaccia del computer per varie funzioni di monitoraggio e gestione. Questo servizio non deve essere disabilitato poiché viene utilizzato da Oracle Enterprise Manager Ops Center per raccogliere dati di inventario hardware, descrizioni delle FRU, informazioni sui sensori hardware e informazioni sullo stato dei componenti hardware.
KVMS remoto	TCP	5120 5121 5123 5555 5556 7578 7579	Le porte KVMS remote offrono un set di protocolli che fornisce tastiera, video, mouse e funzionalità di storage remote che possono essere utilizzate con Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	Utilizzato dal servizio Oracle ServiceTag. Si tratta di un protocollo di ricerca automatica di Oracle utilizzato per identificare i server e semplificare le richieste di servizio. Questo servizio viene utilizzato da prodotti quali Oracle Enterprise Manager Ops Center per trovare il software Oracle ILOM e per l'integrazione con altre soluzioni di servizio automatico Oracle.
WS-Man su HTTPS	TCP	8888	Utilizzato dal servizio WS-Man integrato per fornire un'interfaccia di servizi Web basata su standard utilizzata per gestire Oracle ILOM sul protocollo HTTPS. La disabilitazione di questo servizio impedisce la gestione di Oracle ILOM mediante questo protocollo. A partire dalla versione 3.2 di Oracle ILOM, questo servizio non è più presente.
WS-Man su HTTP	TCP	8889	Questa porta viene utilizzata dal servizio WS-Man integrato per fornire un'interfaccia di servizi Web basata su standard utilizzata per gestire Oracle ILOM sul protocollo HTTP. La disabilitazione di questo servizio impedirà la gestione di Oracle ILOM mediante questo protocollo. A partire dalla versione 3.2 di Oracle ILOM, questo servizio non è più presente.
Single Sign-On	TCP	11626	Questa porta viene utilizzata dalla funzionalità Single Sign-On che riduce il numero di tentativi di inserimento di nome utente e password da parte di un utente. La disabilitazione di questo servizio impedisce l'avvio di KVMS senza reimmettere una password.

Potenziamento della configurazione di sicurezza di Oracle ILOM

Negli argomenti riportati di seguito viene descritto come proteggere Oracle ILOM mediante varie impostazioni di configurazione.

▼ Disabilitare i servizi non necessari (Oracle ILOM)

Disabilitare i servizi non necessari per supportare i requisiti operativi e di gestione della piattaforma.

Per impostazione predefinita, Oracle ILOM include una configurazione di rete sicura predefinita, in cui i servizi non essenziali sono già disabilitati. Tuttavia, in base ai criteri e ai requisiti di sicurezza in uso potrebbe essere necessario disabilitare ulteriori servizi.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Determinare l'elenco dei servizi supportati da Oracle ILOM.**

   ```
   -> show /SP/services
   ```

3. **Determinare se uno specifico servizio è abilitato.**

   Sostituire *servicename* con il nome del servizio identificato nel Passo 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   La maggior parte dei servizi riconosce e utilizza il parametro `servicestate` per stabilire se il servizio è abilitato o disabilitato. Tuttavia, esistono alcuni servizi, come `servicetag`, `ssh`, `sso` e `wsman`, che utilizzano un parametro denominato `state`. Indipendentemente dal parametro effettivo utilizzato, un servizio è abilitato se il parametro `servicestate` o `state` restituisce il valore `enabled`, come illustrato negli esempi seguenti:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled

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

4. **Per disabilitare un servizio non più necessario, impostarne lo stato su `disabled`.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Determinare se uno di questi servizi deve essere disabilitato.**

   A seconda degli strumenti e dei metodi utilizzati, è possibile disabilitare questi servizi aggiuntivi se non sono necessari o non vengono utilizzati.

   - **Per un'interfaccia amministrativa del browser (HTTP, HTTPS), digitare:**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **For il servizio KVMS (tastiera, video, mouse), digitare:**

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **Per la gestione dei servizi Web (WS-Man su HTTP/HTTPS) - (Oracle ILOM versione 3.1 e precedenti), digitare:**:

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **Per i servizi SSO (Single Sign-On), digitare:**

     ```
     -> set /SP/services/sso state=disabled
     ```

▼ Configurare il reindirizzamento HTTP a HTTPS (Oracle ILOM)

Per impostazione predefinita, Oracle ILOM è configurato per reindirizzare le richieste HTTP in entrata al servizio HTTPS in modo da garantire che tutte le comunicazioni basate su browser tra Oracle ILOM e l'amministratore siano cifrate.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Verificare che il reindirizzamento sicuro sia abilitato.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Se l'impostazione predefinita è stata modificata, è possibile abilitare il reindirizzamento sicuro.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

Disabilitare i protocolli non approvati

Consultare gli argomenti riportati di seguito per disabilitare i protocolli non approvati:

- Disabilitare il protocollo SSLv2 per HTTPS [44]
- Disabilitare il protocollo SSLv3 per HTTPS [45]

▼ Disabilitare il protocollo SSLv2 per HTTPS

Per impostazione predefinita, il protocollo SSLv2 è disabilitato per il servizio HTTPS.

Per motivi di sicurezza, è molto importante che SSLv2 sia disabilitato.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Determinare se il protocollo SSLv2 è disabilitato per il servizio HTTP.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **Se il servizio è abilitato, disabilitare il protocollo SSLv2.**

```
-> set /SP/services/https sslv2=disabled
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

▼ Disabilitare il protocollo SSLv3 per HTTPS

Per impostazione predefinita, il protocollo SSLv3 è abilitato per il servizio HTTPS.

Per motivi di sicurezza, disabilitare il protocollo SSLv3.

1. **Sulla rete di gestione eseguire il login a Oracle ILOM.**
   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Determinare se il protocollo SSLv3 è disabilitato per il servizio HTTP.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **Disabilitare il protocollo SSLv3.**

```
-> set /SP/services/https sslv3=disabled
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

▼ Disabilitare i protocolli TLS non approvati per HTTPS

Per impostazione predefinita, i protocolli TLSv1.0, TLSv1.1 e TLSv1.2 sono abilitati per il servizio HTTPS.

È possibile disabilitare una o più versioni del protocollo TLS non conformi ai criteri di sicurezza in uso.

Per motivi di sicurezza, utilizzare TLSv1.2 a meno che non sia richiesto il supporto per le versioni meno recenti del protocollo TLS.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Determinare l'elenco delle versioni dei protocolli TLS abilitate per il servizio HTTPS.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **Disabilitare TLSv1.0.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **Disabilitare TLSv1.1.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **Verificare l'impostazione ripetendo il Passo 2.**

▼ Disabilitare le cifrature SSL con efficacia debole e media per HTTPS

Per impostazione predefinita, Oracle ILOM disabilita l'uso delle cifrature con efficacia debole e media per il servizio HTTPS.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Disabilitare se le cifrature con efficacia debole e media sono disabilitate.**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **Se l'impostazione predefinita è stata modificata, è possibile disabilitare le cifrature con efficacia debole e media.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

Disabilitare i protocolli SNMP non approvati (Oracle ILOM)

Per impostazione predefinita, solo il protocollo SNMPv3 è abilitato per il servizio SNMP utilizzato per monitorare e gestire Oracle ILOM. Assicurarsi che le versioni precedenti del protocollo SNMP rimangano disabilitate a meno che non venga richiesto.

Alcuni prodotti Oracle e di terze parti prevedono delle limitazioni relative al supporto delle versioni più recenti del protocollo SNMP. Per verificare se è previsto il supporto per versioni specifiche del protocollo SNMP, consultare la documentazione del prodotto associata a questi componenti. Assicurarsi che Oracle ILOM sia configurato per supportare qualsiasi versione del protocollo richiesta da questi componenti.

Nota - Nella versione 3 del protocollo SNMP è stato introdotto il supporto per il modello di sicurezza basato sull'utente (USM). Questa funzionalità sostituisce le stringhe community SNMP tradizionali con gli account utente effettivi che possono essere configurati con autorizzazioni, autenticazione, protocolli di riservatezza e password specifici. Per impostazione predefinita, Oracle ILOM non include account USM. Configurare gli account USM SNMPv3 in base ai requisiti personali di distribuzione, gestione e monitoraggio.

---

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Determinare lo stato di ciascun protocollo SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **Se necessario, disabilitare SNMPv1 e SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

Configurare le stringhe community SNMP v1 e v2c (Oracle ILOM)

Questa procedura è applicabile solo se SNMP v1 o SNMPv2c è abilitato e configurato per l'uso.

Per il corretto funzionamento di SNMP, è necessario che un client e un server accettino la stessa stringa community utilizzata per autenticare l'accesso. Pertanto, quando si modificano le stringhe community SNMP, assicurarsi che la nuova stringa sia configurata sia su Oracle ILOM che su tutti i componenti che tenteranno di connettersi a Oracle ILOM utilizzando il protocollo SNMP.

Poiché SNMP viene spesso utilizzato per monitorare lo stato del dispositivo, è importante che le stringhe community SNMP predefinite utilizzate dal dispositivo vengano sostituite con valori definiti dal cliente.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Creare una nuova stringa community SNMP.**

   In questo esempio, sostituire questi elementi nella riga di comando:

   - *string*: sostituire questo elemento con un valore definito dal cliente conforme ai requisiti stabiliti dal Dipartimento della Difesa degli Stati Uniti relativi alla composizione delle stringhe community SNMP.
   - *access*: sostituire questo elemento con `ro` o `rw`, a seconda che si tratti di una stringa di accesso di sola lettura o di lettura-scrittura.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Dopo aver creato nuove stringhe community, è necessario rimuovere quelle predefinite.

3. **Rimuovere le stringhe community SNMP predefinite.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **Verificare le stringhe community SNMP.**

   ```
   -> show /SP/services/snmp/communities
   ```

Sostituire i certificati autofirmati predefiniti (Oracle ILOM)

Oracle ILOM utilizza i certificati autofirmati per consentire l'uso immediato dei protocolli SSL e TLS. Quando possibile, sostituire i certificati autofirmati con certificati approvati per l'ambiente in uso e firmati da un'autorità di certificazione riconosciuta.

Oracle ILOM supporta vari metodi che possono essere utilizzati per accedere al certificato e alla chiave privata SSL/TLS, tra cui HTTPS, HTTP, SCP, FTP e TFTP, e per copiare le informazioni direttamente in un'interfaccia del browser Web. Per ulteriori informazioni, consultare la *guida per gli amministratori relativa a configurazione e gestione di Oracle ILOM* (vedere sezione chiamata «Risorse aggiuntive per Oracle ILOM» [52]).

1. **Determinare se Oracle ILOM sta utilizzando un certificato autofirmato predefinito.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **Installare il certificato dell'organizzazione.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

Timeout di inattività dell'interfaccia amministrativa del browser

Oracle ILOM supporta la possibilità di disconnettersi ed eseguire il logout delle sessioni amministrative rimaste inattive oltre il numero di minuti predefinito. Per impostazione predefinita, il timeout delle sessioni dell'interfaccia del browser si verifica dopo 15 minuti.

I parametri relativi al timeout delle sessioni associati ai servizi HTTPS e HTTP vengono impostati e gestiti indipendentemente. Assicurarsi di impostare i parametri `sessiontimeout` associati a ciascun servizio.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Verificare il parametro relativo al timeout di inattività associato al servizio HTTPS.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **Impostare il parametro relativo al timeout di inattività.**

   Sostituire *n* con un valore specificato in minuti.

```
-> set /SP/services/https sessiontimeout=n
```

4. **Verificare il parametro relativo al timeout di inattività associato al servizio HTTP.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **Impostare il parametro relativo al timeout di inattività.**

   Sostituire *n* con un valore specificato in minuti.

```
-> set /SP/services/http sessiontimeout=n
```

6. **Verificare l'impostazione ripetendo il Passo 2 e il Passo 4.**

▼ Configurare il timeout dell'interfaccia amministrativa (CLI di Oracle ILOM)

Oracle ILOM supporta la possibilità di disconnettersi ed eseguire il logout delle sessioni amministrative rimaste inattive oltre il numero di minuti predefinito.

Per impostazione predefinita, non sono specificati valori di timeout per l'interfaccia CLI SSH; pertanto, gli utenti amministrativi che accedono a questo servizio rimangono collegati per un periodo indefinito.

Per motivi di sicurezza, impostare questo parametro in modo che corrisponda al valore associato all'interfaccia utente del browser. È possibile specificare un valore pari a 15 minuti o un altro valore.

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

Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Verificare il parametro relativo al timeout di inattività associato all'interfaccia CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Impostare il parametro relativo al timeout di inattività.**

   Sostituire *n* con un valore specificato in minuti.

```
-> set /SP/cli timeout=n
```

4. **Verificare l'impostazione ripetendo il Passo 2.**

▼ Configurare i banner di avvertenza di login (Oracle ILOM)

Oracle ILOM supporta la possibilità di visualizzare messaggi specifici dell'utente prima e dopo che un amministratore ha eseguito la connessione a un dispositivo.

Il messaggio di connessione di Oracle ILOM viene visualizzato prima dell'autenticazione, mentre il messaggio di login viene visualizzato dopo l'autenticazione.

Facoltativamente, è possibile configurare Oracle ILOM in modo che richieda l'accettazione del messaggio di login prima di concedere l'accesso alle funzioni di Oracle ILOM. Sia i messaggi di connessione e di login che la richiesta di accettazione facoltativa vengono implementati da entrambe le interfacce di accesso della riga di comando e del browser.

Oracle ILOM supporta messaggi di connessione e di login con una lunghezza massima di 1.000 caratteri.

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

   Vedere Eseguire il login all'interfaccia CLI di Oracle ILOM [37].

2. **Disabilitare se i messaggi di connessione e di login sono configurati.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
```

```
Properties:
connect_message = (none)
login_message = (none)
```

3. **Impostare un messaggio di connessione o di login.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **Determinare se l'accettazione del messaggio di login è abilitata.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(Facoltativo) Applicare l'accettazione del messaggio di login.**

Attenzione - La richiesta di accettazione dei messaggi di login potrebbe influire sul corretto funzionamento dei processi di gestione automatici che utilizzano SSH, poiché potrebbero non essere in grado o non essere configurati per rispondere alla richiesta di accettazione. Di conseguenza, è possibile che si verifichi la sospensione o il timeout di tali connessioni poiché Oracle ILOM non consentirà di utilizzare l'interfaccia CLI finché non è stata soddisfatta la richiesta di accettazione dei messaggi.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **Verificare l'impostazione ripetendo il Passo 2 e il Passo 4.**

Risorse aggiuntive per Oracle ILOM

Per ulteriori informazioni sulle procedure di amministrazione e di sicurezza di Oracle ILOM, consultare la libreria delle documentazione di Oracle ILOM corrispondente alla versione in esecuzione su SuperCluster M7:

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

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager versione 3.2.*x*:

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager versione 3.1.*x*:

  http://docs.oracle.com/cd/E24707_01

- Oracle Integrated Lights Out Manager versione 3.0.*x*:

  http://docs.oracle.com/cd/E19860-01

Protezione dei server di calcolo

In SuperCluster M7 vengono installati uno o due server SPARC M7 (server di calcolo). Ogni server di calcolo è diviso in due partizioni hardware (due PDomain). Ogni PDomain include metà dei processori, della memoria e degli slot di espansione PCIe che possono essere presenti nello chassis. Entrambi i PDomain funzionano come un server distinto all'interno dello stesso chassis. Una coppia ridondante di SPM (Service Processor Module, modulo processore dei servizi) gestisce ogni partizione.

È necessario proteggere ogni PDomain.

In questa sezione viene fornito un set di controlli di sicurezza per i server di calcolo.

▼ Eseguire il login al server di calcolo e modificare la password predefinita

Per accedere a un singolo PDomain tramite Oracle ILOM, è necessario eseguire il login all'SPM attivo che controlla tale PDomain. È possibile accendere, eseguire il reboot o gestire una partizione mentre l'altra continua a funzionare normalmente.

Tanti sono i metodi che è possibile utilizzare per eseguire il login a un server di calcolo SuperCluster. Il metodo descritto in questa procedura prevede il login all'interfaccia CLI di

Oracle ILOM nell'SPM del server di calcolo. Questo metodo consente di accedere al server in uno qualsiasi degli stati riportati di seguito.

- Modalità operativa in standby
- Sistema acceso, ma host non in esecuzione
- Boot del sistema operativo
- Completamente acceso e con il sistema operativo in esecuzione

1. **Nella rete di gestione, eseguire il login utilizzando il comando `ssh`.**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **Quando richiesto, immettere la password.**

   La password `root` predefinita di fabbrica è `welcome1`.

   Se richiesto, modificare la password.

   A questo punto, è possibile eseguire tutte le procedure di sicurezza che vengono effettuate su Oracle ILOM nel server di calcolo.

3. **Se si desidera accedere alla console host del server di calcolo, avviare la console host.**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

Nota - Se l'host non è in esecuzione, verrà visualizzato il prompt di PDomain.

Nota - Per tornare al prompt di Oracle ILOM, digitare i caratteri escape (`#.` sono i caratteri predefiniti).

4. **Se necessario, assumere il ruolo di superutente.**

   Usare il comando `su` per passare a un utente configurato con il ruolo `root`.

Account e password predefiniti (server di calcolo)

Account	Password predefinita	Descrizione
`root`	`welcome1`	Oracle ILOM richiede che la password predefinita venga modificata immediatamente dopo il primo login riuscito.
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ Determinare la versione del software di SuperCluster

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Digitare questo comando.**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

   Nell'output, i numeri aggiunti a `ssc` rappresentano la versione del software.
   Per aggiornare la versione del software di SuperCluster, installare la più recente SuperCluster Quarterly Full Stack Download Patch disponibile in My Oracle Support all'indirizzo `https://support.oracle.com`.

Nota - Per SuperCluster, ulteriori restrizioni possono limitare le versioni del software che è possibile usare e la modalità di aggiornamento di tali versioni. In questi casi, contattare il rappresentante Oracle.

▼ Configurare il servizio Secure Shell

L'esecuzione di questa procedura consente di migliorare la configurazione di sicurezza Secure Shell distribuita in Oracle SuperCluster.

Il file `/etc/ssh/sshd_config` è un file di configurazione a livello di sistema in cui è possibile configurare i parametri per il servizio Secure Shell.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Modificare il file `/etc/ssh/sshd_config`.**

3. **Configurare il parametro `ListenAddress` per assicurare che siano accettate solo le connessioni che hanno origine dalla rete di accesso al client di SuperCluster.**

   Assicurarsi che l'indirizzo IP di `ListenAddress` sia impostato sulla rete del client.

   Ciò garantisce che nelle reti di gestione o IB non sia possibile avviare connessioni Secure Shell tra componenti.

4. **Rivedere gli altri parametri `sshd_config` e impostarli in base ai requisiti del sito.**

   Queste impostazioni proteggono il servizio Secure Shell:

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **Salvare il file `sshd_config`.**

6. **Riavviare il servizio.**

   Per rendere effettive le modifiche è necessario riavviare il servizio.

```
# svcadm restart ssh
```

▼ Verificare che `root` sia un ruolo

Per impostazione predefinita, Oracle Solaris è configurato in modo che `root` sia un ruolo e non un account utente. Inoltre, la configurazione di SuperCluster non consente il login di utenti `root` anonimi. Al contrario, tutti gli utenti devono eseguire il login come utente regolare prima di poter assumere il ruolo root. Tutte le operazioni di amministrazione di SuperCluster devono essere effettuate utilizzando `root` come ruolo.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Verificare che gli attributi `root` siano impostati su `type=role`.**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(Facoltativo) Assegnare un utente regolare al ruolo `root`.**

```
# usermod -R root user_name
```

Servizi di rete esposti predefiniti (server di calcolo)

Nella tabella sono elencati i servizi di rete predefiniti che sono esposti nei server di calcolo.

Nome servizio	Protocollo	Porta	Descrizione
SSH	TCP	22	Usato dal servizio Secure Shell integrato per consentire l'accesso amministrativo ai server di calcolo tramite un'interfaccia CLI.
HTTP (BUI)	TCP	80	Usato dal servizio HTTP integrato per consentire l'accesso amministrativo ai server di calcolo tramite un'interfaccia browser.
HTTPS (BUI)	TCP	443	Usato dal servizio HTTPS integrato per consentire l'accesso amministrativo ai server di calcolo su un canale cifrato (SSL/TLS) tramite un'interfaccia browser.
SNMP	UDP	161	Usato dal servizio SNMP integrato per fornire un'interfaccia di gestione al fine di monitorare lo stato dei server di calcolo e le notifiche di trap ricevute.

Rafforzamento della configurazione di sicurezza dei server di calcolo

In questi argomenti viene descritto come configurare in modo sicuro i server di calcolo.

Abilitare il servizio `intrd`

Il servizio di bilanciamento degli interrupt (`intrd`) monitora le assegnazioni tra gli interrupt e le CPU per assicurare prestazioni ottimali. Per ulteriori informazioni, vedere la pagina man `intrd (1M)`.

Questo servizio viene eseguito solo nella zona globale.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Avviare il servizio.**

```
# svcadm enable intrd
```

▼ Disabilitare i servizi non necessari (server di calcolo)

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Disabilitare il monitoraggio dello stato NFS se il sistema non è un client o un server NFS.**
   Questo servizio interagisce con `lockd(1M)` per fornire le funzioni di crash e recupero per i servizi di blocco in NFS.

   ```
   # svcadm disable svc:/network/nfs/status
   ```

3. **Disabilitare il servizio di gestione del blocco NFS se non si utilizza NFS o se si utilizza NFSv4.**
   Questo servizio supporta le operazioni di blocco dei record su file NFS in NFSv2 e NFSv3.

   ```
   # svcadm disable svc:/network/nfs/nlockmgr
   ```

4. **Se il sistema non sta eseguendo il mount dei file, è possibile disabilitare il servizio client NFS o disinstallare il relativo package.**
   Il servizio client NFS è necessario solo se il sistema sta eseguendo il mount dei file da un server NFS. Per ulteriori informazioni, vedere la pagina man `mount_nfs(1M)`.

   ```
   # svcadm disable svc:/network/nfs/client
   ```

5. **Disabilitare il servizio server NFS in un sistema che non è un file server NFS.**
   Il servizio server NFS gestisce le richieste del file system del client in NFS versioni 2, 3 e 4. Se il sistema in uso non è un server NFS, disabilitare il servizio.

   ```
   # svcadm disable svc:/network/nfs/server
   ```

6. **Se non si utilizza FedFS per i record DNS SRV o i riferimenti basati su LDAP, disabilitare il servizio.**
   Il servizio client FedFS (Federated File System) gestisce le impostazioni predefinite e le informazioni di connessione per i server LDAP che memorizzano informazioni FedFS.

   ```
   # svcadm disable svc:/network/nfs/fedfs-client
   ```

7. **Disabilitare il servizio `rquota`.**

Il server di quota `remote` restituisce le quote per un utente di un file system locale di cui è stato eseguito il mount su NFS. I risultati vengono utilizzati da `quota(1M)` per visualizzare le quote utente per i file system remoti. Il daemon `rquotad(1M)` viene in genere richiamato da `inetd(1M)`. Il daemon fornisce informazioni sulla rete a utenti potenzialmente malintenzionati.

```
# svcadm disable svc:/network/nfs/rquota
```

8. **Disabilitare il servizio `cbd`.**

   Il servizio `cbd` gestisce gli endpoint di comunicazione per il protocollo NFS versione 4. Il daemon `nfs4cbd(1M)` viene eseguito sul client NFS versione 4 e crea una porta di ascolto per i callback.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **Disabilitare il servizio `mapid` se non si utilizza NFSv4.**

   Il servizio daemon di mapping dell'utente NFS e dell'ID gruppo esegue il mapping negli e dagli attributi di identificazione `owner` e `owner_group` di NFS versione 4; i numeri di UID e GID locali vengono usati sia dal client che dal server NFS versione 4.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **Disabilitare il servizio `ftp`.**

    Il servizio FTP fornisce il trasferimento di file non cifrati e utilizza l'autenticazione del testo semplice. Usare il programma di copia sicura `scp(1)` al posto di `ftp`, perché fornisce l'autenticazione cifrata e il trasferimento di file.

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **Disabilitare il servizio di gestione dei volumi remoti.**

    Il servizio di gestione dei volumi removibili è abilitato per HAL e può eseguire e annullare il mount dei supporti removibili e dello storage hot plug in modo automatico. Gli utenti potrebbero importare programmi dannosi o trasferire dati riservati fuori dal sistema. Per ulteriori informazioni, vedere la pagina man `rmvolmgr(1M)`.

    Questo servizio viene eseguito solo nella zona globale.

    ```
    # svcadm disable svc:/system/filesystem/rmvolmgr
    ```

12. **Disabilitare il servizio `smserver`.**

    Il servizio `smserver` viene usato per accedere ai dispositivi di supporto removibili.

    ```
    # svcadm disable rpc/smserver:default
    ```

13. Specificare `pam_deny.so.1` come modulo per lo stack di autenticazione per i servizi `r-protocol` nella directory `/etc/pam.d`.

Per impostazione predefinita, i servizi precedenti come `r-protocols`, `rlogin(1)` e `rsh(1)` non vengono installati. Questi servizi sono comunque definiti in `/etc/pam.d`. Se queste definizioni dei servizi vengono rimosse in `/etc/pam.d`, i servizi utilizzeranno altri servizi, ad esempio SSH, nel caso in cui i servizi precedenti siano abilitati.

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. Modificare il file `/etc/default/keyserv` per cambiare il valore di `ENABLE_NOBODY_KEYS` in `NO`.

Il servizio `keyserv` non può usare la chiave utente `nobody`. Per impostazione predefinita, il valore di `ENABLE_NOBODY_KEYS` è `YES`.

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. Aggiungere gli utenti al file `ftpusers` per limitare l'accesso `ftp`.

I trasferimenti di file FTP non devono essere disponibili per tutti gli utenti; agli utenti qualificati occorre richiedere di fornire il nome e la password. In genere, agli utenti del sistema non è consentito usare FTP. Questo controllo consente di verificare che gli account di sistema siano inclusi nel file `/etc/ftpd/ftpusers` e pertanto non abilitati a usare FTP.

Il file `/etc/ftpd/ftpusers` viene usato per impedire agli utenti l'uso del servizio FTP. Come minimo, includere tutti gli utenti di sistema, come `root`, `bin`, `adm` e così via.

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. Impostare una robusta maschera di creazione file predefinita per i file creati dal server FTP.

Non necessariamente il server FTP usa la maschera di creazione dei file di sistema dell'utente. L'impostazione di umask su FTP assicura che i file trasmessi tramite FTP utilizzino un umask di creazione file robusto.

```
# pfedit /etc/proftpd.conf
Umask          027
```

17. **Disabilitare le risposte alle query sulla topologia di rete.**

    È importante disabilitare le risposte alle richieste di eco. Le richieste ICMP vengono gestite utilizzando il comando `ipadm`.

    Queste impostazioni impediscono la diffusione di informazioni sulla topologia di rete.

    ```
    # ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
    # ipadm set-prop -p _respond_to_echo_broadcast=0 ip
    ```

18. **Disabilitare i messaggi ICMP di reindirizzamento.**

    I router utilizzano i messaggi di reindirizzamento ICMP per informare gli host della presenza di più instradamenti diretti per una destinazione. Un messaggio di reindirizzamento ICMP non valido può provocare un attacco MITM (man-in-the-middle).

    ```
    # ipadm set-prop -p _ignore_redirect=1 ipv4
    ```

19. **Disabilitare `mesg(1)` per impedire che `talk(1)` e `write(1)` accedano ai terminali remoti.**

    ```
    # mesg -n
    ```

20. **(Facoltativo) Rivedere e disabilitare i servizi di ascolto sulla rete non necessari.**

    Per impostazione predefinita, `ssh(1)` è l'unico servizio di rete che può inviare e ricevere pacchetti di rete.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

▼ Abilitare un rigido livello di multihoming

Per i sistemi che sono gateway per altri domini, come firewall o nodi VPN, è necessario abilitare un rigido livello di multihoming. La proprietà `hostmodel` controlla i comportamenti di invio e ricezione dei pacchetti IP in un sistema multihoming. Impostare il rigido livello di multhoming su `1` in modo che i pacchetti non siano accettati in un'altra interfaccia. L'impostazione predefinita è `0`.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare il rigido livello di multihoming su `1`.**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

Abilitare ASLR

Nota - Non abilitare ASLR nei domini di database o nelle zone di database.

Oracle Solaris contrassegna più binari utenti per l'abilitazione di ASLR (Address Space Layout Randomization). ASLR dispone in ordine casuale l'indirizzo di inizio delle parti chiave in uno spazio di indirizzi. Questo meccanismo di difesa e sicurezza può evitare l'esito favorevole di attacchi ROP (Return Oriented Programming) durante i tentativi di sfruttamento delle vulnerabilità del software. Le zone ereditano questo layout casuale per i relativi processi. Poiché l'uso di ASLR può non essere ottimale per tutti i binari, è possibile configurare ASLR a livello di zona e binario.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare ASLR.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                 CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

Configurare le connessioni TCP

Impostando su 4096 il numero massimo di connessioni TCP aperte a metà per indirizzo IP e per porta, è possibile difendersi dagli attacchi SYN flood di tipo DoS (Denial of Service). Impostando su almeno 1024 il numero massimo di connessioni TCP in entrata inserite nella coda, è possibile evitare determinati attacchi di tipo DDoS (Distributed Denial of Service).

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare il numero massimo di connessioni TCP aperte a metà e in entrata inserite nella coda.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

Impostare i log di cronologia e i criteri delle password per la conformità PCI

Il parametro `HISTORY` nel file `/etc/default/passwd` impedisce agli utenti di utilizzare password simili in base al valore di `HISTORY`.

Se `MINWEEKS` è impostato su `3` e `HISTORY` è impostato su `10`, le password non possono essere riutilizzate per 10 mesi.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Modificare il file `/etc/default/passwd` e impostare i parametri per le password.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Modificare il file `/etc/default/login` per includere questi parametri.**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

Assicurare che le directory home degli utenti dispongano delle autorizzazioni appropriate

È necessario che i proprietari delle directory home abbiano accesso alla lettura e alla ricerca in tali relative directory. In genere, gli altri utenti non dispongono dei diritti per modificare

o aggiungere file nelle directory home di cui non sono proprietari. Per garantire questa condizione, impostare le autorizzazioni per la directory dell'utente.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare le autorizzazioni per la directory di un utente.**

```
# chmod 750 /export/home/user_home_directory
```

▼ Abilitare il firewall del filtro IP

Il filtro IP è un firewall basato su host in grado di filtrare i pacchetti con conservazione dello stato ed eseguire la traslazione degli indirizzi di rete (NAT, Network Address Translation). La funzionalità di filtro dei pacchetti fornisce un livello di protezione di base dagli attacchi in rete. Inoltre, il filtro IP include la funzionalità di filtro dei pacchetti senza conservazione dello stato ed è in grado di creare e gestire pool di indirizzi.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare il firewall del filtro IP.**

```
# svcadm svc:/network/ipfilter:default
```

▼ Verificare che i servizi dei nomi utilizzino solo file locali

Il sistema operativo utilizza un determinato numero di database contenenti informazioni sugli elementi host, `ipnodes`, utenti (`passwd(4)`, `shadow(4)`, `user_attr(4)`) e `groups`. I dati relativi a questi elementi provengono da diverse origini. Ad esempio, è possibile trovare i nomi e gli indirizzi host in `/etc/hosts`, NIS, LDAP, DNS o Multicast DNS. I sistemi in ambienti limitati sono più sicuri se per questi elementi vengono usate solo voci di file locali.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Configurare i servizi dei nomi in modo che utilizzino solo file locali.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

Abilitare i servizi sendmail e NTP

È necessario che il servizio sendmail sia in esecuzione, altrimenti i messaggi di posta importanti del sistema per `root` non verranno consegnati.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare sendmail.**

```
# svcadm enable smtp:sendmail
```

3. **Se necessario, installare il servizio NTP.**

   Il servizio `ntp` deve essere installato su tutti i sistemi in cui si desidera conseguire sicurezza e conformità.

```
# pkg install service/network/ntp
```

4. **Configurare il servizio NTP come un client e abilitarlo.**

   È necessario che il daemon NTP (Network Time Protocol) sia abilitato e configurato correttamente come un client. Il file `/etc/inet/ntp.conf` deve includere almeno una definizione di server. Inoltre, il file deve contenere la riga `restrict default ignore` per evitare che il client agisca anche da server.

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

Disabilitare GSS (a meno che non si usi Kerberos)

Il servizio di sicurezza generico (`gss`, generic security service) gestisce la creazione e la convalida dei token di sicurezza GSS-API (Generic Security Service Application Program Interface). Il daemon `gssd(1M)` opera tra il kernel `rpc` e GSS-API.

Nota - Kerberos usa questo servizio. Disabilitare il servizio `rpc/gss` se Kerberos non è configurato e in uso.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare `rpc/gss`.**

```
# svcadm enable rpc/gss
```

3. **Impostare un limite per le dimensioni di `/tmpfs`.**

   Per impostazione predefinita, le dimensioni del file system `tmpfs` non sono limitate. Per evitare impatti sulle prestazioni, è possibile limitare le dimensioni di ogni mount `tmpfs`. Per ulteriori informazioni, vedere le pagine man `mount_tmpfs(1M)` e `vfstab(4)`.

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **Eseguire il reboot del server di calcolo.**

```
# reboot
```

Impostare lo sticky bit per i file scrivibili da tutti

Lo sticky bit in una directory scrivibile a tutti impedisce che i file presenti nella directory possano essere eliminati o spostati da chiunque tranne che dal proprietario del file o dal ruolo `root`. È utile per le directory che sono comuni a più utenti, ad esempio la directory `/tmp`.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare lo sticky bit per `/tmp` e per qualsiasi altro file scrivibile a tutti.**

```
# chmod 1777 /tmp
```

Proteggere i dump core

I dump core possono contenere dati sensibili. Le modalità di protezione possono includere le autorizzazioni dei file e la registrazione degli eventi di dump core. Vedere le pagine man `coreadm(1m)` e `chmod(1M)`.

Usare il comando `coreadm` per visualizzare e impostare la configurazione corrente.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Visualizzare la configurazione corrente.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **Configurare i file core e proteggere la directory dei dump core.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **Controllare le autorizzazioni.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **Impostare correttamente le autorizzazioni per la directory.**

```
# chmod 700 /var/share/cores
```

Applicare stack non eseguibili

L'abilitazione degli stack non eseguibili è una tecnica molto utile per contrastare determinati tipi di attacchi di buffer overflow. Quando `nxstack` di Oracle Solaris è abilitato, il segmento di memoria dello stack del processo viene contrassegnato come non eseguibile. Ciò consente di difendersi dagli attacchi che si basano sull'inserimento di codice dannoso da eseguire nello stack.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare `nxstack`.**

   ```
   # sxadm set model=all nxstack
   ```

3. **Verificare la configurazione.**

   ```
   # sxadm get all nxstack
   EXTENSION     PROPERTY     VALUE
   nxstack         model        all
   ```

Abilitare lo spazio di swap cifrato

Cifrare lo spazio di swap, indipendentemente che si tratti di un volume ZFS o di un dispositivo raw. La cifratura assicura la protezione di tutti i dati sensibili, ad esempio le password degli utenti, nel caso in cui si renda necessario eseguire lo swap delle relative pagine esternamente al disco.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Modificare il file `/etc/vfstab` e impostare `swap` su `encrypted`.**

   ```
   # pfedit /etc/vfstab
   ...
   /dev/zvol/dsk/rpool/swap - - swap - no encrypted
   ```

3. **Creare e inizializzare un keystore PKCS #11.**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **Generare una chiave asimmetrica e memorizzarla in un keystore PKCS #11.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

Abilitare l'audit

Accertarsi che i log di audit acquisiscano tutte le azioni amministrative, inclusi i comandi e gli argomenti.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Configurare la funzionalità di audit.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

Abilitare la protezione del collegamento dati (spoofing) sulle zone globali

La protezione del collegamento dati di Oracle Solaris impedisce il potenziale danno che può essere provocato alla rete da VM guest malevoli.

L'abilitazione della configurazione a prova di snooping migliora le prestazioni della rete, consentendo al traffico di rete dell'ambiente virtuale di essere isolato dal più ampio traffico di ricezione o invio del sistema host. La protezione del collegamento impedisce il danno che può essere provocato alla rete da VM guest potenzialmente malevoli. Questa funzione offre protezione dalle seguenti minacce di base:

- IP spoofing e MAC spoofing

- spoofing di frame L2 come gli attacchi BPDU (Bridge Protocol Data Unit)

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare la protezione del collegamento.**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **Confermare la configurazione.**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **Impostare gli IP consentiti sul collegamento.**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

Abilitare la protezione del collegamento dati (spoofing) sulle zone non globali

La protezione del collegamento dati di Oracle Solaris può anche essere applicata individualmente alle zone non globali di Oracle Solaris distribuite all'interno dell'ambiente SuperCluster.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Applicare la protezione del collegamento dati su una determinata interfaccia di rete utilizzando il comando `zonecfg(1M)`.**
   Assicurarsi che l'elenco di indirizzi IP consentiti sia accurato e completo. Nell'elenco devono essere inclusi tutti gli indirizzi IP virtuali usati da Oracle Solaris IPMP, Oracle Real Application Clusters e così via. Tenere presente che le modifiche apportate alla configurazione della zona non globale del SuperCluster non avranno effetto finché la zona non globale non verrà riavviata.

```
# zonecfg –z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

Creare set di dati ZFS cifrati

Le organizzazioni che richiedono il tipo di protezione *data-at-rest*, possono scegliere di proteggere ulteriormente le applicazioni e le informazioni distribuite nella zona utilizzando i set di dati ZFS cifrati. Per garantire che ciascuna zona non globale sia in grado di avviarsi senza l'intervento dell'amministratore, i data set ZFS cifrati vengono configurati per accedere alle chiavi di cifratura ZFS che sono memorizzate localmente all'interno del singolo database o dominio applicazione.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Creare le chiavi di cifratura ZFS.**

   Per creare le chiavi necessarie in modo agevole, è possibile usare comandi simili a quelli riportati di seguito.

   ```
   # zfs create zfs_pool_name/zfskeystore
   $ chown root:root /zfs_pool_name/zfskeystore
   $ chmod 700 /zfs_pool_name/zfskeystore
   $ pktool genkey keystore=file keytype=aes keylen=256 \
   outkey=/zfs_pool_name/zfskeystore/zone_name.key
   ```

3. **Creare il set di dati ZFS cifrato.**

   ```
   # zfs create -o encryption=aes-256-ccm -o \
   keysource=raw,file:///zfs_pool_name/zone_name.key \
   zfs_pool_name/zone_name
   ```

4. **Cifrare i set di dati u01 e comune.**

   Per cifrare i set di dati u01 e comune è possibile usare la stessa procedura, utilizzando la stessa chiave (specifica di SuperCluster) o una chiave univoca per set di dati in base ai requisiti e ai criteri specifici del sito. In questo esempio, il set di dati comune viene creato utilizzando

la stessa chiave creata nel Passo 3. Durante la creazione di questi ulteriori set di dati, è anche possibile definire parametri di configurazione ZFS aggiuntivi, ad esempio per la compressione.

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

(Facoltativo) Impostare una passphrase per l'accesso al keystore

Nella procedura precedente, Creare set di dati ZFS cifrati [74], viene usato un file chiave (raw) definito localmente che deve essere memorizzato direttamente in un file system. Un'altra tecnica di memorizzazione della chiave sfrutta un keystore PKCS#11 protetto da passphrase e si chiama *token Sun Software PKCS#11*. Per usare questo metodo, attenersi alla procedura descritta di seguito.

È necessario sbloccare manualmente il keystore PKCS#11 affinché la chiave sia resa disponibile per ZFS. In altre parole, ciò significa che occorre l'intervento dell'amministratore per eseguire il mount del set di dati ZFS cifrato, nonché avviare la zona non globale se anche questa utilizza un set di dati ZFS cifrato. Per ulteriori informazioni su altre strategie di memorizzazione della chiave, vedere la pagina man `zfs_encrypt(1M)`.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Impostare un PIN (passphrase) che sarà necessario per accedere al keystore.**

   Il PIN predefinito associato a un nuovo keystore PKCS#11 è `changeme`. Usare questa passphrase al primo prompt dell'esempio riportato di seguito.

   ```
   # pktool setpin keystore=pkcs11
   Enter token passphrase:
   Create new passphrase:
   Re-enter new passphrase:
   ```

3. **Definire una variabile di ambiente `${SOFTTOKEN}` per memorizzare la chiave in una posizione diversa.**

   La chiave usata dal token Sun Software PKCS#11 viene memorizzata per impostazione predefinita nella directory `/var/user/ ${USERNAME}/pkcs11_softtoken`. È possibile definire la variabile di ambiente `${SOFTTOKEN}` per memorizzare la chiave in un'altra posizione. È possibile usare questa funzionalità per abilitare uno storage specifico di SuperCluster per questa chiave protetta da passphase.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Creare una chiave.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **Creare il set di dati ZFS cifrati, facendo riferimento alla chiave creata nel passo precedente.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

Creare zone globali immutabili

L'antimanomissione con immutabilità consente alle zone globali e non globali di creare un ambiente operativo resiliente e altamente integrato all'interno del quale i server di calcolo SuperCluster fanno funzionare i relativi servizi. Basate sulle capacità di sicurezza intrinseca delle zone globali e non globali di Oracle Solaris, le zone immutabili assicurano che non sia possibile modificare directory (alcune o tutte) e file (alcuni o tutti) del sistema operativo senza l'intervento dell'amministratore. L'applicazione di questa impostazione di sola lettura consente di evitare modifiche non autorizzate, promuove pratiche di gestione delle modifiche più robuste e rimuove l'inserimento di malware basato su kernel e utente.

Nota - Una volta configurata, la zona immutabile può essere aggiornata solo tramite login con percorso sicuro o quando viene eseguito il reboot del sistema con la modalità scrivibile utilizzando `reboot -- -w`.

Anche se occorre sempre verificare che il funzionamento del software applicativo sia quello previsto in un ambiente immutabile, tenere presente che la corretta esecuzione delle istanze Oracle Database e dei cluster Oracle RAC viene verificata all'interno delle zone non globali immutabili di Oracle Solaris.

1. **Eseguire il login alla zona globale di Oracle Solaris (dominio dedicato, dominio root o dominio di I/O) come superutente.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Modificare la configurazione della zona globale di Oracle Solaris impostando la proprietà `file-mac-profile`.**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
zonecfg:global> commit
```

3. **Eseguire il reboot della zona globale di Oracle Solaris per rendere effettive le modifiche. Eseguire il login al dominio tramite la console ILOM.**

4. **Avviare la console del percorso sicuro della zona globale immutabile.**

   Poiché la zona globale immutabile è stata configurata, è importante immettere le informazioni di login alla console utilizzando una di queste sequenze di interruzione:

   - **Console grafica**: F1-A
   - **Console seriale**: <Interruzione> o sequenza di interruzione alternativa (CR~ Ctrl-b)

```
trusted path console login:
```

5. **Eseguire il login alla zona globale del dominio di I/O e assumere il ruolo `root` per eseguire eventuali aggiornamenti specifici al sistema, quindi eseguire il reboot del sistema per riportarlo in modalità di sola lettura.**

```
# reboot
```

▼ Configurare zone non globali immutabili

Per configurare una zona non globale di Oracle Solaris in modo che sia immutabile, attenersi alla procedura descritta di seguito.

Nota - Il sistema operativo Oracle Solaris 11 supporta altre configurazioni di zona immutabile oltre a quella descritta in questa procedura (configurazione fissa). Per ulteriori informazioni su queste opzioni, vedere la pagina man `zonecfg(1M)`. Tuttavia, solo l'opzione di configurazione fissa è stata sottoposta a test come parte dell'architettura SuperCluster.

Attenzione - Non è possibile aggiungere, modificare o eliminare account e password degli utenti della zona dopo aver abilitato l'immutabilità della zona non globale di Oracle Solaris, come descritto in questa procedura. Questo problema può comunque essere risolto distribuendo una directory LDAP contenente informazioni specifiche sulla zona, come utenti, ruoli, gruppi, diritti, profili e così via.

Attenzione - La funzionalità di zona immutabile di Oracle Solaris è limitata ai set di dati ZFS che vengono implementati per impostazione predefinita in una zona non globale Oracle Solaris. Ulteriori file system, pool o set di dati non sono soggetti ai criteri di zona immutabile, sebbene l'accesso a questi elementi di file possano essere controllati con altre modalità, come l'uso dei mount di loopback di sola lettura.

1. **Eseguire il login a uno dei server di calcolo e accedere alla console host come superutente.**
   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Assicurarsi che la zona non globale di Oracle Solaris sia arrestata.**
   Se questo comando restituisce un valore, la zona non globale di Oracle Solaris è in esecuzione ed occorre arrestarla.

   Nota - Anche se la zona può essere arrestata utilizzando il comando `zoneadm(1M)`, seguire le procedure di arresto eventualmente stabilite dall'organizzazione per evitare la potenziale interruzione del servizio e la perdita di dati.

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **Regolare la configurazione della zona non globale di Oracle Solaris impostando la proprietà `file-mac-profile`.**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **Se necessario, disabilitare la configurazione immutabile della zona non globale.**

   ```
   # zonecfg -z zone_name set file-mac-profile=none
   ```

5. **Riavviare la zona non globale di Oracle Solaris per rendere effettive le modifiche.**

   ```
   # zoneadm -z zone_name boot
   ```

Abilitare il boot verificato sicuro (interfaccia CLI di Oracle ILOM)

Attenersi alla procedura descritta di seguito per abilitare il boot verificato sicuro tramite l'interfaccia CLI di Oracle ILOM. In alternativa, è possibile usare l'interfaccia Web di

Oracle ILOM. Vedere sezione chiamata «Boot verificato sicuro (interfaccia Web di Oracle ILOM)» [80].

Il boot verificato fa riferimento alla verifica dei moduli oggetto che viene effettuata prima dell'esecuzione utilizzando le firme digitali. Oracle Solaris protegge dal caricamento di moduli kernel dannosi. Il boot verificato aumenta la sicurezza e la robustezza di Oracle Solaris verificando i moduli kernel prima dell'esecuzione.

Se abilitato, il boot verificato di Oracle Solaris controlla la firma di fabbrica di un modulo kernel prima di caricare ed eseguire il modulo. Questo controllo consente di rilevare modifiche accidentali o malevoli di un modulo. L'azione intrapresa è configurabile e, quando abilitata, può visualizzare un messaggio di avvertenza e continuare il caricamento e l'esecuzione del modulo oppure non riuscire e arrestare il caricamento e l'esecuzione del modulo.

1. **Accedere a Oracle ILOM sul server di calcolo.**

   Vedere Eseguire il login al server di calcolo e modificare la password predefinita [55].

2. **Abilitare il boot verificato.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Accedere al certificato fornito da Oracle e visualizzarlo.**

   Un file certificato di boot verificato preinstallato, `/etc/certs/ORCLS11SE`, viene fornito come parte di Oracle ILOM.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **Avviare il caricamento del certificato.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **Copiare il contenuto del file `/etc/certs/ORCLS11SE` e incollarlo nella console di Oracle ILOM.**

   Immettere Ctrl-z per salvare ed elaborare le informazioni.

   Immettere Ctrl-c per uscire e annullare le modifiche.

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
```

```
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. **Verificare il certificato.**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **Verificare che il parametro OBP `use-nvram` sia impostato su `false`.**

   Quando si utilizza il boot verificato, il parametro OBP `use-nvram` deve essere impostato su `false`. In questo modo si impedisce che OBP venga modificato per disabilitare la funzionalità del boot verificato. Il valore predefinito è false. Eseguire il login a Oracle Solaris e digitare:

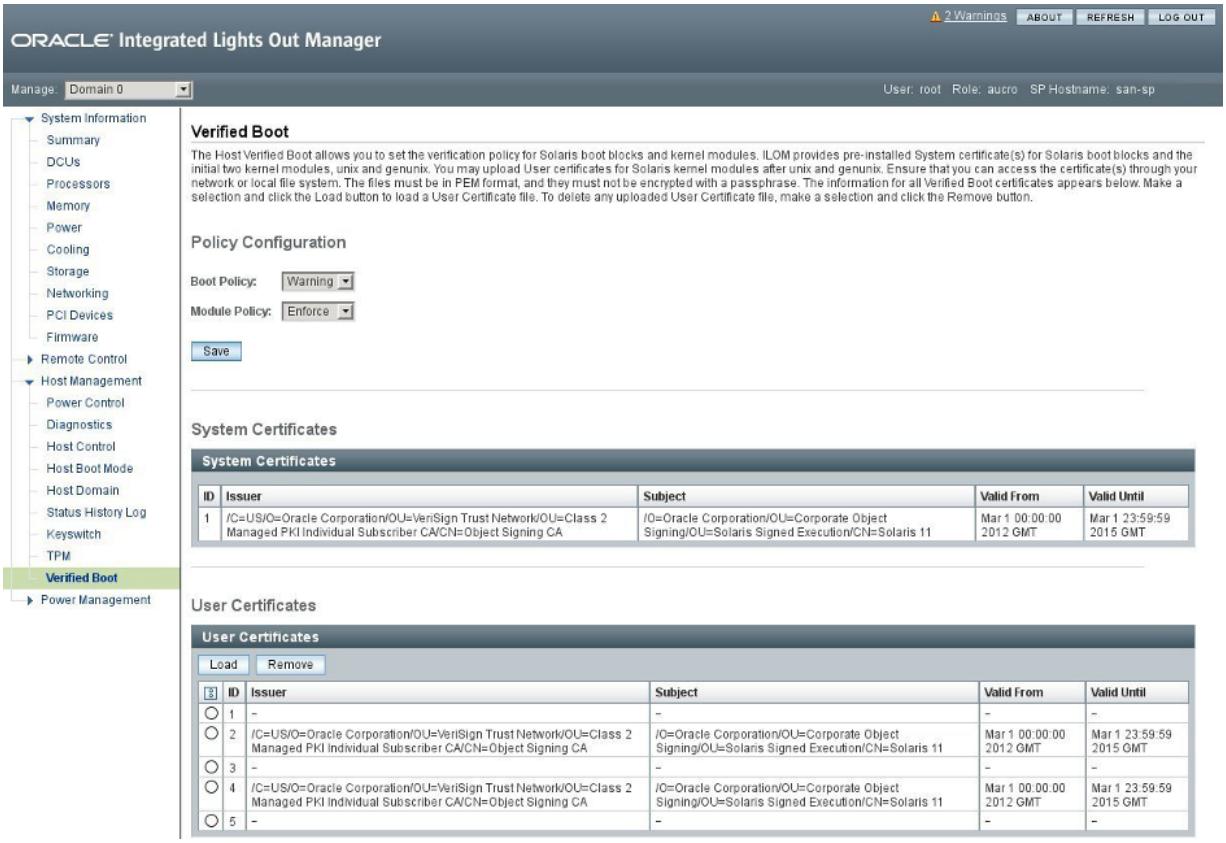
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

Boot verificato sicuro (interfaccia Web di Oracle ILOM)

L'interfaccia Web di Oracle ILOM supporta anche l'impostazione delle variabili dei criteri del boot verificato e la gestione dei file certificato, fornendo la stessa funzionalità dell'interfaccia CLI. Andare al collegamento Boot verificato nel menu di navigazione Gestione host.

Ad esempio:



Risorse aggiuntive dei server di calcolo

Per le guide sulla sicurezza del sistema operativo Oracle Solaris e di Oracle Solaris Cluster, fare riferimento alla libreria della documentazione corrispondente alla versione del sistema operativo. Le librerie sono disponibili all'indirizzo `http:/docs.oracle.com/en/operating-systems`.

Per le informazioni sulla sicurezza di Oracle VM Server per SPARC, fare riferimento alla guida sulla sicurezza all'indirizzo `http://docs.oracle.com/cd/E62357_01`.

Per le informazioni sulla sicurezza dell'hardware del server di calcolo, fare riferimento alla guida sulla sicurezza all'indirizzo `http://docs.oracle.com/cd/E55211_01`.

Protezione di ZFS Storage Appliance

ZFS Storage Appliance è uno dei componenti di SuperCluster utilizzato per supportare il consolidamento dei sistemi di storage in vari carichi di lavoro complessi, quali business intelligence, data warehousing, virtualizzazione, sviluppo e test e protezione dei dati.

ZFS Storage Appliance include due controller di storage ZFS ridondanti. È necessario proteggere entrambi i controller.

Nelle sezioni riportate di seguito vengono descritte le linee guide e le funzioni relative alla sicurezza di ZFS Storage Appliance.

▼ Eseguire il login a ZFS Storage Appliance

Per eseguire le procedure di sicurezza descritte in questa sezione, eseguire il login a ZFS Storage Appliance mediante la rete di gestione.

In questa procedura viene descritto come eseguire il login utilizzando l'interfaccia CLI. Per le istruzioni simili relative al login all'interfaccia Web di Oracle ILOM, consultare la *guida di amministrazione di Oracle ZFS Storage Appliance*. Vedere sezione chiamata «Risorse aggiuntive per ZFS Storage Appliance» [93].

1. **Sulla rete di gestione utilizzare il comando SSH per connettersi a ZFS Storage Appliance.**

Se non sono stati configurati altri utenti per amministrare l'appliance, è necessario eseguire il login come `root`.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **Se necessario, accedere alla Guida dell'interfaccia CLI.**

   Il comando `help` fornisce la Guida specifica del contesto. Per accedere alla Guida su un determinato argomento, specificarlo come argomento in `help`. Gli argomenti disponibili vengono visualizzati utilizzando la funzione di completamento automatico tramite il tasto tab del comando help oppure digitando `help topics`.

▼ Determinare la versione del software di ZFS Storage Appliance

Attenersi alla procedura descritta di seguito per determinare la versione del software di ZFS Storage Appliance.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Visualizzare la versione del software.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

In questo esempio, la versione del software di ZFS Storage Appliance è la `2013.06.05.2.10`.

Per aggiornare la versione del software di ZFS Storage Appliance, installare la versione più recente di SuperCluster Quarterly Full Stack Download Patch disponibile in My Oracle Support all'indirizzo `https://support.oracle.com`.

Nota - Alcune limitazioni aggiuntive definite per SuperCluster potrebbero limitare le versioni del software di ZFS Storage Appliance utilizzabili e le modalità di aggiornamento di tali versioni. In questi casi, contattare il rappresentante Oracle.

Modificare la password root di ZFS Storage Appliance

ZFS Storage Appliance non è preconfigurato con una password root predefinita. La configurazione iniziale di ZFS Storage Appliance viene eseguita mediante una sessione della console del software Oracle ILOM incorporato. La password root dell'appliance viene impostata durante questa sessione di configurazione iniziale.

Quando si accede inizialmente alla console dell'appliance, viene visualizzata una schermata di configurazione dell'interfaccia shell. Verificare le informazioni visualizzate nella schermata e inserire i valori richiesti. La password root di ZFS Storage Appliance viene impostata durante questo processo.

Nota - Oracle ILOM per l'appliance dispone di un account root e della password welcome1 predefiniti. Vedere Protezione di Oracle ILOM [37].

Una volta che si dispone di un account root, è possibile modificare la password in qualsiasi momento, come descritto in questa procedura.

Nota - Quando una password viene modificata per un componente di SuperCluster gestito da Oracle Engineered Systems Hardware Manager (ad esempio, il sistema operativo del controller di storage AFS), è inoltre necessario aggiornare la password in Oracle Engineered Systems Hardware Manager. Per utleriori informazioni, consultare la *Guida all'amministrazione di Oracle SuperCluster serie M7*.

---

1. **Eseguire il login a ZFS Storage Appliance**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Modificare la password root.**

   In questo esempio, sostituire *password* con una password conforme ai criteri di complessità delle password definiti dal Dipartimento della difesa degli Stati Uniti.

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

Per ulteriori informazioni sull'installazione e sulla configurazione iniziali di ZFS Storage Appliance, consultare *Oracle ZFS Storage Appliance Installation Guide*. Vedere sezione chiamata «Risorse aggiuntive per ZFS Storage Appliance» [93].

Servizi di rete esposti predefiniti (ZFS Storage Appliance)

In questa tabella vengono elencati i servizi di rete predefiniti esposti da ZFS Storage Appliance.

Servizio	Protocollo	Porta	Descrizione
SSH	TCP	22	Utilizzato dal servizio Secure Shell integrato per abilitare l'accesso amministrativo a ZFS Storage Appliance utilizzando un'interfaccia CLI.
PORTMAP	TCP/UDP	111	Utilizzato dal daemon di mapping della porta RPC (Remote Procedure Call) (noto come `rpcbind` o `portmap`). Questo servizio è richiesto per supportare NFS versione 3.
NTP	UDP	123	Utilizzato dal servizio NTP (Network Time Protocol) integrato (solo client) per sincronizzare il clock di sistema locale con una o più origini temporali esterne.
HTTPS (BUI)	TCP	215	Utilizzato dal servizio HTTPS integrato per abilitare l'accesso amministrativo a ZFS Storage Appliance su un canale (SSL/TLS) cifrato utilizzando un'interfaccia del browser.
Replica remota	TCP	216	Utilizzato dal servizio di replica dati remota integrato. La replica dati remota duplica e sincronizza i progetti e le condivisioni tra più ZFS Storage Appliance su un canale (SSL/TLS) cifrato.
NFS	TCP/UDP	2049 4045 varia	Utilizzato dal servizio NFS (Network File System) NFS fornisce il servizio di condivisione dei file di rete. Il numero effettivo di porte dipende dalla versione del protocollo NFS utilizzata. NFS versione 3 si basa sul daemon di mapping della porta RPC (elencato sopra) e sulle porte allocate in modo dinamico per fornire servizi di installazione, di gestione dello stato e delle quote nonché servizi correlati. NFS versione 4, tuttavia, si basa solo su TCP/2049. Il servizio di blocco NFS utilizza TCP/4045.
iSCSI / iSNS	TCP	3260	Utilizzato dal servizio iSCSI che fornisce un protocollo di rete di storage basato su IP per il collegamento alle funzioni di memorizzazione dei dati. È possibile configurare ZFS Storage Appliance per condividere i dispositivi iSCSI (chiamati LUN) con i client collegati in rete.
Service Tags	TCP	6481	Utilizzato dal servizio Oracle ServiceTag. Si tratta di un protocollo di ricerca automatica di Oracle utilizzato per identificare i server e semplificare le richieste di servizio. Questo servizio viene utilizzato da prodotti quali Oracle Enterprise Manager Ops Center per trovare il software di ZFS Storage Appliance e per l'integrazione con altre soluzioni di servizio automatico Oracle.
NDMP	TCP	10000	Utilizzato dal servizio NDMP (Network Data Management Protocol) che consente a ZFS Storage Appliance di partecipare a backup coordinati in remoto.

ZFS Storage Appliance supporta anche molti altri servizi disabilitati per impostazione predefinita, inclusi `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV` e così via. Se questi servizio vengono abilitati dopo l'installazione, è possibile che altre porte risultino esposte.

Potenziamento della configurazione di sicurezza di ZFS Storage Appliance

Negli argomenti riportati di seguito viene descritto come potenziare la configurazione di sicurezza di ZFS Storage Appliance:

▼ Implementare il potenziamento della configurazione di sicurezza di Oracle ILOM

Nel prodotto ZFS Storage Appliance è disponibile un software Oracle ILOM incorporato. Così come con altre implementazioni di Oracle ILOM, è possibile implementare alcune modifiche di configurazione rilevanti per la sicurezza per migliorare la configurazione di sicurezza predefinita del dispositivo.

- **Per proteggere l'interfaccia Oracle ILOM di ZFS Storage Appliance, effettuare le procedure riportate in Protezione di Oracle ILOM [37].**

▼ Disabilitare i servizi non necessari (ZFS Storage Appliance)

Disabilitare i servizi non necessari per supportare i requisiti operativi e di gestione della piattaforma.

Per impostazione predefinita, ZFS Storage Appliance utilizza una configurazione di rete *sicura predefinita*, in cui i servizi non essenziali sono disabilitati. Tuttavia, in base ai criteri e ai requisiti di sicurezza in uso potrebbe essere necessario abilitare o disabilitare ulteriori servizi.

1. **Eseguire il login a ZFS Storage Appliance**
   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Visualizzare l'elenco dei servizi supportati da ZFS Storage Appliance.**

   ```
   hostname:> configuration services
   ```

3. **Determinare se uno specifico servizio è abilitato.**
   Sostituire *servicename* con il nome di un servizio identificato nel Passo 2.

   ```
   hostname:> configuration services servicename get <status>
   ```

   Un servizio è abilitato se il relativo parametro state restituisce il valore `enabled`. Ad esempio:

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **Disabilitare un servizio non più necessario.**
   Impostare lo stato del servizio su disable. Ad esempio:

   ```
   hostname:> configuration services iscsi disable
   ```

▼ Disabilitare il routing dinamico

Per impostazione predefinita, ZFS Storage Appliance è configurato per eseguire il protocollo di routing dinamico.

Prima di disabilitare il servizio di routing dinamico, assicurarsi che ZFS Storage Appliance sia connesso direttamente alle reti con cui deve comunicare oppure che sia configurato per utilizzare il routing statico o un percorso predefinito. Questa operazione è necessaria per assicurare che non si verifichino perdite di connettività una volta disabilitato il routing dinamico.

1. **Eseguire il login a ZFS Storage Appliance.**
   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Disabilitare il routing dinamico.**

   ```
   hostname:> configuration services dynrouting disable
   ```

3. **Per determinare se il routing dinamico è abilitato, digitare:**

```
hostname:> configuration services dynrouting get <status>
```

Limitare l'accesso root remoto utilizzando Secure Shell

Per impostazione predefinita, ZFS Storage Appliance è configurato per consentire l'accesso amministrativo remoto all'account root utilizzando il servizio Secure Shell (SSH).

Attenersi alla procedura descritta di seguito per disabilitare l'accesso root remoto utilizzando SSH.

Una volta apportata questa modifica alla configurazione, l'account root non è più in grado di accedere al sistema utilizzando SSH. Tuttavia, l'account root è in grado di accedere a questo sistema utilizzando l'interfaccia amministrativa HTTPS.

1. **Eseguire il login a ZFS Storage Appliance.**
   Vedere Eseguire il login a ZFS Storage Appliance [83].
2. **Disabilitare l'accesso root remoto.**

   ```
   hostname:> configuration services ssh set permit_root_login=false
   ```
3. **Verificare che all'account root non sia più consentito l'accesso al sistema utilizzando SSH.**

   ```
   hostname:> configuration services ssh get permit_root_login
   ```
4. **Se l'accesso amministrativo SSH è richiesto, creare almeno un account non root.**
   Per le istruzioni, consultare *Oracle ZFS Storage Appliance Administration Guide* corrispondente alla release in esecuzione su ZFS Storage Appliance. Vedere sezione chiamata «Risorse aggiuntive per ZFS Storage Appliance» [93].

Configurare il timeout di inattività dell'interfaccia amministrativa (HTTPS)

ZFS Storage Appliance supporta la possibilità di disconnettersi ed eseguire il logout delle sessioni amministrative rimaste inattive oltre il numero di minuti predefinito. Per impostazione

predefinita, il timeout di una sessione dell'interfaccia utente del browser (HTTPS) si verifica dopo 15 minuti.

Nota - Nessun parametro equivalente applica un timeout di inattività nell'interfaccia a riga di comando SSH di ZFS Storage Appliance.

Attenersi alla procedura riportata di seguito per impostare il parametro relativo al timeout di inattività su un valore personalizzato.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Visualizzare il parametro relativo al timeout di inattività associato all'interfaccia del browser.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **Configurare il parametro di timeout.**

   Il valore `session_timeout` è specificato in minuti (10 minuti in questo esempio).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **Verificare il parametro di timeout ripetendo il Passo 2.**

▼ Disabilitare i protocolli SNMP non approvati

Per impostazione predefinita, SNMPv1 e SNMPv2c sono abilitati in ZFS Storage Appliance. ZFS Storage Appliance supporta SNMPv1/v2c in tutte le versioni supportate del prodotto. A partire dalla versione 2013.1.2, ZFS Storage Appliance supporta solo SNMPv3.

Nota - Nella versione 3 del protocollo SNMP è stato introdotto il supporto per il modello di sicurezza basato sull'utente (USM). Questa funzionalità sostituisce le stringhe community SNMP tradizionali con gli account utente effettivi che possono essere configurati con autorizzazioni, autenticazione, protocolli di riservatezza e password specifici. Per impostazione predefinita, ZFS Storage Appliance non include un nome utente o una password per l'account USM (di sola lettura) integrato. Per motivi di sicurezza, configurare le credenziali e i protocolli USM in base ai requisiti di distribuzione, gestione e monitoraggio.

Assicurarsi che le versioni non utilizzate o precedenti del protocollo SNMP siano disabilitate a meno che non venga richiesto.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Determinare se la versione del protocollo SNMP è utilizzata dal dispositivo.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **Abilitare l'uso di SNMPv3 (se disponibile).**

   L'uso di SNMPv1/v2c e SNMPv3 è ad esclusione reciproca, pertanto se si abilita SNMPv3, SNMPv1/v2c sono disabilitati.

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **Verificare la versione di SNMP.**

```
hostname:> configuration services snmp get version
version = v3
```

▼ Configurare le stringhe community SNMP

Eseguire questa procedura solo se ZFS Storage Appliance è configurato per utilizzare SNMPv1 o v2.

Poiché SNMP viene spesso utilizzato per monitorare lo stato del dispositivo, è importante che la stringa community SNMP predefinita utilizzata dal dispositivo venga sostituita con un valore definito dal cliente.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Modificare la stringa community SNMP.**

   In questo esempio, sostituire *string* con un valore conforme ai requisiti stabiliti dal Dipartimento della Difesa degli Stati Uniti relativi alla composizione delle stringhe community SNMP.

```
hostname:> configuration services snmp set community=string
community = value
```

3. **Verificare la stringa community SNMP.**

```
hostname:> configuration services snmp get community
```

Configurare le reti autorizzate SNMP

Eseguire questa procedura solo se ZFS Storage Appliance è configurato per utilizzare SNMPv1 o v2.

Per ridurre al minimo la diffusione delle informazioni di configurazione del sistema, le query SNMP devono essere accettate solo da origini di reti o di host approvate.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Configurare il parametro relativo alle reti autorizzate SNMP.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **Controllare il valore del parametro relativo alle reti autorizzate SNMP.**

   In questo esempio, l'impostazione del parametro di rete su `127.0.0.1/8` blocca effettivamente tutte le query SNMP basata sulla rete. Questo valore deve essere modificato in base alle esigenze per consentire l'utilizzo di host e reti approvati.

   Il valore `0.0.0.0/0` consente le query provenienti da qualsiasi posizione della rete.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

Limitare l'accesso alla rete di gestione

Oltre a queste procedure per il potenziamento della sicurezza, è necessario distribuire le interfacce di gestione esposte da ZFS Storage Appliance su una rete di gestione dedicata e isolata. Questa operazione consente di proteggere ZFS Storage Appliance dal traffico della rete amministrativa non autorizzato o imprevisto. L'accesso alla rete di gestione deve essere

controllato in modo rigoroso e concesso solo a quegli amministratori che richiedono questo livello di accesso.

Inoltre, è possibile configurare ZFS Storage Appliance in modo da abilitare o disabilitare l'accesso (di gestione) amministrativo su specifiche interfacce di rete. È possibile implementare questa modifica effettuando la procedura riportata di seguito.

1. **Eseguire il login a ZFS Storage Appliance.**

   Vedere Eseguire il login a ZFS Storage Appliance [83].

2. **Configurare le interfacce di rete di gestione.**

   In questo esempio, sostituire il valore *interface* con il nome dell'interfaccia di rete effettiva per la quale viene applicata questa impostazione.

```
hostname:> configuration net interfaces select interface set admin=false
```

Risorse aggiuntive per ZFS Storage Appliance

Per ulteriori linee guida relative alla sicurezza di ZFS Storage Appliance, consultare la guida alla sicurezza corrispondente alla release in esecuzione su ZFS Storage Appliance. Vedere Determinare la versione del software di ZFS Storage Appliance [84].

Le seguenti guide forniscono informazioni aggiuntive sulle funzioni di sicurezza, sulle funzionalità e sulle opzioni di configurazione del prodotto:

- *Guida sulla sicurezza di Oracle ZFS Storage Appliance* (Release 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Guida sulla sicurezza di Oracle ZFS Storage Appliance* (Release 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Guida sulla sicurezza di Oracle ZFS Storage Appliance* (Release 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

Protezione degli Exadata Storage Server

Gli Exadata Storage Server (storage server) sono il componente essenziale di SuperCluster. Ogni storage server viene fornito preinstallato e integrato come parte di SuperCluster M7 con tutti i relativi componenti di calcolo, di storage e software.

Nota - È consentito solo apportare modifiche alla configurazione tramite l'applicazione di metodi, patch o aggiornamenti approvati. Il software degli storage server non può essere modificato in nessun altro modo.

SuperCluster M7 presenta un minimo di tre storage server. È possibile installare ulteriori storage server nel rack principale di SuperCluster e nei rack di espansione facoltativi. È necessario proteggere ogni singolo storage server.

In questi argomenti viene descritto come proteggere gli storage server.

▼ Eseguire il login al sistema operativo degli storage server

- **Nella rete di gestione, eseguire il login a uno degli storage server come `celladmin`.**
  Per la password predefinita, vedere sezione chiamata «Account e password predefiniti» [96].

```
# ssh celladmin@Storage_Server_IP_address
```

Account e password predefiniti

Nella tabella sono elencati gli account predefiniti e le password predefinite degli storage server.

Nome account	Tipo	Password predefinita	Descrizione
`root`	Amministratore	`welcome1`	Usato per accedere al sistema operativo degli storage server, per eseguire attività amministrative generali e per aggiornare il software degli storage server.
`celladmin`	Amministratore cella	`welcome`	Usato per eseguire l'installazione e la configurazione degli storage server. Inoltre, tutti i servizi di storage della piattaforma operano con questo account.
`cellmonitor`	Monitoraggio	`welcome`	Usato solo a scopo di monitoraggio. Questo account utilizza una shell limitata; ciò assicura che la configurazione e gli oggetti che risiedono nello storage server non possano essere modificati da questo account.

▼ Modifica delle password degli storage server

Per l'elenco degli account predefiniti e delle password predefinite, vedere sezione chiamata «Account e password predefiniti» [96].

Nota - Quando si modifica una password di qualsiasi componente SuperCluster gestito da Oracle Engineered Systems Hardware Manager, come il sistema operativo degli Exadata Storage Server, è necessario anche aggiornare la password in Oracle Engineered Systems Hardware Manager. Per ulteriori informazioni, consultare la *Guida all'amministrazione di Oracle SuperCluster serie M7*.

---

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Modificare una password predefinita utilizzando uno dei metodi descritti di seguito.**

   - **Modificare la password di un account nel server a cui è stato eseguito il login.**

     ```
     # passwd account_name
     ```

   - **Modificare la password di un account in tutti gli storage server.**

`cell_group` è un file di testo semplice in cui sono elencati i nomi host di tutti gli storage server (uno per riga).

Nell'esempio riportato di seguito, sostituire i seguenti elementi della riga di comando:

- *new_password*: sostituire con la nuova password conforme ai criteri del sito;
- *account_name*: sostituire con il nome dell'account Oracle Linux.

```
# dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
```

Determinare la versione del software degli Exadata Storage Server

1. **Eseguire il login a uno degli storage server.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Digitare questo comando.**

   In questo esempio, la versione del software degli storage server è 12.1.2.1.1.150316.2.

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   Per aggiornare la versione del software, installare la più recente SuperCluster Quarterly Full Stack Download Patch disponibile in My Oracle Support all'indirizzo `https://support.oracle.com`.

Nota - Per SuperCluster, ulteriori restrizioni possono limitare le versioni del software che è possibile usare e la modalità di aggiornamento di tali versioni. In questi casi, contattare il rappresentante Oracle.

Servizi di rete esposti predefiniti (storage server)

Nome servizio	Protocollo	Porta	Descrizione
SSH	TCP	22	Usato dal servizio Secure Shell integrato nel software degli storage server per fornire accesso amministrativo al sistema tramite un'interfaccia CLI. Per impostazione predefinita, il server Secure Shell è configurato per rispondere alle richieste di connessione solo sulle reti di gestione (NET 0) e IB (BONDIB0).

Il server di storage comunica anche con Oracle Database Domains in SuperCluster tramite il protocollo RDSv3 (Reliable Datagram Sockets) su interfacce RDMA (Remote Direct Memory Access). Questa comunicazione point-to-point non utilizza TCP/IP ed è limitata alla partizione di rete IB interna in cui risiedono sia i domini Oracle Database di SuperCluster che gli storage server.

Rafforzamento della configurazione di sicurezza degli storage server

Nota - Lo storage server include un Oracle ILOM integrato come parte del prodotto. Come per altre implementazioni di Oracle ILOM, è possibile implementare modifiche pertinenti la configurazione di sicurezza per migliorare la configurazione di sicurezza predefinita del dispositivo. Per ulteriori informazioni, vedere Protezione di Oracle ILOM [37].

In questi argomenti viene descritto come rafforzare la sicurezza degli storage server.

Limitazioni della configurazione di sicurezza

La utility `host_access_control` è l'unico metodo consentito e supportato per implementare le modifiche alla configurazione di sicurezza degli storage server. In base alla nota del supporto Oracle 1068804.1, non è consentito apportare modifiche manuali alla configurazione di questi

dispositivi. Inoltre, prima di utilizzare questo strumento, è necessario ottenere dal supporto Oracle SuperCluster l'approvazione esplicita per la modifica della configurazione di sicurezza degli storage server. Per richiedere l'approvazione, aprire una richiesta di servizio per il supporto Oracle.

Il comando `host_access_control`, disponibile dalla versione 11.2.3.3.0 del software di Exadata, viene usato per implementare un set limitato di impostazioni relative all'accesso e alla configurazione di sicurezza.

- Limitazione dell'accesso root remoto.
- Limitazione dell'accesso alla rete per determinati account.
- Implementazione di criteri per la durata e la complessità delle password.
- Implementazione di messaggi di avvio di avvertenza al login.
- Definizione di criteri per il blocco dell'account e il timeout della sessione.

Visualizzare le configurazioni di sicurezza disponibili con `host_access_control`

Per visualizzare gli elementi disponibili nella utility `host_access_control`, attenersi alla procedura riportata di seguito.

1. **Eseguire il login al sistema operativo degli storage server.**
   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **(Facoltativo) Per ulteriori informazioni, visualizzare la guida di `host_access_control`.**

```
# /opt/oracle.cellos/host_access_control --help
```

Configurare una password per il boot loader di sistema

È possibile configurare gli storage server in modo che richiedano una password per il boot loader di sistema ogni volta che un amministratore tenta di accedere all'editor dei boot loader (GRUB) o all'interfaccia dei comandi.

1. **Eseguire il login allo storage server come `celladmin`.**
   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Configurare una password per il boot loader di sistema.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **Verificare l'impostazione.**

   Se il comando restituisce un valore simile a quello dell'esempio, significa che la password del boot loader è stata installata.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

Disabilitare l'accesso alla console di sistema di Oracle ILOM

Ogni storage server include un Oracle ILOM integrato per consentire il monitoraggio e la gestione remoti. Oracle ILOM può essere utilizzato anche per fornire l'accesso remoto alla console di sistema degli storage server.

Eseguire la procedura riportata di seguito se si desidera disabilitare l'accesso agli storage server tramite Oracle ILOM.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Disabilitare l'accesso alla console di sistema di Oracle ILOM.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **Verificare l'impostazione.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

Limitare l'accesso remoto di `root` tramite SSH

Per impostazione predefinita, all'utente `root` è consentito accedere in remoto a ciascuno degli storage server.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Disabilitare l'accesso remoto di `root` tramite SSH.**

   ```
   # /opt/oracle.cellos/host_access_control rootssh --lock
   ```

3. **Verificare l'impostazione.**

   ```
   # /opt/oracle.cellos/host_access_control rootssh --status
   ```

Configurare il blocco degli account di sistema

Per impostazione predefinita, gli storage server sono configurati per bloccare gli account di sistema dopo cinque tentativi di autenticazione consecutivi non riusciti.

Per modificare questa soglia, attenersi alla procedura descritta di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Modificare la soglia.**

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti, specificare il valore `3`. Se necessario, sostituire questo valore con uno conforme ai criteri del sito locale.

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --deny 3
   ```

3. **Verificare l'impostazione.**

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
   ```

Configurare le regole di complessità delle password

Per impostazione predefinita, gli storage server non implementano limitazioni significative che regolano la complessità delle password degli account di sistema.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Definire un criterio di complessità delle password.**

   Sintassi:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

   Sostituire *N0,N1,N2,N3,N4* con un set di cinque valori separati da virgole. Questi cinque valori impostano in modo collettivo il criterio di complessità delle password effettivo. I valori, elencati anche nella pagina man `passwdqc.conf(5)`, sono descritti di seguito.

   - *N0*: usato per le password costituite da un'unica classe di caratteri (valori numerici, caratteri minuscoli, maiuscoli e speciali). In generale, questo parametro è impostato su `disabled` perché le password semplici non sono sicure.
   - *N1*: usato per le password costituite da due classi di caratteri che non soddisfano i requisiti per una passphrase. Per poter applicare questa regola, è necessario che la password abbia una lunghezza minima di N1 caratteri.
   - *N2*: usato per le password costituite da una passphrase. Per poter applicare questa regola, è necessario che la password abbia una lunghezza minima di N2 caratteri e soddisfi i requisiti di passphrase.
   - *N3*: usato per le password costituite da almeno tre classi di caratteri. Per poter applicare questa regola, è necessario che la password abbia una lunghezza minima di N3 caratteri.
   - *N4*: usato per le password costituite da almeno quattro classi di caratteri. Per poter applicare questa regola, è necessario che la password abbia una lunghezza minima di *N4* caratteri.

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti, impostare i parametri *N0,N1,N2,N3,N4* su `disabled,disabled,disabled,disabled,15`. Ciò assicura che le uniche password che vengono accettate sono costituite da almeno quattro classi di caratteri (maiuscoli, minuscoli, numerici e speciali) e da almeno 15 caratteri.

   Nota - Le lettere maiuscole all'inizio della password e i valori numerici alla fine dalla password non vengono contati quando si calcola il numero di classi di caratteri.

   Ad esempio, per impostare una regola di complessità delle password che soddisfi i requisiti del Dipartimento della Difesa degli Stati Uniti, digitare:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **Verificare lo stato corrente di questa impostazione.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

Configurare un criterio di cronologia delle password

Per impostazione predefinita, gli storage server definiscono un criterio di cronologia delle password che impedisce agli utenti di riutilizzare le ultime dieci (10) password.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Visualizzare l'impostazione corrente.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **Modificare la cronologia delle password.**

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti e PCI-DSS, impostare il criteri di cronologia delle password su `5`. Ciò assicura che un account non potrà riutilizzare nessuna delle precedenti cinque password assegnate. Se necessario, sostituire questo valore con uno conforme ai criteri del sito locale.

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --remember 5
   ```

4. **Per verificare l'impostazione, ripetere il Passo 2.**

Configurare un ritardo del blocco per autenticazione non riuscita

Per impostazione predefinita, gli storage server implementano un criterio per cui un account di sistema viene bloccato per 10 minuti dopo ogni singolo tentativo di autenticazione non riuscito.

Per modificare questa soglia, attenersi alla procedura descritta di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Visualizzare l'impostazione corrente.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **Modificare la soglia.**

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti, impostare il valore su 4 (secondi). Se necessario, sostituire questo valore con uno conforme ai criteri del sito locale.

   ```
   # /opt/oracle.cellos/host_access_control pam-auth --lock 4
   ```

4. **Per verificare l'impostazione, ripetere il Passo 2.**

▼ Configurare i criteri di controllo per la durata delle password

Gli storage server supportano diversi tipi di controlli di durata delle password, inclusi i parametri per controllare il numero massimo di giorni di utilizzo di una password, il numero minimo di giorni tra le modifiche della password e il numero di giorni precedenti alla scadenza della password in cui l'utente viene avvisato.

Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti e PCI-DSS, usare i valori specificati dal Dipartimento della Difesa degli Stati Uniti descritti nella tabella riportata di seguito.

Criterio	Valore predefinito Oracle	Valore Dipartimento della Difesa
Durata massima della password	90 giorni	60 giorni
Durata minima della password	1 giorno	1 giorno
Lunghezza minima della password	8 caratteri	15 caratteri
Avvertenza di scadenza della password	7 giorni	7 giorni

Per modificare uno qualsiasi di questi parametri, attenersi alla procedura descritta di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Visualizzare le impostazioni correnti.**

   ```
   # /opt/oracle.cellos/host_access_control password-policy --status
   ```

3. **Configurare i seguenti criteri in base ai criteri delle password del sito.**

- **Per modificare il parametro della durata massima della password, digitare:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

- **Per modificare il parametro della durata minima della password, digitare:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

- **Per modificare il parametro della lunghezza minima della password, digitare:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

- **Per modificare il parametro dell'avvertenza di scadenza della password, digitare:**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **Per verificare le impostazioni, ripetere il Passo 2.**

Configurare il timeout di inattività dell'interfaccia amministrativa (shell di login)

Lo storage server supporta la funzionalità di interruzione delle sessioni amministrative che risultano inattive per un numero di secondi superiore a quello predefinito.

Per definire il timeout di inattività dell'interfaccia amministrativa per una shell di login degli account di sistema, attenersi alla procedura riportata di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**
   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Visualizzare l'impostazione corrente.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **Definire il timeout di inattività dell'interfaccia amministrativa.**
   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti e PCI-DSS, specificare il valore `900` (secondi). Se necessario, sostituire questo valore con uno conforme ai criteri del sito locale.

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **Per verificare l'impostazione, ripetere il Passo 2.**

Configurare il timeout di inattività dell'interfaccia amministrativa (Secure Shell)

Lo storage server supporta la funzionalità di interruzione delle sessioni SSH amministrative che risultano inattive per un numero di secondi superiore a quello predefinito.

Per definire il timeout di inattività dell'interfaccia amministrativa per una sessione SSH, attenersi alla procedura riportata di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Visualizzare l'impostazione corrente.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
   ```

3. **Definire il timeout di inattività dell'interfaccia amministrativa per una sessione SSH.**

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti, specificare il valore `900` (secondi). Se necessario, sostituire questo valore con uno conforme ai criteri del sito locale.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **Per verificare l'impostazione, ripetere il Passo 2.**

Configurare un messaggio di avvio di avvertenza al login (storage server)

Lo storage server supporta la funzionalità di visualizzazione di messaggi specifici del cliente prima che un utente esegua la corretta autenticazione al sistema.

Per definire un messaggio di avvio di avvertenza al login, precedente all'autenticazione, attenersi alla procedura descritta di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**

   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Determinare l'impostazione corrente.**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **Creare un file di testo che contenga il messaggio di login di avvertenza approvato.**

4. **Definire un messaggio di avvio di avvertenza al login, precedente all'autenticazione.**

   Per conformità ai requisiti di sicurezza del Dipartimento della Difesa degli Stati Uniti, sostituire *filename* con il percorso e il nome del file che contiene il messaggio di avvio di avvertenza al login approvato.

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **Per verificare l'impostazione, ripetere il Passo 2.**

Limitazione dell'accesso della rete remota

È possibile limitare l'accesso della rete remota in entrata agli storage server tramite l'implementazione di un set di regole di filtro. È anche possibile ottimizzare l'accesso della rete attraverso la definizione di un set di regole personalizzate.

Per limitare l'accesso remoto, usare le seguenti procedure.

- sezione chiamata «Isolamento della rete di gestione dello storage server» [108]
- Limitare l'accesso della rete remota [108]

Isolamento della rete di gestione dello storage server

Lo storage server viene distribuito su una rete di gestione dedicata e isolata. Ciò consente di proteggere lo storage server dal traffico di rete non autorizzato o involontario. L'accesso alla rete di gestione deve essere strettamente controllato e può essere concesso solo agli amministratori che richiedono questo livello di accesso.

▼ Limitare l'accesso della rete remota

Sono disponibili diverse modalità per limitare l'accesso della rete remota negli storage server. Per limitare l'accesso della rete in entrata agli storage server, è possibile implementare un set di regole di filtro dall'alto verso il basso che definiscono l'accesso in base all'account e all'origine dell'utente. È inoltre possibile definire un set di regole personalizzate per consentire o negare l'accesso in base ai requisiti del Dipartimento della Difesa degli Stati Uniti e PCI-DSS.

Attenzione - Prestare attenzione quando si implementano criteri non predefiniti per assicurare che l'accesso al sistema non subisca interruzioni. Quando si aggiungono nuove singole regole, le modifiche diventano effettive immediatamente.

Per implementare un set di regole, attenersi alla procedura descritta di seguito.

1. **Eseguire il login allo storage server come `celladmin`.**
   Vedere Eseguire il login al sistema operativo degli storage server [95].

2. **Esaminare il set di regole attivo.**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **Esportare il set di regole corrente in un file e salvarlo come una copia di backup.**
   Questo comando esporta il set di regole in un file di testo ASCII:

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Per configurare il set di regole eseguire uno o più comandi tra quelli riportati di seguito, in base al metodo che si desidera usare per creare il set di regole.**

   - **Per implementare un set di regole aperto che rimuove le limitazioni per la rete in entrata, digitare:**

```
# /opt/oracle.cellos/host_access_control access --open
```

- **Per implementare un set di regole chiuso che consente solo l'accesso in entrata tramite SSH, digitare:**

```
# /opt/oracle.cellos/host_access_control access --close
```

- **Per modificare il set di regole esistente, digitare:**

  Esportare il set di regole corrente in un file di testo ASCII:

```
# /opt/oracle.cellos/host_access_control access-export --file filename
```

  Usare un editor per modificare il file di testo e configurare il set di regole.

  Importare il set di regole dal file di testo, ignorando il set di regole esistente:

```
# /opt/oracle.cellos/host_access_control access-import --file filename
```

- **Per aggiungere singolarmente regole specifiche:**

  Questo metodo include il consenso e la negazione per l'accesso in base ai seguenti parametri:

  - **nome utente**: valori validi sono la parola chiave `all` oppure uno o più nomi utente di account locali validi.
  - **origine**: valori validi sono la parola chiave `all` oppure singole voci che descrivono l'origine dell'accesso al sistema e che includono la console, la console virtuale, Oracle ILOM, l'indirizzo IP, l'indirizzo di rete, il nome host o il dominio DNS.

  In questo esempio, l'accesso allo storage server viene concesso all'utente `celladmin` quando la connessione viene avviata dall'host `trusted.example.org` o da qualsiasi host all'interno del dominio `.trusted.domain.com`.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

Risorse aggiuntive degli storage server

Consultare il documento Exadata Database Machine Security Guide all'indirizzo http://docs.oracle.com/cd/E50790_01/welcome.html.

Protezione degli switch IB ed Ethernet

Lo switch Oracle Sun Data Center InfiniBand Switch 36 utilizzato da SuperCluster fornisce l'elemento di rete di base per un backplane ad alte prestazioni, altamente scalabile e completamente ridondante in tutti i componenti interni.

Gli switch IB collegano i server di calcolo, le celle di storage e ZFS Storage Appliance. Negli switch IB è presente un firmware Oracle ILOM incorporato che fornisce funzionalità di gestione e monitoraggio avanzate. In particolare, Oracle ILOM consente il monitoraggio e il controllo degli utenti, dell'hardware, dei servizi, dei protocolli e di altri parametri di configurazione.

La configurazione minima di SuperCluster M7 prevede due switch IB. Se necessario, è possibile installare ulteriori switch IB per configurazioni più grandi. È necessario proteggere ogni switch IB.

Negli argomenti riportati di seguito viene descritto come proteggere gli switch IB in SuperCluster M7:

▼ Eseguire il login a uno switch IB

Nella procedura seguente viene descritto come eseguire il login all'interfaccia Oracle ILOM sullo switch, in cui viene eseguita la maggior parte delle attività amministrative.

- **Sulla rete di gestione, eseguire il login a Oracle ILOM sullo switch IB come `ilom-admin`.**

  Per le password predefinite, vedere sezione chiamata «Account e password predefiniti (switch IB)» [113].

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ Determinare la versione del firmware degli switch IB

Per utilizzare le funzioni, le funzionalità e i miglioramenti della sicurezza più recenti, assicurarsi che lo switch IB sia aggiornato con la versione firmware più recente supportata.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Visualizzare la versione del firmware.**

   In questo esempio, la versione dello switch IB è la `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

Per aggiornare la versione del firmware dello switch IB, installare la versione più recente di SuperCluster Quarterly Full Stack Download Patch disponibile in My Oracle Support all'indirizzo `https://support.oracle.com`.

Nota - Alcune limitazioni aggiuntive definite per SuperCluster M7 potrebbero limitare le versioni del software degli switch IB utilizzabili. Le limitazioni indicano anche le modalità di aggiornamento del firmware. In questi casi, contattare il rappresentante Oracle.

Account e password predefiniti (switch IB)

Nome account	Tipo	Password predefinita	Descrizione
`root`	Amministratore	`welcome1`	Utilizzato per accedere al sistema operativo degli switch IB. Questo account non viene in genere utilizzato per `ilom-admin`, `ilom-operator` o per gli account definiti dal cliente.
`ilom-admin`	Amministratore	`ilom-admin`	Utilizzato per eseguire funzioni amministrative sul software Oracle ILOM incorporato, eseguire aggiornamenti del software, configurare utenti e servizi ed eseguire funzioni di gestione dei fabric e di diagnostica sugli switch IB.
`ilom-operator`	Operatore	`ilom-operator`	Utilizzato solo per le funzioni di diagnostica dei fabric IB e di monitoraggio di Oracle ILOM.
`nm2user`	Sola lettura	`changeme`	Questo account dispone solo dei privilegi di lettura per l'interfaccia amministrativa a riga di comando dello switch IB. Questo account viene spesso utilizzato da Oracle Enterprise Manager per sopportare il monitoraggio dell'hardware e del software dello switch.

▼ Modificare le password `root` e `nm2user`

Lo switch IB gestisce gli account di sistema in due posizioni. Gli account `root` e `nm2user` vengono configurati e visualizzati dal sistema operativo di base dello switch. L'operazione di aggiunta, rimozione o modifica degli account non è supportata in questo layer. Tuttavia, è necessario modificare le password predefinite.

Per altri account e password, vedere Modificare le password degli switch IB (Oracle ILOM) [114].

Lo switch IB non è in grado di definire o applicare regole di complessità, scadenza, cronologia o di altro tipo per le password. È necessario assicurarsi che le password assegnate siano conformi ai requisiti di complessità delle password definiti dal Dipartimento della Difesa degli Stati Uniti e che i processi vengano implementati per garantire l'aggiornamento delle password in conformità con le norme stabilite dal Dipartimento della Difesa degli Stati Uniti.

Per ulteriori informazioni sulla gestione degli account degli switch IB, incluse le modalità di creazione di nuovi account, di assegnazione delle autorizzazioni agli account esistenti o di rimozione degli account, consultare i manuali *Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide* e *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*. Vedere sezione chiamata «Risorse aggiuntive per gli switch IB» [121].

Nota - Quando una password viene modificata per un componente di SuperCluster gestito da Oracle Engineered Systems Hardware Manager (ad esempio, gli switch IB), è necessario aggiornare la password anche in Oracle Engineered Systems Hardware Manager. Per ulteriori informazioni, consultare la *Guida all'amministrazione di Oracle SuperCluster serie M7*.

1. **Eseguire il login allo switch IB come `root`.**

```
# ssh root@IB_Switch_IP_address
```

Per le password predefinite, vedere sezione chiamata «Account e password predefiniti (switch IB)» [113].

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

```
$ passwd root
```

3. **Modificare la password `nm2user`.**

```
$ passwd nm2user
```

Modificare le password degli switch IB (Oracle ILOM)

Lo switch IB gestisce gli account di sistema in due posizioni. In questa sezione viene descritto come modificare le password nell'interfaccia Oracle ILOM dello switch IB. Per altri account e password, vedere Modificare le password `root` e `nm2user` [113].

Gli account degli switch IB predefiniti e gli account definiti dal cliente vengono gestiti mediante il software Oracle ILOM incorporato sugli switch IB.

Per visualizzare gli account e modificare le password, effettuare la procedura riportata di seguito.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

Vedere Eseguire il login a uno switch IB [111].

Per le password predefinite, vedere sezione chiamata «Account e password predefiniti (switch IB)» [113].

2. **Visualizzare gli account Oracle ILOM configurati sullo switch IB.**

```
-> show /SP/users
```

3. **Modificare la password per l'account `ilom-admin`.**

```
-> set /SP/users/ilom-admin password=password
```

Isolamento della rete sugli switch IB

L'interfaccia di gestione dello switch IB viene distribuita su una rete di gestione isolata dedicata. In questo modo, lo switch IB viene protetto dal traffico di rete non autorizzato o imprevisto.

L'accesso a questa rete di gestione deve essere controllato in modo rigoroso e concesso solo a quegli amministratori che richiedono questo livello di accesso.

Servizi di rete esposti predefiniti (switch IB)

Nome servizio	Protocollo	Porta	Descrizione
SSH	TCP	22	Utilizzato dal servizio Secure Shell integrato per abilitare l'accesso amministrativo allo switch IB utilizzando un'interfaccia CLI.
HTTP (BUI)	TCP	80	Utilizzato dal servizio HTTP integrato per abilitare l'accesso amministrativo allo switch IB utilizzando un'interfaccia del browser. Sebbene TCP/80 venga in genere utilizzato per l'accesso con testo in chiaro, per impostazione predefinita lo switch IB reindirizza automaticamente le richieste in entrata alla versione sicura di questo servizio in esecuzione su TCP/443.
NTP	UDP	123	Utilizzato dal servizio NTP (Network Time Protocol) integrato (solo client) che consente di sincronizzare il clock di sistema locale con una o più origini temporali esterne.
SNMP	UDP	161	Utilizzato dal servizio SNMP integrato per fornire un'interfaccia di gestione che consente di monitorare lo stato dello switch IB e le notifiche trap ricevute.
HTTPS (BUI)	TCP	443	Utilizzato dal servizio HTTPS integrato per abilitare l'accesso amministrativo allo switch IB su un canale (SSL/TLS) cifrato utilizzando un'interfaccia del browser.
IPMI	TCP	623	Utilizzato dal servizio IPMI (Intelligence Platform Management Interface) integrato per fornire un'interfaccia del computer per varie funzioni di monitoraggio e gestione. Non disabilitare questo servizio poiché viene utilizzato da Oracle Enterprise Manager Ops Center per raccogliere dati di inventario hardware, descrizioni delle FRU, informazioni sui sensori hardware e informazioni sullo stato dei componenti hardware.

Nome servizio	Protocollo	Porta	Descrizione
ServiceTag	TCP	6481	Utilizzato dal servizio Oracle ServiceTag. Si tratta di un protocollo di ricerca automatica di Oracle utilizzato per identificare i server e semplificare le richieste di servizio. Questo servizio viene utilizzato da prodotti quali Oracle Enterprise Manager Ops Center per trovare il software dello switch IB e per l'integrazione con altre soluzioni di servizio automatico Oracle.

Potenziamento della configurazione degli switch IB

Negli argomenti riportati di seguito viene descritto come proteggere lo switch IB mediante varie impostazioni di configurazione.

▼ Disabilitare i servizi non necessari (switch IB)

Disabilitare i servizi non necessari per supportare i requisiti operativi e di gestione della piattaforma. Per impostazione predefinita, lo switch IB include una configurazione di rete sicura predefinita, in cui i servizi non essenziali sono già disabilitati. Tuttavia, in base ai criteri e ai requisiti di sicurezza del cliente, potrebbe essere necessario disabilitare ulteriori servizi.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Determinare l'elenco dei servizi supportati dallo switch IB.**

   ```
   -> show /SP/services
   ```

3. **Determinare se uno specifico servizio è abilitato.**

   Sostituire *servicename* con il nome di un servizio identificato nel Passo 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

La maggior parte dei servizi riconosce e utilizza il parametro `servicestate` per stabilire se il servizio è abilitato o disabilitato. Tuttavia, esistono alcuni servizi, come `servicetag`, `ssh`, `sso` e `wsman`, che utilizzano un parametro denominato `state`. Indipendentemente dal parametro effettivo utilizzato, un servizio è abilitato se il parametro state del servizio restituisce il valore `enabled`, come illustrato negli esempi seguenti:

```
-> show /SP/services/https servicestate
/SP/services/https
Properties:
servicestate = enabled
```

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

4. **Per disabilitare un servizio non più necessario, impostarne lo stato su `disabled`.**

```
-> set /SP/services/http servicestate=disabled
```

5. **Determinare se uno di questi servizi deve essere disabilitato.**

   A seconda degli strumenti e dei metodi utilizzati, è possibile disabilitare i servizi del browser HTTP e HTTPS se non sono necessari o non vengono utilizzati. Tipo:

```
-> set /SP/services/http servicestate=disabled
-> set /SP/services/http secureredirect=disabled
-> set /SP/services/https servicestate=disabled
```

   - Interfaccia amministrativa del browser (HTTP, HTTPS):
     - `->` **set /SP/services/http servicestate=disabled**
     - `->` **set /SP/services/http secureredirect=disabled**
     - `->` **set /SP/services/https servicestate=disabled**

Configurare il reindirizzamento HTTP a HTTPS (switch IB)

Per impostazione predefinita, lo switch IB è configurato per reindirizzare le richieste HTTP in entrata al servizio HTTPS in modo da garantire che tutte le comunicazioni basate sul browser tra lo switch e l'amministratore siano cifrate.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Verificare che il reindirizzamento sicuro sia abilitato.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Se l'impostazione predefinita è stata modificata, è possibile abilitare il reindirizzamento sicuro.**

```
-> set /SP/services/http secureredirect=enabled
```

Disabilitare i protocolli SNMP non approvati (switch IB)

Per impostazione predefinita, i protocolli SNMPv1, SNMPv2c e SNMPv3 sono tutti abilitati per il servizio SNMP utilizzato per monitorare e gestire lo switch IB. Assicurarsi che le versioni precedenti del protocollo SNMP rimangano disabilitate a meno che non venga richiesto.

Nota - Nella versione 3 del protocollo SNMP è stato introdotto il supporto per il modello di sicurezza basato sull'utente (USM). Questa funzionalità sostituisce le stringhe community SNMP tradizionali con gli account utente effettivi che possono essere configurati con autorizzazioni, autenticazione, protocolli di riservatezza e password specifici. Per impostazione predefinita, lo switch IB non include account USM. Configurare gli account USM SNMPv3 in base ai requisiti personali di distribuzione, gestione e monitoraggio.

---

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Determinare lo stato di ciascun protocollo SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **Se necessario, disabilitare SNMPv1 e SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

Configurare le stringhe community SNMP (switch IB)

Questa procedura è applicabile solo se SNMP v1 o SNMPv2c è abilitato e configurato per l'uso.

Poiché SNMP viene spesso utilizzato per monitorare lo stato del dispositivo, è importante che le stringhe community SNMP predefinite utilizzate dal dispositivo vengano sostituite con valori definiti dal cliente.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**
   Vedere Eseguire il login a uno switch IB [111].

2. **Creare una nuova stringa community SNMP.**
   In questo esempio, sostituire questi elementi nella riga di comando:

   - *string*: sostituire questo elemento con un valore definito dal cliente conforme ai requisiti stabiliti dal Dipartimento della Difesa degli Stati Uniti relativi alla composizione delle stringhe community SNMP.
   - *access*: sostituire questo elemento con `ro` o `rw`, a seconda che si tratti di una stringa di accesso di sola lettura o di lettura-scrittura.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Dopo aver creato nuove stringhe community, è necessario rimuovere quelle predefinite.

3. **Rimuovere le stringhe community SNMP predefinite.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **Verificare le stringhe community SNMP.**

   ```
   -> show /SP/services/snmp/communities
   ```

Sostituire i certificati autofirmati predefiniti (switch IB)

Gli switch IB utilizzano i certificati autofirmati per consentire l'uso immediato del protocollo HTTPS. È consigliabile sostituire i certificati autofirmati con certificati approvati per l'ambiente in uso e firmati da un'autorità di certificazione riconosciuta.

Lo switch IB supporta vari metodi che possono essere utilizzati per accedere al certificato e alla chiave privata SSL/TLS, tra cui HTTPS, HTTP, SCP, FTP e TFTP, e per copiare le informazioni direttamente in un'interfaccia del browser Web. Per ulteriori informazioni, consultare il documento *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*. Vedere sezione chiamata «Risorse aggiuntive per gli switch IB» [121].

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Determinare se lo switch IB sta utilizzando un certificato autofirmato predefinito.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Installare il certificato dell'organizzazione.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

Configurare il timeout delle sessioni CLI amministrative (switch IB)

Gli switch IB supportano la possibilità di disconnettersi ed eseguire il logout delle sessioni CLI amministrative rimaste inattive oltre il numero di minuti predefinito.

Per impostazione predefinita, il timeout dell'interfaccia CLI si verifica dopo 15 minuti.

1. **Eseguire il login a uno switch IB come `ilom-admin`.**

   Vedere Eseguire il login a uno switch IB [111].

2. **Verificare il parametro relativo al timeout di inattività associato all'interfaccia CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Impostare il parametro relativo al timeout di inattività.**

Sostituire *n* con un valore specificato in minuti.

```
-> set /SP/cli timeout=n
```

Risorse aggiuntive per gli switch IB

Per ulteriori informazioni sulle procedure di sicurezza e amministrative per gli switch IB, fare riferimento alla libreria della documentazione di Sun Datacenter InfiniBand Switch 36 all'indirizzo http://docs.oracle.com/cd/E36265_01.

▼ Modificare la password dello switch Ethernet

Nota - Quando una password viene modificata per un componente di SuperCluster gestito da Oracle Engineered Systems Hardware Manager (ad esempio, lo switch Ethernet), è necessario aggiornare la password anche in Oracle Engineered Systems Hardware Manager. Per ulteriori informazioni, consultare la *Guida all'amministrazione di Oracle SuperCluster serie M7*.

1. **Collegare un cavo seriale dalla console dello switch Ethernet a un laptop o a un dispositivo simile.**

   La velocità della porta seriale predefinita è pari a 9600 baud, 8 bit, nessuna parità, 1 bit di stop e nessun handshake.

   ```
   sscsw-adm0 con0 is now available
   Press RETURN to get started.
   ```

2. **Impostare lo switch sulla modalità di abilitazione.**

   ```
   sscsw-adm0> enable
   ```

3. **Impostare la password.**

   ```
   sscsw-adm0# configure terminal
   Enter configuration commands,one per line.End with CNTL/Z.
   sscsw-adm0(config)# enable password *******
   sscsw-adm0(config)# enable secret *******
   sscsw-adm0(config)# end
   sscsw-adm0# write memory
   *Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
   console
   ```

```
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Salvare la configurazione.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Uscire dalla sessione.**

```
sscsw-adm0# exit
```

6. **Scollegare il laptop dallo switch Ethernet.**

Audit della conformità

Usare la utility di conformità di Oracle Solaris per valutare la conformità di un sistema rispetto a un benchmark noto e generare i relativi report.

Il comando `compliance` di Oracle Solaris associa i requisiti di un benchmark all'output del codice, di un file o di un comando che verifica la conformità a un requisito specifico. Attualmente Oracle SuperCluster supporta due profili benchmark di conformità alla sicurezza:

- **Recommended**: profilo basato sul benchmark di Center of Internet Security.
- **PCI-DSS**: profilo che verifica i requisiti di conformità a PCI DSS (Payment Card Industry Data Security Standard).

Questi profili associano i controlli di sicurezza ai requisiti di conformità; i report sulla conformità che ne derivano consentono di ridurre in modo significativo i tempi di audit. Inoltre, la funzione della conformità offre guide che contengono le motivazioni per ciascun controllo di sicurezza e la procedura per correggere un controllo non riuscito. Le guide possono risultare utili per la formazione e come linee guida per i test futuri. Per impostazione predefinita, durante l'installazione vengono create le guide per ciascun profilo di sicurezza. L'amministratore di SuperCluster Solaris può aggiungere o modificare un benchmark e creare una nuova guida.

In questi argomenti viene descritto come eseguire report sulla conformità e viene descritta la conformità a FIPS-140.

▼ Generare una valutazione della conformità

Per eseguire questa procedura, è necessario che all'utente sia assegnato il profilo di diritti per l'installazione del software (Software Installation) che consente di aggiungere pacchetti al sistema. È necessario che all'utente siano assegnati i diritti amministrativi per la maggior parte dei comandi di conformità.

1. **Installare il pacchetto della conformità.**

```
# pkg install compliance
```

Il seguente messaggio indica che il pacchetto è installato.

```
No updates necessary for this image.
```

Per ulteriori informazioni, vedere la pagina man `pkg(1)`.

Nota - Installare il pacchetto in ogni zona in cui si pianifica di eseguire i test di conformità.

2. **Visualizzare i benchmark, i profili e le eventuali valutazioni precedenti disponibili.**

In questo esempio, sono disponibili due benchmark.

- **`pci-dss`**: include un profilo denominato `Solaris_PCI-DSS`
- **`solaris`**: include due profili denominati `Baseline` e `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Generare una valutazione della conformità.**

Eseguire il comando `compliance` con la seguente sintassi:

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	Specifica un determinato benchmark. Se non specificato, per impostazione predefinita viene utilizzato il valore `solaris`.
`-p`	Specifica il profilo. Il nome del profilo fa distinzione tra maiuscole e minuscole. Se non specificato, per impostazione predefinita viene utilizzato il primo profilo.

Esempi:

- Uso del profilo `Recommended`.

```
# compliance assess -b solaris -p Recommended
```

Il comando crea una directory in `/var/share/compliance/assessments` che contiene la valutazione in tre file: un file di log, un file XML e un file HTML.

- Uso del profilo PCI-DSS.

```
# compliance assess -b pci-dss
```

Nota - Il benchmark `pci-dss` dispone di un solo profilo, pertanto l'opzione per specificare il profilo (`-p`) non è necessaria nella riga di comando.

4. **Verificare che i file della conformità siano stati creati.**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

Nota - Se si esegue di nuovo lo stesso comando `compliance`, i file non vengono sostituiti. È necessario rimuovere i file prima di riutilizzare la directory di una valutazione.

5. **(Facoltativo) Creare un report personalizzato.**

   È possibile eseguire report personalizzati ripetutamente. È tuttavia possibile eseguire la valutazione una sola volta nella directory originale.

   Nell'esempio riportato di seguito, l'opzione `-s` viene usata per selezionare i tipi di risultati che devono essere inclusi nel report.

   Per impostazione predefinita, nel report vengono inclusi tutti i tipi di risultati ad eccezione di `notselected` o `notapplicable`. I tipi di risultati da includere in aggiunta a quelli previsti per impostazione predefinita vengono specificati in forma di elenco separato da virgole. Per eliminare singoli tipi di risultati è possibile anteporre loro il carattere `-`, mentre iniziando un elenco con il carattere `=` si specificano esattamente i tipi di risultati che devono essere inclusi. I tipi di risultati sono: `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error` o `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

   Questo comando crea un report contenente gli elementi non riusciti e quelli non selezionati in formato HTML. Il report viene eseguito in base alla valutazione più recente.

6. **Visualizzare il report completo.**

   È possibile visualizzare il file di log in un editor di testo, il file HTML in un browser oppure il file XML in un visualizzatore XML. Ad esempio, per visualizzare il report HTML personalizzato del passo precedente, digitare la seguente voce nel browser:

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. **Correggere gli errori che devono essere risolti in base a quanto indicato dal criterio di sicurezza.**

   Se la correzione richiede il reboot del sistema, effettuare il reboot prima di eseguire di nuovo la valutazione.

8. **Ripetere la valutazione fino a quando non si verificano errori.**

▼ (Facoltativo) Eseguire report sulla conformità con un job `cron`

- **Come superutente, usare il comando `crontab -e` per aggiungere l'inserimento appropriato nel file `crontab`.**

  Nell'elenco riportato di seguito vengono forniti esempi di inserimenti per `crontab`.

  - Esegue valutazioni della conformità ogni giorno alle ore 2:30.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Esegue valutazioni della conformità ogni settimana alle ore 1:15.

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Esegue valutazioni della conformità ogni mese, il primo giorno del mese alle ore 4:00.

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Esegue valutazioni della conformità il primo lunedì del mese alle ore 3:45.

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

Conformità a FIPS-140-2, Livello 1

Le applicazioni di crittografia presenti in SuperCluster 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, decifratura, 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) Abilitare il funzionamento conforme a FIPS 140 (Oracle ILOM) [39].

Nella tabella riportata di seguito vengono elencati gli algoritmi approvati in base a FIPS che sono supportati da Oracle Solaris in SuperCluster M7.

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		
Creazione/verifica di firme RSA PKCS#1.5: 1024 bit, 2048 bit (con SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
Creazione/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, decifratura, 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 il server Web Apache 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 i moduli del provider FIPS 140-2 utilizzano le risorse della CPU in modo intensivo, 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`.

Mantenere sicuri i sistemi SuperCluster serie M7

Negli argomenti riportati di seguito vengono descritte le funzioni di SuperCluster serie M7 che è possibile usare per mantenere la sicurezza per tutta la durata del sistema.

Gestione della sicurezza di SuperCluster

SuperCluster M7 sfrutta le capacità di gestione della sicurezza di una vasta gamma di prodotti, inclusi Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager e la suite Oracle Identity Management. Nelle sezioni riportate di seguito vengono descritti i dettagli.

Oracle ILOM per la gestione sicura

Oracle ILOM è un processore di servizi integrato in molti componenti di SuperCluster M7. Usare Oracle ILOM per eseguire le attività di gestione fuori banda descritte di seguito.

- Fornire accesso sicuro per eseguire la gestione remota sicura dei componenti di SuperCluster. I tipi di accesso includono l'accesso basato sul Web protetto da SSL, l'accesso dalla riga di comando basato su Secure Shell e i protocolli IPMI v2.0 e SNMP v3.
- Separare i requisiti dei diversi incarichi utilizzando un modello RBAC. Assegnare singoli utenti a ruoli specifici che limitano le funzioni che gli utenti possono eseguire.
- Fornire un log di audit di tutti i login e di tutte le modifiche alla configurazione. Ciascuna voce del log di audit mostra l'utente che esegue l'azione e un indicatore di data e ora. Questa funzionalità consente di rilevare attività o modifiche non autorizzate e attribuire tali azioni ad utenti specifici.

Per ulteriori informazioni, consultare la documentazione di Oracle Integrated Lights Out Manager all'indirizzo: http://docs.oracle.com/en/hardware/?tab=4

Suite Oracle Identity Management

La suite Oracle Identity Management gestisce la durata end-to-end delle identità e degli account degli utenti nell'intera organizzazione. La suite include il supporto per la funzionalità Single Sign-On, il controllo dell'accesso basato su Web, la sicurezza dei servizi Web, l'amministrazione delle identità, l'autenticazione complessa e i criteri di accesso.

Oracle Identity Management è in grado di fornire un singolo punto per la gestione delle identità e dell'accesso non solo per le applicazioni e i servizi in esecuzione su Oracle SuperCluster, ma anche per la struttura di base e i servizi che vengono gestiti.

Per ulteriori informazioni, consultare la documentazione di Oracle Identity Management all'indirizzo:

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager è un sistema di gestione chiavi completo (KMS, Key Management System) in grado di semplificare la gestione e il monitoraggio delle chiavi di cifratura che proteggono le informazioni.

Oracle Key Manager supporta gli ambienti delle imprese che presentano un'architettura altamente scalabile e disponibile, in grado di gestire centinaia di dispositivi e milioni di chiavi. Questa funzione opera in un ambiente operativo potenziato, applica il controllo dell'accesso

complesso e la separazione dei ruoli per le operazioni di gestione e monitoraggio delle chiavi e facoltativamente supporta la memorizzazione sicura delle chiavi in Sun Crypto Accelerator 6000 PCIe Card di Oracle, un modulo sicuro con classificazione hardware FIPS 140-2.

Nel contesto di SuperCluster, Oracle Key Manager può autorizzare, proteggere e gestire l'accesso alle chiavi di cifratura usate dalle unità nastro di cifratura Oracle StorageTek, agli Oracle Database cifrati con la cifratura trasparente dei dati e ai file system ZFS cifrati e disponibili nel sistema operativo Oracle Solaris 11.

Per ulteriori informazioni, consultare la documentazione di Oracle Key Manager all'indirizzo:

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager è uno strumento di gestione dell'hardware a livello rack, basato su BUI e destinato all'uso da parte del personale dell'assistenza Oracle. Per ulteriori informazioni, consultare *Oracle SuperCluster M7 Series Owner's Guide: Administration*.

Oracle Engineered Systems Hardware Manager include i seguenti due set di informazioni di autenticazione.

- **Password dei componenti di SuperCluster M7**

  Oracle Engineered Systems Hardware Manager mantiene una memorizzazione sicura delle password per tutti gli account di fabbrica di tutti i componenti hardware di SuperCluster M7. Il software utilizza queste password per gestire i componenti di SuperCluster M7.

  Quando una di queste password viene modificata, è necessario aggiornare l'applicazione Oracle Engineered Systems Hardware Manager con la nuova password.
- **Autenticazione locale**

  Oracle Engineered Systems Hardware Manager dispone di due account utente locali. Un account viene usato dai clienti per personalizzare Oracle Engineered Systems Hardware Manager in base all'ambiente in uso e per gestire l'account dei servizi. L'altro account viene usato dal personale dell'assistenza Oracle per configurare, supportare e prestare assistenza all'hardware di SuperCluster M7.

Oracle Engineered Systems Hardware Manager fornisce le risorse di gestione locali descritte di seguito.

- **Criterio della password**: la possibilità di configurare le password dell'applicazione in base ai criteri aziendali assicura la conformità delle password agli standard aziendali.

Nota - Per le impostazioni del criterio della password, consultare il responsabile della sicurezza aziendale.

- **Certificati**: Oracle Engineered Systems Hardware Manager utilizza i certificati per proteggere la comunicazione tra i server di calcolo e i server Oracle Engineered Systems Hardware Manager e BUI. I certificati vengono creati automaticamente durante l'installazione e sono univoci per ogni istanza di SuperCluster, tuttavia possono essere sostituiti da chiavi e certificati forniti dal cliente.
- **Porte**: le porte per la comunicazione di rete usate da Oracle Engineered Systems Hardware Manager sono configurabili in caso di conflitto con il criterio aziendale. Vengono usate le porte da 8001 a 8004 (incluse).

Per le istruzioni di configurazione, consultare il documento *Oracle SuperCluster M7 Series Owner's Guide: Administration*.

Oracle Enterprise Manager

La suite Oracle Enterprise Manager è una soluzione di gestione cloud completa e integrata, incentrata sulla gestione del ciclo di vita di applicazioni, middleware, database, infrastruttura fisica e virtuale (utilizzando Oracle Enterprise Manager Ops Center). Oracle Enterprise Manager fornisce le tecnologie di gestione descritte di seguito.

- Supporta il monitoraggio dettagliato, la notifica degli eventi, l'applicazione di patch, la gestione delle modifiche, la configurazione continua, la gestione della conformità e la creazione di report a livello di applicazione, middleware e database.
- Consente di gestire in modo centralizzato le impostazioni della configurazione di sicurezza, nonché il controllo dell'accesso e i criteri di audit per gruppi di database. L'accesso a queste funzioni può essere limitato a utenti autorizzati, assicurando che l'accesso alla gestione supporti i requisiti di conformità per la separazione degli incarichi, i privilegi minimi e le responsabilità.
- Supporta l'autenticazione complessa tramite diversi metodi, i controlli capillari dell'accesso e l'audit completo, assicurando che la gestione dell'ambiente SuperCluster può essere effettuata in modo sicuro.

Per ulteriori informazioni, consultare la documentazione di Oracle Enterprise Manager all'indirizzo: `http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html`

Oracle Enterprise Manager Ops Center (facoltativo)

Oracle Enterprise Manager Ops Center è una tecnologia facoltativa che è possibile usare per gestire alcuni aspetti della sicurezza di Oracle SuperCluster.

Oracle Enterprise Manager Ops Center, componente della suite Oracle Enterprise Manager, è una soluzione di gestione dell'hardware convergente in grado di fornire una singola interfaccia amministrativa per server, sistemi operativi, firmware, virtual machine, zone, storage e fabric di rete.

È possibile usare Oracle Enterprise Manager Ops Center per assegnare l'accesso amministrativo a raccolte di sistemi fisici e virtuali, monitorare l'attività dell'amministratore, rilevare gli errori, configurare e gestire gli avvisi. Oracle Enterprise Manager Ops Center supporta un'ampia gamma di report che consentono di confrontare i sistemi rispetto ad elementi noti quali le linee di base della configurazione, i livelli di patch e le vulnerabilità della sicurezza.

Per ulteriori informazioni, consultare la documentazione di Oracle Enterprise Manager Ops Center all'indirizzo: `http://docs.oracle.com/cd/E27363_01/index.htm`

Nota - Per le versioni precedenti di Oracle Enterprise Manager Ops Center, il software Ops Center veniva installato ed eseguito dal sistema SuperCluster. A partire da Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0), il software Ops Center deve essere installato ed eseguito in un sistema esterno al sistema SuperCluster.

Monitoraggio della sicurezza

Indipendentemente che la finalità sia ottenere report sulla conformità o risposte agli incidenti, il monitoraggio e l'audit sono funzioni fondamentali che devono essere usate per ottenere maggiore visibilità all'interno dell'ambiente IT. Il grado di utilizzo delle funzioni di monitoraggio e audit spesso dipende dal rischio o dalla natura critica dell'ambiente.

I sistemi SuperCluster serie M7 forniscono funzionalità complete di monitoraggio e audit a livello di server, rete, database e storage, assicurando che le informazioni possono essere rese disponibili a supporto dei requisiti di audit e conformità.

Nelle sezioni riportate di seguito vengono descritti il monitoraggio e l'audit dei carichi di lavoro e dei database.

- sezione chiamata «Monitoraggio dei carichi di lavoro» [134]

- sezione chiamata «Monitoraggio e audit dell'attività dei database» [134]
- sezione chiamata «Monitoraggio delle reti» [135]

Monitoraggio dei carichi di lavoro

Il sistema operativo Oracle Solaris dispone di una funzionalità di audit completa in grado di monitorare le azioni amministrative, i richiami della riga di comando e anche le singole chiamate di sistema a livello kernel. Questa funzionalità è altamente configurabile e offre criteri di audit globali, per zona e anche per utente.

Quando il sistema è configurato per usare Oracle Solaris Zones, nella zona globale è possibile memorizzare i record di audit di ogni zona per proteggerli dalla monomissione.

L'audit di Oracle Solaris consente di inviare i record di audit a punti di raccolta remoti tramite la funzionalità del log di sistema (`syslog`). I record di audit di Oracle Solaris possono essere usati da più servizi di rilevamento e prevenzione delle intrusioni commerciali come input aggiuntivo per le analisi e i report.

Oracle VM Server per SPARC sfrutta la funzionalità di audit nativa di Oracle Solaris per registrare azioni ed eventi associati agli eventi di virtualizzazione e all'amministrazione dei domini.

Per ulteriori informazioni, consultare la sezione Monitoraggio e manutenzione della sicurezza di Oracle Solaris del documento Linee guida per la sicurezza di Oracle Solaris all'indirizzo:

`http://docs.oracle.com/cd/E26502_01`

Monitoraggio e audit dell'attività dei database

Il supporto di Oracle Database della funzionalità di audit capillare consente di stabilire i criteri che determinano in modo selettivo quando vengono generati i record di audit. Questa possibilità consente di concentrarsi su altre attività dei database e ridurre il carico di lavoro spesso associato alle attività di audit.

Oracle Audit Vault and Database Firewall centralizza la gestione delle impostazioni di audit dei database e automatizza il consolidamento dei dati di audit in un repository sicuro. Questo software include report integrati per monitorare un'ampia gamma di attività, incluse l'attività dell'utente con privilegi e le modifiche alle strutture dei database. I report generati da Oracle Audit Vault and Database Firewall offrono visibilità su diverse attività delle applicazioni e dei database amministrativi e forniscono informazioni dettagliate per supportare la responsabilità delle azioni.

Oracle Audit Vault and Database Firewall consente il rilevamento proattivo di attività che possono indicare tentativi di accesso non autorizzato o abuso dei privilegi di sistema con conseguente emissione di avvisi. Questi avvisi possono includere sia eventi di sistema che definiti dall'utente e condizioni, come la creazione di account utente con privilegi o la modifica di tabelle contenenti informazioni sensibili.

Oracle Audit Vault and Database Firewall Remote Monitor è in grado di offrire il monitoraggio della sicurezza dei database in tempo reale. Questa funzione esegue delle query sulle connessioni al database per rilevare traffico malevolo, come l'azione di ignorare l'applicazione, attività non autorizzata, inserimento SQL e altre minacce. Utilizzando un approccio accurato basato sulla grammatica SQL, questo software consente di identificare rapidamente eventuale attività sospetta del database.

Per ulteriori informazioni, consultare la documentazione di Oracle Audit Vault and Database Firewall all'indirizzo: http://docs.oracle.com/cd/E37100_01/index.htm

Monitoraggio delle reti

Dopo aver configurato le reti in base alle linee guida sulla sicurezza, è necessario svolgere regolarmente le attività di controllo e manutenzione.

Attenersi alle istruzioni fornite di seguito per garantire la sicurezza dell'accesso locale e remoto al sistema.

- Controllare la presenza di incidenti nei log e archiviare i log rispettando i criteri di sicurezza dell'organizzazione.
- Eseguire revisioni periodiche della rete di accesso del client per assicurare che le impostazioni di host e Oracle ILOM rimangono invariate.

Per ulteriori informazioni, consultare le guide sulla sicurezza del sistema operativo Oracle Solaris:

- sistema operativo Oracle Solaris 11: http://www.oracle.com/goto/Solaris11/docs
- sistema operativo Oracle Solaris 10: http://www.oracle.com/goto/Solaris10/docs

Aggiornamento del software e del firmware

Gli aggiornamenti del sistema SuperCluster serie M7 vengono forniti nella QFSDP. Installando la QFSDP, tutti i componenti vengono aggiornati contemporaneamente. Questa modalità

assicura che tutti i componenti continuino ad essere eseguiti in una combinazione di versioni del software che sono state sottoposte insieme a test completi da parte di Oracle.

Ottenere la più recente QFSDP da My Oracle Support all'indirizzo: `http://support.oracle.com`

Per ulteriori informazioni sul software e sul firmware supportati, consultare il documento *Oracle SuperCluster M7 Series Product Notes*. Le istruzioni per l'accesso alle note sul prodotto sono disponibili nella nota MOS 1605591.1.

Nota - Eseguire l'upgrade, l'aggiornamento o l'applicazione di patch a singoli componenti in isolamento per la manutenzione reattiva solo su consiglio del supporto Oracle.

Indice

D

E

R

S