Guida per la sicurezza di Oracle® VM Server per SPARC 3.5

N. di parte: E86375-01
Agosto 2017

N. di parte: E86375-01

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 sull'uso sicuro del software Oracle VM Server per SPARC 3.5.
- **Destinatari**: amministratori di sistema che gestiscono la sicurezza su server SPARC virtualizzati
- **Conoscenze richieste**: gli amministratori di sistema di questi server devono avere una conoscenza pratica dei sistemi UNIX e del sistema operativo Oracle Solaris (SO Oracle Solaris)

Raccolta di documentazione sul prodotto

La documentazione e le risorse per questo e per i prodotti correlati sono disponibili all'indirizzo `http://www.oracle.com/technetwork/documentation/vm-sparc-194287.html`.

Feedback

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

♦ ♦ ♦ CAPITOLO 1

Panoramica della sicurezza di Oracle VM Server per SPARC

Sebbene il numero di consigli correlati alla sicurezza riportati in questo documento possa dare un'impressione diversa, l'installazione tipica di Oracle VM Server per SPARC offre già una buona protezione dall'uso non autorizzato. Permangono alcuni punti di vulnerabilità agli attacchi e un livello ridotto di rischio, anche se è improbabile che vengano sfruttati. Allo stesso modo in cui si sceglie di aggiungere un allarme anti-intrusione alla protezione della propria abitazione per potenziare deterrenti standard come le porte blindate, le misure di sicurezza della rete aggiuntive possono aiutare a ridurre la probabilità che si verifichino problemi imprevisti o a minimizzare il danno potenziale.

In questo capitolo sono descritti gli argomenti correlati alla sicurezza di Oracle VM Server per SPARC elencati di seguito.

Funzioni di sicurezza utilizzate da Oracle VM Server per SPARC

Il software Oracle VM Server per SPARC è un prodotto di virtualizzazione che consente l'esecuzione di più macchine virtuali (VM, Virtual Machine) Oracle Solaris su un solo sistema fisico, ciascuna con il proprio SO Oracle Solaris 10 o Oracle Solaris 11 installato. Ogni VM è anche denominata *dominio logico*. I domini sono istanze indipendenti e supportano l'esecuzione di versioni diverse di SO Oracle Solaris, nonché software applicativi diversi. Sui domini, ad esempio, possono essere installate versioni diverse dei pacchetti, abilitati servizi diversi e

utilizzati account di sistema con password diverse. Per informazioni sulla sicurezza di Oracle Solaris, vedere *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.

Il comando `ldm` richiama Logical Domains Manager e deve essere eseguito nel dominio di controllo per configurare i domini e recuperare informazioni sullo stato. Per la sicurezza dei domini in esecuzione nel sistema, è fondamentale limitare l'accesso al dominio di controllo e al comando `ldm`. Per limitare l'accesso ai dati di configurazione del dominio, utilizzare le funzioni di sicurezza di Oracle VM Server per SPARC, ad esempio i diritti Oracle Solaris per le console e le autorizzazioni `solaris.ldoms`. Vedere «Logical Domains Manager Profile Contents» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Il software Oracle VM Server per SPARC utilizza le funzioni di sicurezza elencate di seguito.

- Le funzioni di sicurezza disponibili nei SO Oracle Solaris 10 e Oracle Solaris 11 sono disponibili anche nei domini su cui è in esecuzione il software Oracle VM Server per SPARC. Vedere *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.
- Le funzioni di sicurezza di SO Oracle Solaris possono essere applicate al software Oracle VM Server per SPARC. Per informazioni complete su come garantire la sicurezza di Oracle VM Server per SPARC, vedere sezione chiamata «Sicurezza in un ambiente virtualizzato» [15] e sezione chiamata «Difesa dagli attacchi» [17].
- I SO Oracle Solaris 10 e Oracle Solaris 11 includono alcune correzioni alla sicurezza disponibili per il sistema in uso. Richiedere le correzioni per il SO Oracle Solaris 10 come patch o aggiornamenti della sicurezza. Richiedere le correzioni per il SO Oracle Solaris 11 come SRU (Support Repository Update).
- Per informazioni su come limitare l'accesso ai comandi di amministrazione e alle console dei domini di Oracle VM Server per SPARC, vedere Capitolo 2, «Oracle VM Server for SPARC Security» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

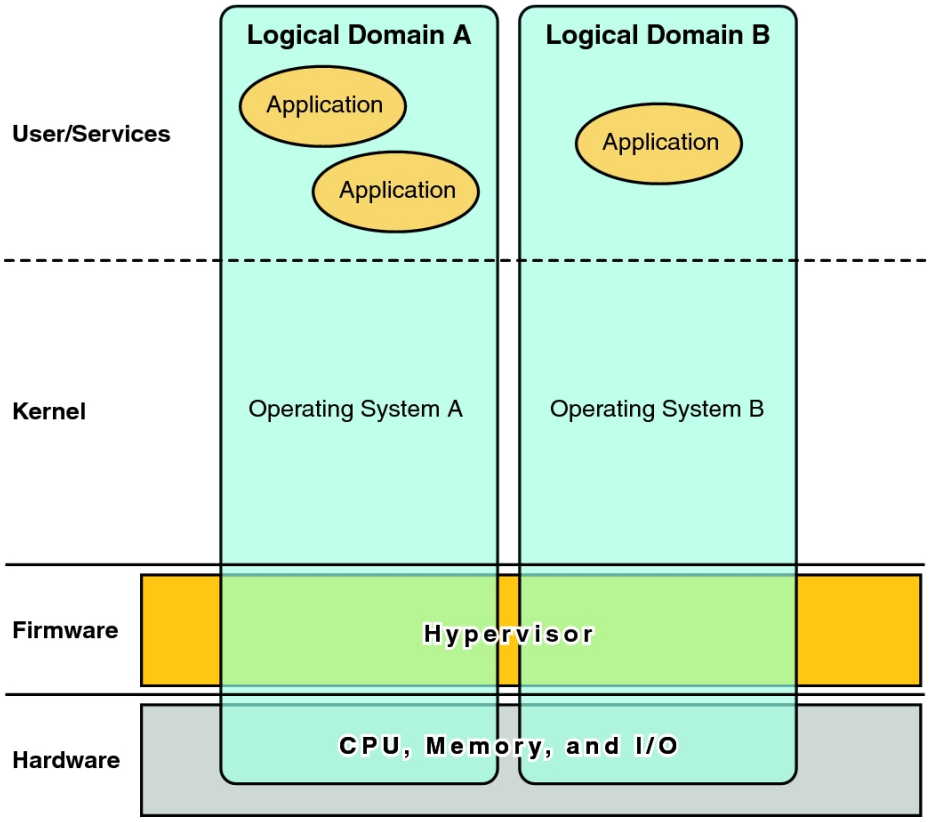
Panoramica del prodotto Oracle VM Server per SPARC

Oracle VM Server per SPARC offre funzionalità di virtualizzazione per le imprese ad elevata efficienza per i server Oracle SPARC di serie T, nonché per i server SPARC M5 e Server Fujitsu M10. Il software Oracle VM Server per SPARC consente di creare molti server virtuali, denominati domini logici, su un singolo sistema. Questo tipo di configurazione consente di sfruttare l'imponente quantità di thread offerta da questi server SPARC e da SO Oracle Solaris.

Un *dominio logico* è una macchina virtuale contenente un raggruppamento logico discreto di risorse. Un dominio logico è dotato di un sistema operativo proprio e si identifica con un singolo sistema informatico. Ciascun dominio logico può essere creato, eliminato, riconfigurato e sottoposto a reboot in modo indipendente, senza richiedere l'esecuzione di un ciclo di alimentazione del server. È possibile eseguire più software applicativi in domini logici diversi e mantenerli indipendenti per garantirne le prestazioni e la sicurezza.

Per informazioni sull'uso del software Oracle VM Server per SPARC, vedere *Oracle VM Server for SPARC 3.5 Administration Guide* e *Oracle VM Server for SPARC 3.5 Reference Manual*. Per informazioni sui componenti hardware e software necessari, vedere *Oracle VM Server for SPARC 3.5 Installation Guide*.

FIGURA 1 Hypervisor con supporto di due domini logici



Il software Oracle VM Server per SPARC utilizza i componenti elencati di seguito per offrire la virtualizzazione del sistema.

- **Hypervisor.** L'hypervisor è un piccolo componente firmware che offre un'architettura stabile per macchina virtualizzata su cui è possibile installare un sistema operativo. I server Sun di Oracle che utilizzano l'hypervisor sono dotati di funzioni hardware per il supporto del controllo dell'hypervisor sulle attività del sistema operativo in un dominio logico.

Il numero di domini e le funzionalità di ciascun dominio supportati da uno specifico hypervisor SPARC sono caratteristiche che dipendono dal server. L'hypervisor può allocare sottoinsiemi della CPU, della memoria e delle risorse I/O del server in un determinato dominio logico. Tale allocazione consente il supporto della coesistenza di più sistemi operativi, ciascuno nel proprio dominio logico. Le risorse possono essere ridisposte tra domini logici separati con una granularità arbitraria. Le CPU, ad esempio, possono essere assegnate a un dominio logico con la granularità di un thread di CPU.

Il *processore di servizio* (SP, Service Processor), anche denominato *controller di sistema* (SC, System Controller), è responsabile del monitoraggio e dell'esecuzione della macchina fisica. I domini logici stessi sono gestiti da Logical Domains Manager e non dal processore di servizio.

- **Dominio di controllo.** Logical Domains Manager viene eseguito in questo dominio e consente di creare e gestire altri domini logici, nonché di allocare risorse virtuali ad altri domini. È supportato un solo dominio di controllo per ciascun server. Il dominio di controllo è il primo dominio creato quando si installa il software Oracle VM Server per SPARC. Il dominio di controllo è denominato `primary`.
- **Dominio di servizio.** Un dominio di servizio offre servizi per dispositivi virtuali ad altri domini, ad esempio uno switch virtuale, un concentratore di console virtuale e un server su disco virtuale. Qualsiasi dominio può essere configurato come dominio di servizio.
- **Dominio I/O.** Un dominio I/O ha accesso diretto ai dispositivi I/O fisici, ad esempio una scheda di rete in un controller PCIe (PCI EXPRESS). Un dominio I/O può possedere un complesso radice PCIe, uno slot PCIe o un dispositivo PCIe su scheda mediante la funzione di I/O diretto (DIO, Direct I/O). Vedere «Creating an I/O Domain by Assigning PCIe Endpoint Devices» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

  Quando un dominio I/O viene utilizzato anche come dominio di servizio, può condividere dispositivi I/O fisici con altri domini sotto forma di dispositivi virtuali.
- **Dominio radice.** A un dominio radice è assegnato un complesso radice PCIe. Questo dominio possiede il fabric PCIe di tale complesso radice e fornisce tutti i servizi correlati al fabric, ad esempio la gestione degli errori del fabric. Un dominio radice è anche un dominio I/O, in quanto possiede i dispositivi I/O fisici e può accedervi direttamente.

  Il numero di domini radice consentito dipende dall'architettura della piattaforma in uso. Se ad esempio si utilizza un server SPARC T4-4 di Oracle, è possibile disporre di quattro domini radice.
- **Dominio guest.** Un dominio guest è un dominio non I/O che utilizza i servizi per dispositivi virtuali forniti da uno o più domini di servizio. Un dominio guest non possiede alcun dispositivo I/O fisico, ma solo dispositivi I/O virtuali, come dischi virtuali e interfacce di rete virtuali.

Un sistema Oracle VM Server per SPARC spesso prevede solo un dominio di controllo che fornisce i servizi eseguiti dai domini I/O e dai domini di servizio. Per migliorare la ridondanza

e la funzionalità della piattaforma, considerare la possibilità di configurare più domini I/O nel sistema Oracle VM Server per SPARC.

Applicazione di principi di sicurezza generali a Oracle VM Server per SPARC

È possibile configurare i domini guest in diversi modi per offrire livelli diversi di isolamento del dominio guest, condivisione dell'hardware e connettività del dominio. Questi fattori contribuiscono al livello di sicurezza della configurazione generale di Oracle VM Server per SPARC. Per consigli sull'implementazione sicura del software Oracle VM Server per SPARC, vedere sezione chiamata «Sicurezza in un ambiente virtualizzato» [15] e sezione chiamata «Difesa dagli attacchi» [17].

È possibile applicare alcuni dei principi di sicurezza generali indicati di seguito.

- **Ridurre i punti di vulnerabilità agli attacchi.**
  - Ridurre gli errori di configurazione involontari tramite la creazione di linee guida operative che consentono di valutare la sicurezza del sistema a intervalli regolari. Vedere sezione chiamata «Contromisura: creazione di linee guida operative» [20].
  - Pianificare attentamente l'architettura dell'ambiente virtuale per ottimizzare l'isolamento dei domini. Vedere le contromisure descritte per sezione chiamata «Minaccia: errori nell'architettura dell'ambiente virtuale» [20].
  - Pianificare attentamente le risorse da assegnare e stabilire se è necessario condividerle. Vedere sezione chiamata «Contromisura: assegnazione attenta di risorse hardware» [23] e sezione chiamata «Contromisura: assegnazione attenta di risorse condivise» [23].
  - Accertarsi che i domini logici siano protetti dalla manipolazione applicando le contromisure descritte in sezione chiamata «Minaccia: manipolazione dell'ambiente di esecuzione» [24] e sezione chiamata «Contromisura: protezione del SO del dominio guest» [38].
    - sezione chiamata «Contromisura: protezione dei percorsi di accesso interattivi» [25].
    - sezione chiamata «Contromisura: riduzione di SO Oracle Solaris» [25].
    - sezione chiamata «Contromisura: rafforzamento di SO Oracle Solaris» [25].
    - sezione chiamata «Contromisura: rafforzamento di Logical Domains Manager» [32].
    - In sezione chiamata «Contromisura: uso della separazione dei ruoli e dell'isolamento dell'applicazione» [26] viene descritta l'importanza di assegnare ruoli con funzionalità ai diversi domini e garantire che nel dominio di controllo venga eseguito il software che fornisce l'infrastruttura necessaria per i domini guest host.

È necessario eseguire applicazioni che possano essere eseguite da altri sistemi su domini guest progettati a questo scopo.

- In sezione chiamata «Contromisura: configurazione di una rete di gestione dedicata» [26] viene descritta una configurazione di rete più avanzata che prevede la connessione dei server con processori di servizio a una rete di gestione dedicata per proteggere il processore di servizio dall'accesso di rete.

- Esporre un dominio guest alla rete *solo* se necessario. È possibile utilizzare gli switch virtuali per limitare la connettività di rete del dominio guest *solo* alle reti appropriate.
- Attenersi alle procedure di riduzione dei punti di vulnerabilità agli attacchi per Oracle Solaris 10 e Oracle Solaris 11, come descritto in *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.
- Proteggere il nucleo dell'hypervisor come descritto in sezione chiamata «Contromisura: convalida di firme software e firmware» [29] e sezione chiamata «Contromisura: convalida dei moduli kernel» [30].
- Proteggere il dominio di controllo dagli attacchi di negazione del servizio. Vedere sezione chiamata «Contromisura: protezione dell'accesso della console» [31].
- Accertarsi che Logical Domains Manager non possa essere eseguito da utenti non autorizzati. Vedere sezione chiamata «Minaccia: uso non autorizzato delle utility di configurazione» [31].
- Accertarsi che nessun utente o processo non autorizzato possa accedere al dominio di servizio. Vedere sezione chiamata «Minaccia: manipolazione di un dominio di servizio» [34].
- Proteggere un dominio I/O o un dominio di servizio dagli attacchi di negazione del servizio. Vedere sezione chiamata «Minaccia: negazione del servizio di un dominio I/O o di un dominio di servizio» [36].
- Accertarsi che nessun utente o processo non autorizzato possa accedere a un dominio I/O. Vedere sezione chiamata «Minaccia: manipolazione di un dominio I/O» [37].
- Disabilitare i servizi di gestione dei domini non necessari. Logical Domains Manager offre servizi di rete per l'accesso, il monitoraggio e la migrazione dei domini. Vedere sezione chiamata «Contromisura: rafforzamento di Logical Domains Manager» [32] e sezione chiamata «Contromisura: protezione di Oracle ILOM» [28].
- **Concedere il privilegio minimo per l'esecuzione di un'operazione.**
  - Isolare i sistemi in *classi di sicurezza*, ossia gruppi di singoli sistemi guest che condividono gli stessi requisiti e privilegi di sicurezza. Se si assegnano solo domini guest da una singola classe di sicurezza a una singola piattaforma hardware, si crea una barriera di isolamento che impedisce ai domini di passare a una classe di sicurezza diversa. Vedere sezione chiamata «Contromisura: assegnazione attenta di guest a piattaforme hardware» [20].
  - Utilizzare i diritti per limitare la capacità di gestire i domini con il comando `ldm`. Questa capacità deve essere concessa *solo* agli utenti che devono amministrare i

domini. Assegnare un ruolo che utilizza il profilo dei diritti LDoms Management agli utenti che richiedono l'accesso a tutti i sottocomandi `ldm`. Assegnare un ruolo che utilizza il profilo dei diritti LDoms Review agli utenti che richiedono l'accesso solo ai sottocomandi `ldm` correlati all'elenco. Vedere «Using Rights Profiles and Roles» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

- Utilizzare i diritti per limitare l'accesso alla console *solo* dei domini amministrati dall'amministratore di Oracle VM Server per SPARC. *Non* consentire l'accesso generale a tutti i domini. Vedere «Controlling Access to a Domain Console by Using Rights» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Sicurezza in un ambiente virtualizzato

Per proteggere in modo efficace l'ambiente virtualizzato di Oracle VM Server per SPARC, proteggere il sistema operativo e ciascun servizio in esecuzione in ciascun dominio. Per ridurre gli effetti di una violazione riuscita, separare i servizi implementandoli in domini diversi.

L'ambiente Oracle VM Server per SPARC utilizza un hypervisor per virtualizzare CPU, memory e risorse I/O per i domini logici. Ciascun dominio è un server virtualizzato discreto che è necessario proteggere da potenziali attacchi.

Un ambiente virtualizzato consente di consolidare più server in un unico server mediante la condivisione delle risorse hardware. In Oracle VM Server per SPARC le risorse di memoria e CPU sono allocate in modo esclusivo a ciascun dominio, per impedire eventuali abusi dovuti a un uso eccessivo della CPU o all'allocazione di memoria. Le risorse di rete e su disco vengono in genere fornite dai domini di servizio a più domini guest.

Quando si valuta la sicurezza, partire *sempre* dal presupposto che nell'ambiente è presente un difetto che può essere sfruttato da un intruso. Un intruso, ad esempio, potrebbe sfruttare una debolezza dell'hypervisor per eseguire l'hijack dell'intero sistema, inclusi i domini guest. È pertanto importante implementare *sempre* i sistemi in modo da ridurre il rischio di danno in caso di violazione.

Ambiente di esecuzione

L'ambiente di esecuzione include i componenti elencati di seguito.

- **Hypervisor**: firmware specifico della piattaforma per la virtualizzazione dell'hardware che si basa prevalentemente sul supporto hardware creato nella CPU.
- **Dominio di controllo**: dominio specializzato per la configurazione dell'hypervisor e l'esecuzione di Logical Domains Manager che gestisce i domini logici.

- **Dominio I/O o dominio radice**: dominio che possiede alcuni o tutti i dispositivi I/O disponibili della piattaforma e li condivide con altri domini.
- **Dominio di servizio**: dominio che offre servizi ad altri domini. Un dominio di servizio può fornire ad altri domini l'accesso alla console o a dischi virtuali. Un dominio di servizio che fornisce ad altri domini l'accesso a dischi virtuali è anche denominato dominio I/O.

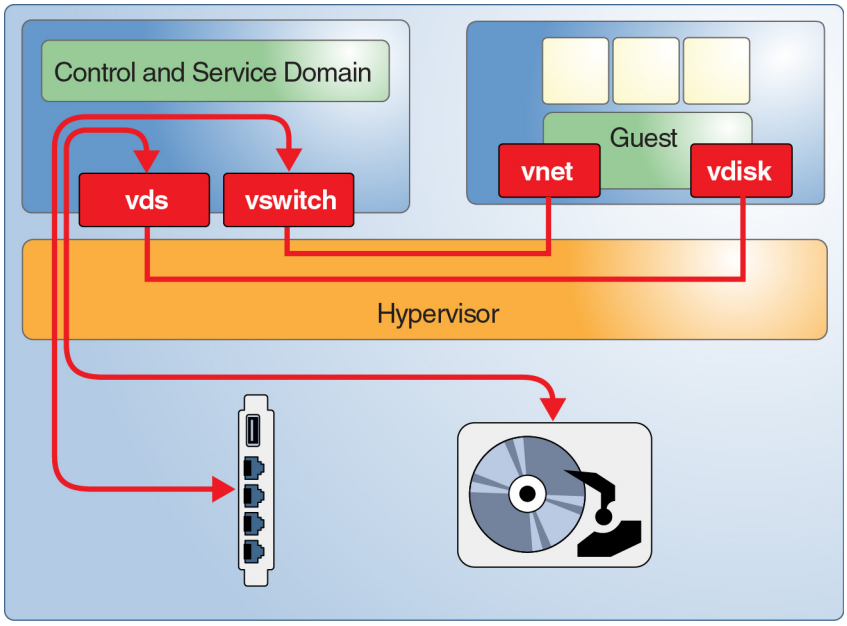
Per ulteriori informazioni su questi componenti, vedere Figura 1 e le descrizioni dei componenti più dettagliate.

È possibile migliorare la funzionalità delle configurazioni I/O ridondanti configurando un secondo dominio I/O. È anche possibile utilizzare un secondo dominio I/O per isolare l'hardware rispetto alle violazioni della sicurezza. Per informazioni sulle opzioni di configurazione, vedere *Oracle VM Server for SPARC 3.5 Administration Guide*.

Protezione dell'ambiente di esecuzione

L'ambiente di esecuzione di Oracle VM Server per SPARC presenta diversi obiettivi di attacco. Figura 2 mostra una configurazione semplice di Oracle VM Server per SPARC in cui il dominio di controllo fornisce servizi di rete e su disco a un domino guest. Questi servizi vengono implementati mediante daemon e moduli kernel in esecuzione nel dominio di controllo. Logical Domains Manager assegna i canali LDC (Logical Domain Channel) per ciascun servizio e un client per facilitare la comunicazione punto-punto tra di loro. Un intruso potrebbe sfruttare un errore in uno qualsiasi dei componenti per violare l'isolamento dei domini guest. Un intruso potrebbe, ad esempio, eseguire codice arbitrario nel dominio di servizio o interferire con le normali operazioni della piattaforma.

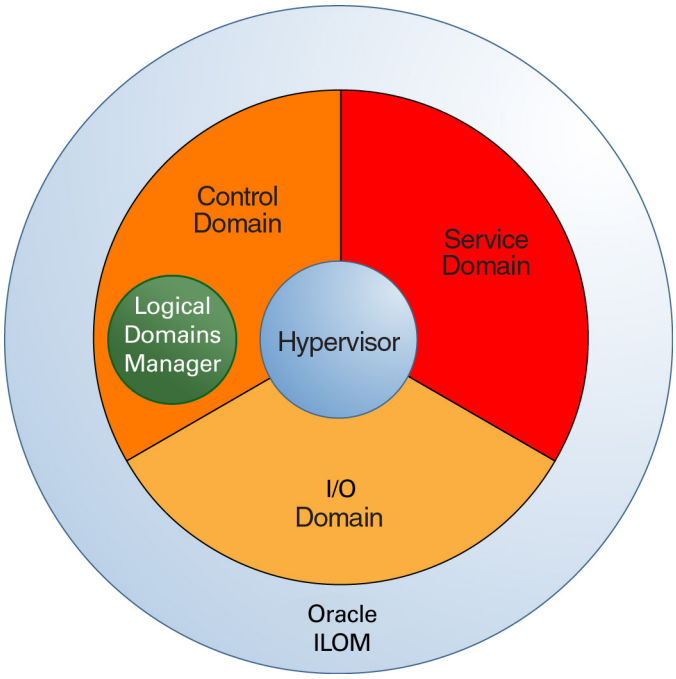
FIGURA 2 Esempio di ambiente Oracle VM Server per SPARC



Difesa dagli attacchi

La figura seguente mostra i componenti di virtualizzazione che compongono l'ambiente di esecuzione di Oracle VM Server per SPARC. Questi componenti non sono rigorosamente separati. La configurazione più semplice consiste nel combinare tutte queste funzioni in un singolo dominio. Il dominio di controllo può fungere anche da dominio I/O e da dominio di servizio per altri domini.

FIGURA 3 Componenti dell'ambiente di esecuzione



Si supponga che un intruso tenti di violare l'isolamento del sistema e di manipolare quindi l'hypervisor o un altro componente dell'ambiente di esecuzione per raggiungere un dominio guest. È necessario proteggere ciascun dominio guest come se si trattasse di un server standalone.

Nella parte restante di questo capitolo sono illustrate le possibili minacce e le diverse misure che è possibile intraprendere per respingerle. Ciascuno di questi attacchi è volto a vincere o eliminare l'isolamento dei diversi domini in esecuzione in una singola piattaforma. Nelle sezioni successive sono descritte le minacce a ciascuna parte di un sistema Oracle VM Server per SPARC.

- sezione chiamata «Ambiente operativo» [19]
- sezione chiamata «Ambiente di esecuzione» [24]
- sezione chiamata «Oracle ILOM» [27]
- sezione chiamata «Hypervisor» [29]
- sezione chiamata «Dominio di controllo» [30]

- sezione chiamata «Logical Domains Manager» [31]
- sezione chiamata «Dominio I/O» [35]
- sezione chiamata «Dominio di servizio» [33]
- sezione chiamata «Domini guest» [37]

Ambiente operativo

L'ambiente operativo include sistemi fisici e relativi componenti, responsabili dell'architettura dei centri dati, amministratori e membri dell'organizzazione IT. Una violazione della sicurezza può verificarsi in qualsiasi componente dell'ambiente operativo.

La virtualizzazione inserisce un livello software tra l'hardware effettivo e i domini guest su cui sono in esecuzione i servizi di produzione, per aumentare la complessità. È pertanto necessario pianificare e configurare con estrema attenzione il sistema virtuale e cercare di evitare l'errore umano. Cercare anche di evitare i tentativi degli intrusi di ottenere l'accesso all'ambiente operativo utilizzando il "social engineering".

Nelle sezioni seguenti sono descritte le diverse minacce che è possibile respingere a livello di ambiente operativo.

Minaccia: errore di configurazione involontario

La preoccupazione principale correlata alla sicurezza per un ambiente virtualizzato consiste nel mantenere l'isolamento del server separando i segmenti di rete, isolando l'accesso amministrativo e implementando i server in classi di sicurezza, ossia gruppi di domini con gli stessi requisiti e privilegi di sicurezza.

Configurare con attenzione le risorse virtuali per evitare alcuni degli errori elencati di seguito.

- Creazione di canali di comunicazione non necessari tra domini guest di produzione e ambiente di esecuzione
- Creazione di accesso non necessario ai segmenti di rete
- Creazione di connessioni involontarie tra classi di sicurezza discrete
- Migrazione involontaria di un dominio guest alla classe di sicurezza errata
- Allocazione di hardware insufficiente, che può portare a sovraccarico imprevisto delle risorse
- Assegnazione di dischi o dispositivi I/O al dominio errato

Contromisura: creazione di linee guida operative

Prima di iniziare, definire attentamente le linee guida operative per l'ambiente Oracle VM Server per SPARC. In queste linee guida sono descritte le attività riportate di seguito e le relative modalità di esecuzione.

- Gestione di patch per tutti i componenti dell'ambiente
- Abilitazione dell'implementazione sicura, ben definita e riscontrabile delle modifiche
- Controllo dei file di log a intervalli regolari
- Monitoraggio dell'integrità e della disponibilità dell'ambiente

Eseguire regolarmente i controlli per accertarsi che queste linee guida rimangano aggiornate e adeguate e per verificare che vengano seguite nelle operazioni quotidiane.

Oltre a queste linee guida, è possibile intraprendere diverse altre misure tecniche per ridurre il rischio di azioni involontarie. Vedere sezione chiamata «Logical Domains Manager» [31].

Minaccia: errori nell'architettura dell'ambiente virtuale

Quando si sposta un sistema fisico in un ambiente virtualizzato, in genere è possibile lasciare invariata la configurazione riutilizzando i LUN originali. È tuttavia necessario adattare la configurazione di rete all'ambiente virtualizzato e l'architettura risultante potrebbe essere notevolmente diversa rispetto a quella utilizzata nel sistema fisico.

È necessario considerare come mantenere l'isolamento delle classi di sicurezza discrete e le relative esigenze. Considerare inoltre l'hardware condiviso della piattaforma e i componenti condivisi come i switch di rete e i switch SAN.

Per ottimizzare la sicurezza dell'ambiente, accertarsi di mantenere l'isolamento dei domini guest e delle classi di sicurezza. Quando si progetta l'architettura, prevedere i possibili errori e attacchi e implementare le opportune linee di difesa. Un buon progetto consente di limitare i potenziali problemi di sicurezza e di gestire complessità e costi.

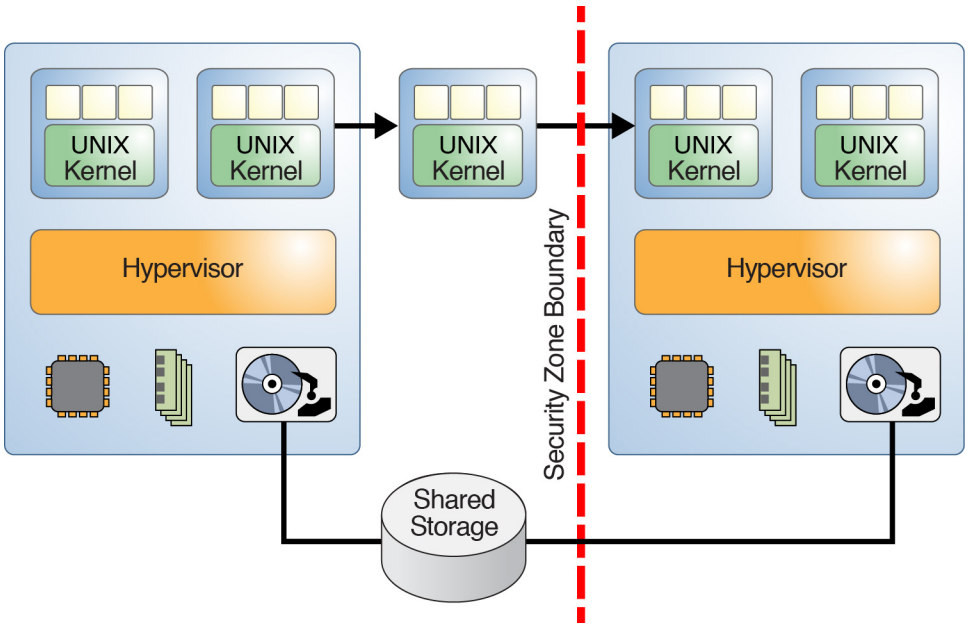
Contromisura: assegnazione attenta di guest a piattaforme hardware

Utilizzare le classi di sicurezza, ossia gruppi di domini caratterizzati dagli stessi requisiti e privilegi di sicurezza, per isolare i singoli domini gli uni dagli altri. Se si assegnano domini guest inclusi nella stessa classe di sicurezza a una determinata piattaforma hardware, anche in caso di violazione dell'isolamento l'attacco non potrà penetrare in un'altra classe di sicurezza.

Contromisura: pianificazione di una migrazione al dominio Oracle VM Server per SPARC

La funzione di migrazione del dominio in tempo reale ha il potenziale di rompere l'isolamento qualora venga inavvertitamente eseguita la migrazione di un dominio guest a una piattaforma assegnata a una classe di sicurezza diversa, come mostra la figura seguente. Pianificare pertanto con attenzione la migrazione del dominio guest in modo da accertarsi che non sia consentita una migrazione che superi i confini delle classi di sicurezza.

FIGURA 4 Migrazione del dominio che supera i confini di sicurezza



Per ridurre o eliminare il problema della vulnerabilità della sicurezza posto dall'operazione di migrazione, è necessario eseguire manualmente lo scambio e installare i certificati host generati con il comando `ldmd` fuori banda all'interno di ogni coppia costituita da sistema di origine e sistema di destinazione. Per informazioni su come configurare i certificati SSL, vedere «Configuring SSL Certificates for Migration» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Contromisura: configurazione corretta delle connessioni virtuali

Se si perde traccia di tutte le connessioni di rete virtuali, è possibile che un dominio ottenga erroneamente l'accesso a un segmento di rete. Tale accesso potrebbe ad esempio eludere il firewall o una classe di sicurezza.

Per ridurre il rischio di errori di implementazione, pianificare e documentare attentamente tutte le connessioni virtuali e fisiche nell'ambiente. Ottimizzare il piano di connessione del dominio in modo da garantire semplicità e facilità di gestione. Documentare in modo chiaro il piano e verificare l'esattezza dell'implementazione a fronte del piano prima di passare alla produzione. Anche dopo avere avviato la produzione dell'ambiente virtuale, verificare l'implementazione a fronte del piano a intervalli regolari.

Contromisura: uso di tag della VLAN

È possibile utilizzare i tag della VLAN per consolidare più segmenti Ethernet in una singola rete fisica. Questa funzione è disponibile anche per gli switch virtuali. Per ridurre i rischi impliciti negli errori software che si verificano durante l'implementazione degli switch virtuali, configurare uno switch virtuale per ciascun NIC fisico e VLAN. Come ulteriore protezione dagli errori del driver Ethernet, evitare di utilizzare VLAN con tag. La probabilità che si verifichino questi errori è tuttavia ridotta in quanto la vulnerabilità della VLAN con tag è ben nota. I test di intrusione sulla piattaforma Sun SPARC serie T di Oracle con il software Oracle VM Server per SPARC non hanno mostrato questa vulnerabilità.

Contromisura: uso di appliance di sicurezza virtuali

Le appliance di sicurezza come i filtri pacchetti e i firewall sono strumenti di isolamento e proteggono l'isolamento delle classi di sicurezza. Poiché queste appliance sono soggette alle stesse minacce di tutti gli altri domini guest, il relativo utilizzo non garantisce una protezione completa da una violazione dell'isolamento. Considerare pertanto attentamente tutti gli aspetti di rischio e sicurezza prima di decidere di virtualizzare un servizio di questo tipo.

Minaccia: effetti collaterali della condivisione delle risorse

La condivisione delle risorse in un ambiente virtualizzato può portare ad attacchi di negazione del servizio (DoS, Denial of Service), che determinano il sovraccarico di una risorsa fino a ottenere un effetto negativo su un altro componente, ad esempio un altro dominio.

In un ambiente Oracle VM Server per SPARC un attacco DoS può avere effetto solo su alcune risorse. Le risorse di CPU e memoria vengono assegnate in modo esclusivo a ciascun dominio

guest, per impedire la maggior parte degli attacchi DoS. Persino l'assegnazione esclusiva di queste risorse può rallentare un dominio guest nei modi indicati di seguito.

- Tramite allocazione delle aree della cache condivise tra settori e assegnate a due domini guest
- Tramite sovraccarico della larghezza di banda della memoria

A differenza delle risorse di CPU e memoria, i servizi di rete e su disco vengono in genere condivisi tra domini guest. Questi servizi vengono forniti ai domini guest da uno o più domini di servizio. Considerare attentamente come assegnare e distribuire queste risorse ai domini guest. Tenere presente che tutte le configurazioni che offrono massime prestazioni e utilizzo delle risorse riducono al contempo il rischio di effetti collaterali.

Valutazione: effetti collaterali dovuti alle risorse condivise

È possibile che un collegamento di rete diventi saturo o che un disco venga sovraccaricato, indipendentemente dal fatto che sia assegnato a un dominio o condiviso tra più domini. Ciò incide negativamente sulla disponibilità di un servizio per tutta la durata dell'attacco. L'obiettivo dell'attacco non viene compromesso e non si verifica alcuna perdita di dati. È possibile ridurre gli effetti di questa minaccia, ma è necessario tenerla presente anche se si limita alle risorse di rete e su disco di Oracle VM Server per SPARC.

Contromisura: assegnazione attenta di risorse hardware

Accertarsi di assegnare solo le risorse hardware necessarie ai domini guest. Annullare l'assegnazione di una risorsa inutilizzata quando questa non è più necessaria, ad esempio, una porta di rete o un'unità DVD necessaria solo durante un'installazione. Questa pratica consente di ridurre il numero di possibili punti di accesso per un attacco.

Contromisura: assegnazione attenta di risorse condivise

Le risorse hardware condivise, come le porte di rete fisiche, costituiscono un obiettivo possibile per gli attacchi DoS. Per limitare l'impatto degli attacchi DoS a un solo gruppo di domini guest, determinare attentamente i domini guest e le risorse hardware da questi condivise.

I domini guest che condividono risorse hardware, ad esempio, possono essere raggruppati in base alla disponibilità o ai requisiti di sicurezza comuni. Oltre al raggruppamento, è possibile applicare diversi tipi di controlli delle risorse.

È necessario considerare come condividere le risorse su disco e di rete. È possibile ridurre i problemi separando l'accesso al disco tramite percorsi di accesso fisico dedicati o servizi su disco virtuali dedicati.

Riepilogo: effetti collaterali dovuti alle risorse condivise

Tutte le contromisure descritte in questa sezione richiedono la comprensione dei dettagli tecnici dell'implementazione e le relative implicazioni in termini di sicurezza. Eseguire con attenzione le operazioni di pianificazione e documentazione e creare un'architettura il più semplice possibile. Accertarsi di comprendere le implicazioni dell'hardware virtualizzato in modo da prepararsi a un'implementazione sicura del software Oracle VM Server per SPARC.

I domini logici sono resistenti agli effetti della condivisione di CPU e memoria, in quanto richiedono una condivisione effettiva ridotta. Ciò nonostante, è preferibile applicare controlli delle risorse come la gestione delle risorse Solaris all'interno dei domini guest. Questi controlli offrono protezione da comportamenti errati dell'applicazione, sia per un ambiente virtuale che per un ambiente non virtualizzato.

Ambiente di esecuzione

Figura 3 mostra i componenti dell'ambiente di esecuzione. Ciascun componente fornisce determinati servizi, che insieme compongono la piattaforma generale su cui eseguire i domini guest di produzione. Una configurazione corretta dei componenti è di vitale importanza per l'integrità del sistema.

Tutti i componenti dell'ambiente di esecuzione sono potenziali obiettivi di attacco. In questa sezione sono descritte le minacce a cui può essere esposto ciascun componente nell'ambiente di esecuzione. Alcune minacce e contromisure possono interessare più componenti.

Minaccia: manipolazione dell'ambiente di esecuzione

La manipolazione dell'ambiente di esecuzione offre molti modi per ottenere il controllo. È possibile, ad esempio, installare il firmware manipolato in Oracle ILOM per esaminare tutti gli I/O del dominio guest da un dominio I/O. Con questo tipo di attacco è possibile accedere alla configurazione del sistema e modificarla. Un intruso che assume il controllo del dominio di controllo di Oracle VM Server per SPARC può riconfigurare il sistema in qualsiasi modo, mentre un intruso che assume il controllo di un dominio I/O può apportare modifiche ai dispositivi di memorizzazione collegati, come i dischi di boot.

Valutazione: manipolazione dell'ambiente di esecuzione

Un intruso che riesce a violare Oracle ILOM o qualsiasi altro dominio nell'ambiente di esecuzione può leggere e manipolare tutti i dati disponibili per tale dominio. Questo accesso

può avvenire dalla rete o mediante un errore nello stack di virtualizzazione. Questo tipo di attacco è difficile da eseguire in quanto in genere Oracle ILOM e i domini non possono essere attaccati direttamente.

Le contromisure per la protezione dalla manipolazione dell'ambiente di esecuzione sono pratiche di sicurezza standard e devono essere implementate in ogni sistema. Le pratiche di sicurezza standard offrono un livello di protezione aggiuntivo attorno all'ambiente di esecuzione che riduce ulteriormente il rischio di intrusione e manipolazione.

Contromisura: protezione dei percorsi di accesso interattivi

Accertarsi di creare *solo* gli account necessari per le applicazioni in esecuzione sul sistema.

Accertarsi che gli account necessari per l'amministrazione siano protetti utilizzando l'autenticazione basata su chiave o password sicure. Tali chiavi o password non devono essere condivise tra domini diversi. Considerare anche la possibilità di implementare l'autenticazione a due fattori o una "regola dei due operatori" per eseguire determinate azioni.

Non utilizzare login anonimi per account come l'account `root` in modo da garantire la completa tracciabilità e responsabilità dell'esecuzione dei comandi nel sistema. Utilizzare piuttosto i diritti per concedere ai singoli amministratori *solo* l'accesso alle funzioni che sono autorizzati a eseguire. Accertarsi che l'accesso amministrativo alla rete utilizzi sempre una cifratura come SSH e che la workstation di un amministratore sia considerata un sistema ad elevata sicurezza.

Contromisura: riduzione di SO Oracle Solaris

Poiché qualsiasi componente software installato in un sistema può essere compromesso, accertarsi di installare *solo* il software necessario, per ridurre la possibilità di violazioni.

Contromisura: rafforzamento di SO Oracle Solaris

Oltre a installare una versione ridotta di SO Oracle Solaris, configurare pacchetti software finalizzati al rafforzamento del software contro gli attacchi. Eseguire in primo luogo un numero limitato di servizi di rete per disabilitare in modo efficace tutti i servizi di rete ad eccezione di SSH. Questo criterio corrisponde al comportamento predefinito nei sistemi Oracle Solaris 11. Per informazioni su come proteggere SO Oracle Solaris, vedere *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.

Contromisura: uso della separazione dei ruoli e dell'isolamento dell'applicazione

Le applicazioni di produzione sono necessariamente collegate ad altri sistemi e sono pertanto più esposte agli attacchi esterni. *Non* implementare applicazioni di produzione in un dominio incluso nell'ambiente di esecuzione. Accertarsi piuttosto di implementarle *solo* nei domini guest privi di ulteriori privilegi.

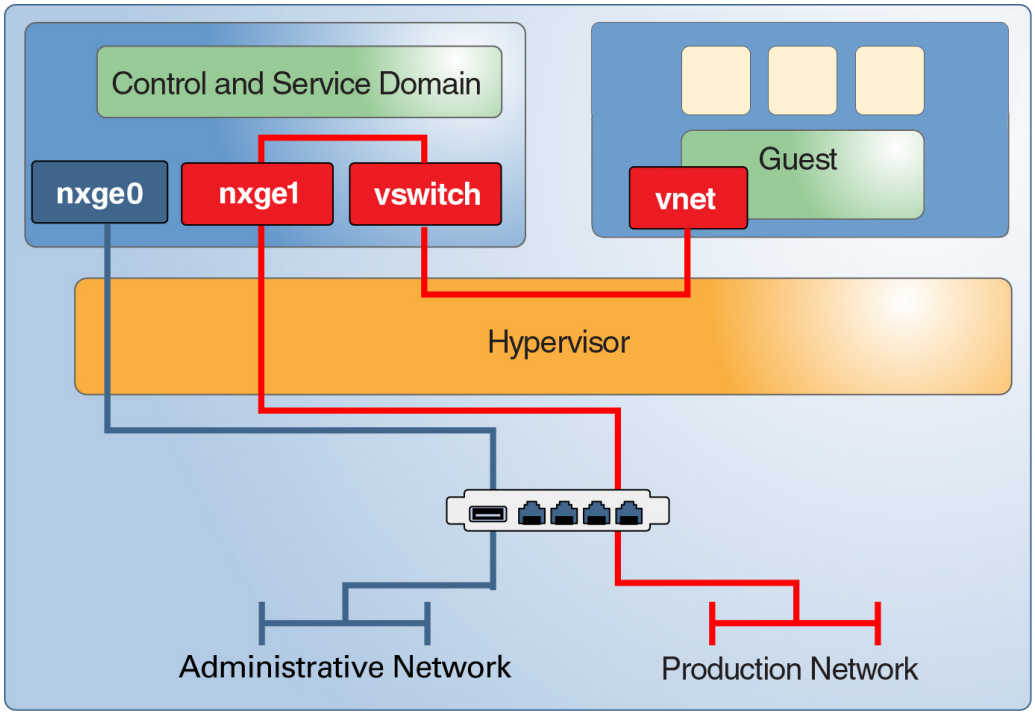
L'ambiente di produzione deve fornire solo l'infrastruttura necessaria per questi domini guest. La separazione dell'ambiente di esecuzione dalle applicazioni di produzione consente di implementare la granularità nei privilegi di amministrazione. L'amministratore di un dominio guest di produzione non ha bisogno dell'accesso all'ambiente di esecuzione e l'amministratore di un ambiente di esecuzione non ha bisogno dell'accesso ai domini guest di produzione. Se possibile, assegnare i diversi ruoli dell'ambiente di esecuzione, come il dominio di controllo e il dominio I/O, a domini diversi. Questo tipo di configurazione riduce la quantità di danni che possono essere causati in caso di compromissione di uno qualsiasi di questi domini.

È anche possibile estendere la separazione dei ruoli all'ambiente di rete utilizzato per collegare i diversi server.

Contromisura: configurazione di una rete di gestione dedicata

Collegare tutti i server dotati di processori di servizio (SP) a una rete di gestione dedicata. Questa configurazione è consigliata anche per i domini dell'ambiente di esecuzione. Se questi domini sono in rete, ubicarli nella propria rete dedicata. *Non* collegare i domini dell'ambiente di esecuzione direttamente alle reti assegnate ai domini di produzione. Sebbene sia possibile eseguire tutte le attività di amministrazione tramite la singola connessione alla console disponibile dal processore di servizio Oracle ILOM, questa configurazione rende l'amministrazione talmente scomoda da risultare impraticabile. La separazione della rete di produzione da quella di amministrazione offre protezione dalle intercettazioni e dalle manipolazioni. Questo tipo di separazione elimina anche la possibilità di attacco nell'ambiente di esecuzione dai domini guest della rete condivisa.

FIGURA 5 Rete di gestione dedicata



Oracle ILOM

Tutti i sistemi SPARC Oracle correnti includono un controller di sistema incorporato (Oracle ILOM) dotato delle funzionalità elencate di seguito.

- Gestione di controlli ambientali di base come la velocità della ventola e l'alimentazione dello chassis
- Abilitazione di aggiornamenti firmware
- Disponibilità della console di sistema per il dominio di controllo

È possibile accedere a Oracle ILOM tramite una connessione seriale o da una porta di rete mediante SSH, HTTP, HTTPS, SNMP o IPMI. I Server Fujitsu M10 utilizzano XSCF anziché Oracle ILOM per eseguire funzioni simili.

Minaccia: negazione del servizio del sistema completo

Un intruso che assume il controllo di Oracle ILOM può compromettere il sistema in molti modi, inclusi quelli elencati di seguito.

- Disattivazione di tutti i domini guest in esecuzione
- Installazione di firmware manipolato per ottenere l'accesso ad almeno un dominio guest

Questi scenari possono verificarsi in qualsiasi sistema dotato di un dispositivo di controllo di questo tipo. In un ambiente virtualizzato il danno può essere notevolmente maggiore rispetto a un ambiente fisico in quanto molti domini ospitati nello stesso system enclosure sono a rischio.

Allo stesso modo, un intruso che assume il controllo del dominio di controllo o di un dominio I/O può facilmente disabilitare tutti i domini guest dipendenti arrestando i servizi I/O corrispondenti.

Valutazione: negazione del servizio del sistema completo

Oracle ILOM è in genere collegato a una rete di amministrazione che deve essere ben protetta e isolata dalle reti di produzione normali.

Allo stesso modo, un intruso può violare un dominio di servizio dalla rete o tramite un errore nello stack di virtualizzazione, quindi bloccare gli I/O guest o eseguire un arresto di sistema. Sebbene il danno sia limitato in quanto non comporta perdita né compromissione dei dati, esso può avere un effetto negativo su molti domini guest. Garantire pertanto la protezione dalla possibilità di questa minaccia per limitare il danno potenziale.

Contromisura: protezione di Oracle ILOM

In qualità di processore di servizio del sistema, Oracle ILOM controlla funzioni critiche quali l'alimentazione dello chassis, le configurazioni di avvio di Oracle VM Server per SPARC e l'accesso della console al dominio di controllo. Le misure elencate di seguito consentono di proteggere Oracle ILOM.

- Posizionamento della porta di rete di Oracle ILOM in un segmento di rete separato dalla rete amministrativa, utilizzata per i domini nell'ambiente di esecuzione.
- Disabilitazione di tutti i servizi non necessari per il funzionamento, come HTTP, IPMI, SNMP, HTTPS e SSH.
- Configurazione di account dedicati e personali degli amministratori per concedere solo i diritti necessari. Per massimizzare la responsabilità delle azioni eseguite dagli amministratori, accertarsi di creare account personali per gli amministratori. Questo tipo

di accesso è particolarmente importante per l'accesso della console, gli aggiornamenti firmware e la gestione delle configurazioni di avvio.

Hypervisor

L'hypervisor è il livello di firmware per l'implementazione e il controllo della virtualizzazione dell'hardware effettivo. L'hypervisor include i componenti elencati di seguito.

- Hypervisor effettivo, implementato nel firmware e supportato dalle CPU del sistema.
- Moduli kernel eseguiti nel dominio di controllo per la configurazione dell'hypervisor.
- Moduli kernel e daemon eseguiti nei domini I/O e nei domini di servizio per fornire l'I/O virtualizzato, nonché moduli kernel che comunicano mediante Logical Domain Channel (LDC).
- Moduli kernel e driver di dispositivi in esecuzione nei domini guest per l'accesso ai dispositivi I/O virtualizzati, nonché moduli kernel che comunicano mediante LDC.

Minaccia: violazione dell'isolamento

Un intruso può eseguire l'hijack dei domini guest o dell'intero sistema violando l'ambiente runtime isolato offerto dall'hypervisor. Potenzialmente, questa minaccia può causare il danno più grave a un sistema.

Valutazione: violazione dell'isolamento

La struttura di un sistema modulare può migliorare l'isolamento concedendo livelli diversi di privilegi a domini guest, all'hypervisor e al dominio di controllo. Ciascun modulo funzionale viene implementato in un modulo kernel, driver di dispositivo o daemon separato e configurabile. Questa modularità richiede API chiare e protocolli di comunicazione semplici per ridurre il rischio generale di errori.

Anche se lo sfruttamento di un errore sembra improbabile, il danno potenziale può portare al controllo dell'intero sistema da parte dell'intruso.

Contromisura: convalida di firme software e firmware

Sebbene sia possibile scaricare le patch del firmware di sistema e del SO direttamente da un sito Web Oracle, tali patch possono essere manipolate. Prima di installare il software, verificare

i checksum MD5 dei pacchetti software. I checksum di tutti i componenti software scaricabili sono pubblicati da Oracle.

Contromisura: convalida dei moduli kernel

Oracle VM Server per SPARC utilizza diversi driver e moduli kernel per implementare il sistema di virtualizzazione generale. Tutti i moduli kernel e la maggior parte dei binari distribuiti con SO Oracle Solaris sono dotati di una firma digitale. Utilizzare la utility `elfsign` per controllare la firma digitale di ciascun modulo kernel e driver. È possibile utilizzare il comando `pkg verify` di Oracle Solaris 11 per controllare l'integrità del binario di Oracle Solaris. Vedere `https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it`.

È necessario in primo luogo stabilire l'integrità della utility `elfsign`. Utilizzare lo strumento di audit e reporting di base (BART, Basic Audit and Reporting Tool) per automatizzare il processo di verifica della firma digitale. In Integrating BART and the Solaris Fingerprint Database in the Solaris 10 Operating System (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`) viene descritto come combinare lo strumento BART e Solaris Fingerprint Database per eseguire automaticamente controlli dell'integrità simili. Sebbene Fingerprint Database non sia più in produzione, i concetti descritti in questo documento possono essere adottati per un uso simile di `elfsign` e BART.

È possibile utilizzare la funzione di boot verificato come contromisura per convalidare i moduli kernel. Per configurare la convalida automatica dei moduli kernel in fase di boot, impostare i criteri di boot verificato in Oracle ILOM. Consultare la documentazione per la piattaforma specifica all'indirizzo `http://docs.oracle.com/en/hardware/`. Per convalidare i moduli kernel nel dominio di controllo, impostare i criteri di boot verificato in Oracle ILOM. Per convalidare i moduli kernel nei domini guest, utilizzare Logical Domains Manager per impostare i criteri di boot verificato.

Dominio di controllo

Il dominio di controllo, che spesso svolge il ruolo di un dominio I/O e di un dominio di servizio, deve essere protetto in quanto può modificare la configurazione dell'hypervisor, che controlla tutte le risorse hardware collegate.

Minaccia: negazione del servizio del dominio di controllo

L'arresto del dominio di controllo può determinare la negazione di servizio degli strumenti di configurazione. Poiché i domini di controllo sono necessari solo per le modifiche alla configurazione, i domini guest non sono coinvolti se dispongono dell'accesso alla rete e alle risorse su disco tramite altri domini di servizio.

Valutazione: negazione del servizio del dominio di controllo

L'attacco al dominio di controllo mediante la rete è equivalente all'attacco di qualsiasi altra istanza di SO Oracle Solaris protetta in modo appropriato. Il danno derivante da un arresto o da una simile negazione di servizio del dominio di controllo è relativamente ridotto. I domini guest rimangono tuttavia coinvolti se il dominio di controllo funge anche da dominio di servizio per tali domini guest.

Contromisura: protezione dell'accesso della console

Evitare di configurare l'accesso della rete amministrativa ai domini dell'ambiente di esecuzione. Questo scenario richiede l'uso del servizio console di Oracle ILOM nel dominio di controllo per eseguire tutte le attività di amministrazione. L'accesso della console a tutti gli altri domini è comunque possibile utilizzando il servizio `vntsd` in esecuzione nel dominio di controllo.

Considerare attentamente questa opzione. Sebbene questa opzione riduca il rischio di attacco tramite la rete amministrativa, l'accesso alla console sarà consentito a un solo amministratore alla volta.

Per informazioni sulla configurazione sicura di `vntsd`, vedere «How to Enable the Virtual Network Terminal Server Daemon» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Logical Domains Manager

Logical Domains Manager viene eseguito nel dominio di controllo e consente di configurare l'hypervisor, nonché di creare e configurare tutti i domini e le relative risorse hardware. Accertarsi che l'uso di Logical Domains Manager sia protetto da login e sia monitorato.

Minaccia: uso non autorizzato delle utility di configurazione

Un intruso potrebbe assumere il controllo dell'ID utente di un amministratore oppure un amministratore di un gruppo diverso potrebbe ottenere l'accesso non autorizzato a un altro sistema.

Valutazione: uso non autorizzato delle utility di configurazione

Per accertarsi che a un amministratore non sia concesso l'accesso superfluo a un sistema, implementare un'efficace gestione delle identità. Implementare anche un controllo dell'accesso rigido e specifico e altre misure come la regola dei due operatori.

Contromisura: applicazione della regola dei due operatori

Considerare la possibilità di implementare la regola dei due operatori per Logical Domains Manager e per altri strumenti amministrativi utilizzando i diritti. Questa regola protegge da attacchi di social engineering, compromissione degli account amministrativi ed errori umani.

Contromisura: uso dei diritti per Logical Domains Manager

L'uso dei diritti per il comando `ldm` consente di implementare un controllo dell'accesso specifico e di mantenere una tracciabilità completa. Per informazioni sulla configurazione dei diritti, vedere *Oracle VM Server for SPARC 3.5 Administration Guide*. L'uso dei diritti facilita la tutela dagli errori umani in quanto consente di scegliere le funzioni del comando `ldm` da rendere disponibili e gli amministratori autorizzati a utilizzarle.

Contromisura: rafforzamento di Logical Domains Manager

Disabilitare i servizi di gestione dei domini non necessari. Logical Domains Manager offre servizi di rete per l'accesso, il monitoraggio e la migrazione dei domini. La disabilitazione dei servizi di rete riduce i punti di vulnerabilità agli attacchi di Logical Domains Manager al minimo necessario per un funzionamento normale. Questo scenario consente di contrastare gli attacchi di negazione del servizio e altri tentativi di uso improprio dei servizi di rete.

Nota - Sebbene la disabilitazione dei servizi di gestione dei domini aiuti a ridurre i punti di vulnerabilità agli attacchi, non è possibile conoscere preventivamente tutti gli effetti collaterali di questa operazione nelle diverse configurazioni specifiche.

Disabilitare i servizi di rete elencati di seguito quando non vengono utilizzati.

- Servizio di migrazione sulla porta TCP `8101`

  Per disabilitare questo servizio, vedere la descrizione delle proprietà `ldmd/incoming_migration_enabled` e `ldmd/outgoing_migration_enabled` nella pagina man `ldmd`(1M).
- Supporto del protocollo XMPP (Extensible Messaging and Presence Protocol) sulla porta TCP `6482`

  Per informazioni su come disabilitare questo servizio, vedere «XML Transport» in *Oracle VM Server for SPARC 3.5 Developer's Guide*.

  La disabilitazione di XMPP impedisce il funzionamento di alcuni strumenti di gestione e funzioni chiave di Oracle VM Server per SPARC. Vedere sezione chiamata «Interfaccia XML di Oracle VM Server per SPARC» [41].
- Protocollo SNMP (Simple Network Management Protocol) sulla porta UDP `161`

Determinare se si desidera utilizzare MIB (Management Information Base) di Oracle VM Server per SPARC per osservare i domini. Questa funzione richiede l'abilitazione del servizio SNMP. In base alla decisione presa, effettuare una delle operazioni indicate di seguito.

- **Abilitare il servizio SNMP per utilizzare MIB di Oracle VM Server per SPARC.** Installare in modo sicuro MIB di Oracle VM Server per SPARC. Vedere «How to Install the Oracle VM Server for SPARC MIB Software Package» in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide* e Capitolo 3, «Managing Security» in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide*.
- **Disabilitare il servizio SNMP.** Per informazioni su come disabilitare questo servizio, vedere «How to Remove the Oracle VM Server for SPARC MIB Software Package» in *Oracle VM Server for SPARC 3.5 Management Information Base User's Guide*.

- Servizio di ricerca su un indirizzo multicast `239.129.9.27` e sulla porta `64535`

Nota - Tenere presente che questo meccanismo di ricerca viene utilizzato anche dal daemon `ldmd` per rilevare eventuali conflitti durante l'assegnazione automatica degli indirizzi MAC. Se si disabilita il servizio di ricerca, il rilevamento dei conflitti tra indirizzi MAC non verrà eseguito e, di conseguenza, l'allocazione automatica dell'indirizzo MAC non funzionerà correttamente.

Non è possibile disabilitare questo servizio mentre il daemon di Logical Domains Manager, `ldmd`, è in esecuzione. Utilizzare piuttosto la funzionalità di filtro IP di Oracle Solaris per bloccare l'accesso a questo servizio, allo scopo di ridurre i punti di vulnerabilità agli attacchi di Logical Domains Manager. Il blocco dell'accesso impedisce l'uso non autorizzato della utility e contrasta in modo efficace gli attacchi di negazione del servizio e altri tentativi di uso improprio di questi servizi di rete. Vedere Capitolo 20, «IP Filter in Oracle Solaris (Overview)» in *Oracle Solaris Administration: IP Services* e «Using IP Filter Rule Sets» in *Oracle Solaris Administration: IP Services*.

Vedere anche sezione chiamata «Contromisura: protezione di Oracle ILOM» [28].

Dominio di servizio

Un dominio di servizio fornisce alcuni servizi virtuali ai domini guest nel sistema. Tali servizi possono includere servizi di switch virtuale, disco virtuale o console virtuale.

Figura 6 mostra un dominio di servizio di esempio che fornisce servizi di console. Il dominio di controllo spesso ospita i servizi di console, assumendo in tal modo la funzionalità di un dominio

di servizio. I domini dell'ambiente di esecuzione spesso combinano le funzioni di un dominio di controllo, un dominio I/O e un dominio di servizio in uno o due domini.

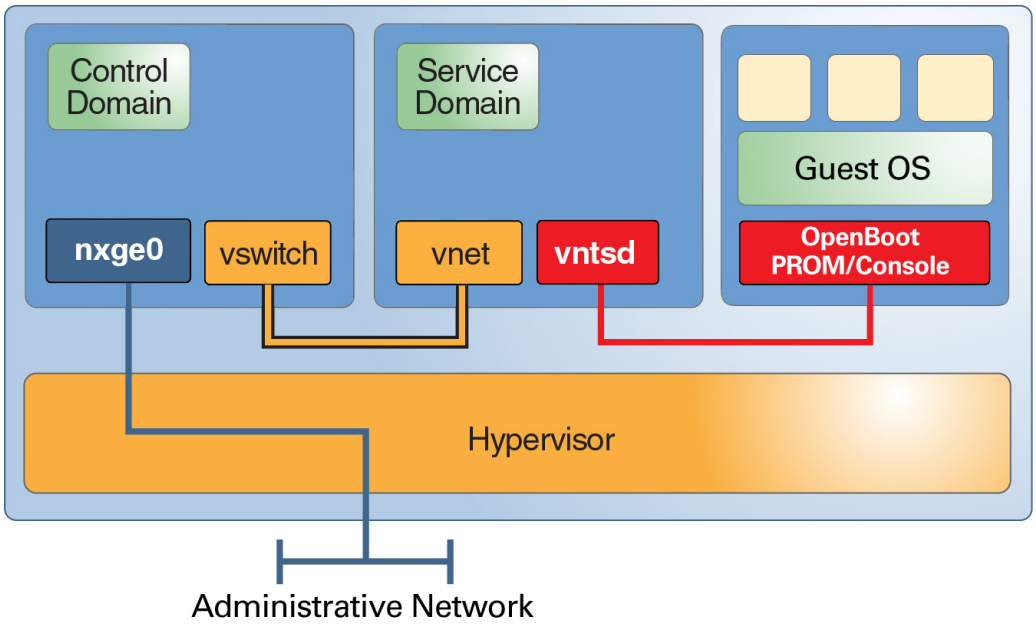
Minaccia: manipolazione di un dominio di servizio

Un intruso che assume il controllo di un dominio di servizio può manipolare i dati o intercettare qualsiasi comunicazione eseguita tramite i servizi offerti. Questo controllo può includere l'accesso della console ai domini guest, l'accesso ai servizi di rete o l'accesso ai servizi su disco.

Valutazione: manipolazione di un dominio di servizio

Sebbene le strategie di attacco siano le stesse di un attacco al dominio di controllo, i danni possibili sono inferiori in quanto l'intruso non può modificare la configurazione del sistema. Il danno risultante potrebbe includere il furto o la manipolazione di dati offerti dal dominio di servizio, ma non la manipolazione di alcuna sorgente di dati. A seconda del servizio, è possibile che un intruso debba scambiare i moduli kernel.

FIGURA 6 Esempio di dominio di servizio



Contromisura: isolamento dei domini di servizio tramite granularità

Se possibile, fare in modo che ciascun dominio di servizio offra solo *un* servizio ai client. Questa configurazione garantisce che, in caso di violazione di un dominio di servizio, venga compromesso un solo servizio. Accertarsi tuttavia di valutare l'importanza di questo tipo di configurazione a fronte della complessità aggiuntiva. Tenere presente che la presenza di domini I/O ridondanti è altamente consigliata.

Contromisura: isolamento dei domini di servizio e dei domini guest

È possibile isolare i domini di servizio sia di Oracle Solaris 10 che di Oracle Solaris 11 rispetto ai domini guest. Le soluzioni riportate di seguito sono elencate nell'ordine di implementazione preferito.

- Accertarsi che il dominio di servizio e il dominio guest non condividano la stessa porta di rete. Evitare inoltre di attivare (plumb) qualsiasi interfaccia dello switch virtuale nel dominio di servizio. Per i domini di servizio di Oracle Solaris 11, evitare di attivare (plumb) qualsiasi VNIC sulle porte fisiche utilizzate per gli switch virtuali.
- Qualora sia necessario utilizzare la stessa porta di rete sia per il SO Oracle Solaris 10 che per Oracle Solaris 11, situare il traffico del dominio I/O in una VLAN non utilizzata dai domini guest.
- Qualora non sia possibile implementare alcuna delle soluzioni precedenti, evitare di attivare (plumb) lo switch virtuale nel SO Oracle Solaris 10 e applicare i filtri IP nel SO Oracle Solaris 11.

Contromisura: limitazione dell'accesso alle console virtuali

Accertarsi che l'accesso alle singole console virtuali sia limitato *solo* agli utenti che hanno necessità di accedervi. Questa configurazione garantisce che nessun singolo amministratore possa accedere a tutte le console e impedire in tal modo l'accesso a tutte le console non assegnate a un account compromesso. Vedere «How to Create Default Services» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Dominio I/O

Qualsiasi dominio con accesso diretto ai dispositivi I/O fisici, come porte di rete o dischi, è un dominio I/O. Per informazioni sulla configurazione dei domini I/O, vedere Capitolo 6, «Configuring I/O Domains» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

Un dominio I/O può fungere anche da dominio di servizio se fornisce servizi I/O a domini guest, concedendo in tal modo ai domini l'accesso all'hardware.

Minaccia: negazione del servizio di un dominio I/O o di un dominio di servizio

Un attacco che blocca i servizi I/O di un dominio I/O garantisce un blocco equivalente in tutti i domini guest dipendenti. Un attacco DoS può essere portato a termine con successo tramite il sovraccarico della rete di back-end o dell'infrastruttura del disco mediante l'inserimento di un errore nel dominio. Entrambi gli attacchi possono forzare la sospensione o un errore grave del dominio. Allo stesso modo, un attacco che determina la sospensione dei servizi di un dominio di servizio causa la sospensione immediata di tutti i domini guest che dipendono da tali servizi. In caso di sospensione del dominio guest, le operazioni verranno riprese quando verrà ripristinato il servizio I/O.

Valutazione: negazione del servizio di un dominio I/O o di un dominio di servizio

Gli attacchi DoS vengono in genere eseguiti in rete. È possibile che questo tipo di attacco abbia successo in quanto le porte di rete sono aperte per la comunicazione e possono essere sovraccariche a causa del traffico di rete. La perdita di servizio risultante determina il blocco dei domini guest dipendenti. Un attacco simile alle risorse su disco può essere eseguito mediante l'infrastruttura SAN o il dominio I/O. L'unico danno è un arresto temporaneo di tutti i domini guest dipendenti. Sebbene l'impatto delle attività DoS possa essere considerevole, i dati non vengono compromessi né persi e la configurazione del sistema rimane intatta.

Contromisura: configurazione granulare dei domini I/O

La configurazione di più domini I/O riduce l'impatto causato dall'errore o dalla compromissione di un singolo dominio. È possibile assegnare singoli slot PCIe a un dominio guest per conferirgli le funzionalità di dominio I/O. In caso di crash del dominio radice proprietario del bus PCIe, il bus viene reimpostato, con conseguente crash del dominio assegnato al singolo slot. Questa funzione non elimina completamente la necessità di utilizzare due domini radice, ciascuno proprietario di un bus PCIe separato.

Contromisura: configurazione di hardware e domini radice ridondanti

L'alta disponibilità contribuisce anche a una maggiore sicurezza in quanto garantisce che i servizi possano resistere agli attacchi di negazione del servizio. Oracle VM Server per SPARC implementa metodologie di alta disponibilità come l'uso di risorse su disco e in rete ridondanti in domini I/O ridondanti. Questa opzione di configurazione consente di eseguire gli aggiornamenti senza interruzioni dei domini I/O e protegge dall'impatto di un errore in un dominio I/O dovuto a un attacco DoS riuscito. Con l'avvento di SR-IOV, i domini guest sono

dotati di accesso diretto ai singoli dispositivi I/O. Quando tuttavia non è possibile utilizzare SR-IOV, considerare la possibilità di creare domini I/O ridondanti. Vedere sezione chiamata «Contromisura: isolamento dei domini di servizio tramite granularità» [35].

Minaccia: manipolazione di un dominio I/O

Un dominio I/O è dotato di accesso diretto ai dispositivi di back-end, in genere dischi, che virtualizza e in seguito offre ai domini guest. Un attacco riuscito comporta l'accesso completo a questi dispositivi e la lettura dei dati sensibili o la manipolazione del software nei dischi di boot dei domini guest.

Valutazione: manipolazione di un dominio I/O

L'attacco a un dominio I/O è verosimile quanto un attacco riuscito a un dominio di servizio o al dominio di controllo. Il dominio I/O è un obiettivo interessante in quanto offre potenziale accesso a un numero elevato di dispositivi su disco. Considerare pertanto questa minaccia quando si gestiscono dati sensibili in un dominio guest in esecuzione su dischi virtualizzati.

Contromisura: protezione dei dischi virtualizzati

Quando un dominio I/O è compromesso, l'intruso dispone di accesso completo ai dischi virtuali del dominio guest.

Proteggere il contenuto dei dischi virtuali effettuando le operazioni elencate di seguito.

- **Cifratura del contenuto dei dischi virtuali.** Nei sistemi Oracle Solaris 10 è necessario utilizzare un'applicazione in grado di cifrare i propri dati, come `pgp`/`gpg` o le tablespace cifrate di Oracle 11g. Nei sistemi Oracle Solaris 11 è necessario utilizzare i set di dati cifrati ZFS per fornire una cifratura trasparente di tutti i dati archiviati nel file system.
- **Distribuzione dei dati in più dischi virtuali in diversi domini I/O.** Un dominio guest deve creare un volume con striping (RAID 1/RAID 5) che esegue lo striping di più dischi virtuali ottenuti da due domini I/O. Se uno di questi domini I/O è compromesso, l'intruso avrà difficoltà nell'utilizzare la parte di dati disponibile.

Domini guest

Sebbene non facciano parte dell'ambiente di esecuzione, i domini guest costituiscono l'obiettivo più probabile di un attacco in quanto sono collegati alla rete. Un intruso che viola un sistema virtualizzato può attaccare l'ambiente di esecuzione.

Contromisura: protezione del SO del dominio guest

Il sistema operativo del dominio guest costituisce spesso la prima linea di difesa da qualsiasi attacco. Ad eccezione degli attacchi che hanno origine in un centro dati, un intruso deve violare un dominio guest dotato di connessioni esterne prima di tentare di violare l'isolamento del dominio guest e acquisire l'ambiente completo. È pertanto necessario rafforzare il SO di un dominio guest.

Per rafforzare ulteriormente il SO, è possibile implementare l'applicazione in Solaris Zones, aggiungendo un ulteriore livello di isolamento tra il servizio di rete dell'applicazione e il sistema operativo del dominio guest. Un attacco riuscito al servizio compromette solo la zona e non il sistema operativo sottostante, impedendo all'intruso di espandere il controllo oltre le risorse allocate alla zona. L'eventuale violazione dell'isolamento del dominio guest risulterà pertanto più difficile. Per ulteriori informazioni sulla protezione del SO del dominio guest, vedere *Oracle Solaris 10 Security Guidelines* e *Oracle Solaris 11 Security Guidelines*.

♦ ♦ ♦ CAPITOLO 2

Installazione e configurazione sicure di Oracle VM Server per SPARC

In questo capitolo sono riportate le considerazioni sulla sicurezza correlate all'installazione e alla configurazione del software Oracle VM Server per SPARC.

Installazione

Il software Oracle VM Server per SPARC viene installato automaticamente in modo sicuro come un pacchetto Oracle Solaris 11. Al termine dell'installazione, è necessario disporre dei privilegi di amministratore per configurare i domini con le funzioni relative a diritti e autorizzazione. Queste funzioni non sono abilitate per impostazione predefinita.

Configurazione postinstallazione

Effettuare le operazioni indicate di seguito dopo aver installato il software Oracle VM Server per SPARC per ottimizzare l'uso sicuro:

- Configurare il dominio di controllo con i servizi I/O virtuali necessari, come i servizi di switch virtuale, server su disco virtuale e concentratore di console virtuale. Vedere Capitolo 3, «Setting Up Services and the Control Domain» in *Oracle VM Server for SPARC 3.5 Administration Guide*.
- Configurare i domini guest. Vedere Capitolo 4, «Setting Up Guest Domains» in *Oracle VM Server for SPARC 3.5 Administration Guide*.

  È possibile utilizzare uno switch virtuale per configurare i domini guest mediante una rete amministrativa e una rete di produzione. In questo caso viene creato uno switch virtuale utilizzando l'interfaccia di rete di produzione come dispositivo di rete dello switch virtuale. Vedere sezione chiamata «Contromisura: configurazione di una rete di gestione dedicata» [26].

La sicurezza di un dominio guest viene compromessa quando viene compromesso uno qualsiasi dei dischi virtuali. Accertarsi quindi che i dischi virtuali (archivi collegati in rete, file immagine del disco archiviati in locale o dischi fisici) siano archiviati in un'ubicazione sicura.

Il daemon `vntsd` è disabilitato per impostazione predefinita. Quando questo daemon è abilitato, tutti gli utenti che hanno eseguito il login al dominio di controllo possono connettersi alla console di un dominio guest. Per impedire questo tipo di accesso, accertarsi che il daemon `vntsd` sia disabilitato oppure utilizzare i diritti per limitare l'accesso alla connettività della console *solo* agli utenti autorizzati.

- Il processore di servizio (SP, Service Processor) è configurato in modo sicuro per impostazione predefinita. Per informazioni sull'uso del software Oracle Integrated Lights Out Management (Oracle ILOM) per la gestione del processore di servizio, consultare la documentazione della piattaforma in uso all'indirizzo `http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html`.

♦ ♦ ♦ CAPITOLO 3

Considerazioni di sicurezza per gli sviluppatori

Questo capitolo fornisce informazioni agli sviluppatori di applicazioni per il software Oracle VM Server per SPARC.

Interfaccia XML di Oracle VM Server per SPARC

È possibile creare programmi esterni che interagiscono con il software Oracle VM Server per SPARC mediante il meccanismo di comunicazione XML (Extensible Markup Language). XML utilizza il protocollo XMPP (Extensible Messaging and Presence Protocol). L'interfaccia XML supporta solo la versione 1.2 del protocollo TLS (Transport Layer Security).

Poiché gli autori di attacchi potrebbero tentare di sfruttare il protocollo di rete XMPP per accedere a un sistema, si consiglia di disabilitarlo. Per informazioni sulla disabilitazione del protocollo XMPP, vedere «XML Transport» in *Oracle VM Server for SPARC 3.5 Developer's Guide*. Per informazioni sui meccanismi di sicurezza utilizzati da Logical Domains Manager, vedere «XMPP Server» in *Oracle VM Server for SPARC 3.5 Developer's Guide*.

La disabilitazione di XMPP impedisce a Oracle VM Manager o a Ops Center di gestire il sistema e impedisce all'utente di utilizzare alcune funzioni chiave di Oracle VM Server per SPARC come i comandi riportati di seguito.

- `ldm migrate-domain`
- `ldm init-system`
- `ldm remove-core -g`
- `ldm add-memory`
- `ldm set-memory`
- `ldm remove-memory`
- `ldm grow-socket`
- `ldm shrink-socket`
- `ldm set-socket`
- `ldm list-socket`

♦ ♦ ♦ APPENDICE A

Lista di controllo di distribuzione sicura

La presente lista di controllo riassume le operazioni che è possibile eseguire per rendere l'ambiente Oracle VM Server per SPARC più sicuro. Le informazioni dettagliate vengono fornite in altri documenti, come quelli elencati di seguito.

- *Oracle VM Server for SPARC 3.5 Administration Guide*
- *Oracle Solaris 10 Security Guidelines*
- *Oracle Solaris 11 Security Guidelines*

Lista di controllo di sicurezza di Oracle VM Server per SPARC

- Eseguire le operazioni per rendere più sicuro SO Oracle Solaris nei domini guest come se si trattasse di un ambiente non virtualizzato.
- Utilizzare i profili dei diritti LDoms Management e LDoms Review per delegare i privilegi appropriati agli utenti.
- Utilizzare i diritti per limitare l'accesso alla console dei domini alla quale deve accedere *solo* l'amministratore di Oracle VM Server per SPARC.
- Disabilitare i servizi di gestione dei domini non necessari.
- Implementare solo i domini guest della stessa classe di sicurezza in una piattaforma fisica.
- Accertarsi che non siano presenti connessioni di rete tra la rete di amministrazione dell'ambiente di esecuzione e i domini guest.
- Assegnare solo le risorse necessarie ai domini guest.