# Guida per la sicurezza del sistema modulare Netra

**N. di parte: E68386-01**
Agosto 2015

**N. di parte: E68386-01**



**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

# Panoramica sulla sicurezza

Sistema modulare Netra di Oracle è una piattaforma preintegrata e precablata che può essere virtualizzata completamente per ridurre i costi e i tempi di distribuzione nel centro dati. Il sistema modulare include i componenti hardware specificati e viene assemblato in fabbrica e spedito al cliente.

Negli argomenti elencati di seguito vengono descritti i concetti e le funzioni di sicurezza per il sistema modulare.


- sezione chiamata «Principi di sicurezza di base» [7]
- sezione chiamata «Considerazioni avanzate sulla sicurezza» [8]
- sezione chiamata «Funzioni di sicurezza» [9]


## Principi di sicurezza di base

Attenersi ai principi di sicurezza di base elencati di seguito per tutti i componenti software e hardware del sistema modulare.

- Autenticazione: l'autenticazione indica il modo in cui un utente viene identificato, in genere mediante informazioni riservate quali il nome utente e la password o le chiavi condivise. L'autenticazione garantisce la convalida degli utenti di hardware o software. Per impostazione predefinita, per l'autenticazione vengono utilizzati i nomi utente e le password locali. È disponibile anche l'autenticazione basata sulle chiavi condivise.
- Accounting e controllo: l'accounting e il controllo consentono di gestire un record dell'attività dell'utente sul sistema. Le funzionalità hardware e software del sistema modulare consentono agli amministratori di monitorare l'attività di login e gestire gli inventari hardware.
  - I login utente vengono monitorati mediante i log di sistema. Gli account di servizio e amministratore di sistema dispongono di privilegi per l'accesso a comandi che, se usati in modo errato, possono causare danni e perdita di dati.
  - Gli asset hardware vengono tracciati tramite i numeri di serie. I numeri di parte Oracle sono registrati elettronicamente su tutte le schede, i moduli e le schede madri ed è possibile utilizzarli per l'inventario.

# Considerazioni avanzate sulla sicurezza

Oltre ai principi di sicurezza di base, il sistema modulare è caratterizzato da capacità di sopravvivenza e difesa avanzata. Il sistema modulare offre una serie di funzionalità di sicurezza bene integrate in grado di soddisfare importanti requisiti di sicurezza e problemi correlati. Nelle sezioni che seguono vengono descritti questi principi.

- Capacità di sopravvivenza dei carichi di lavoro mission-critical: le organizzazioni che selezionano piattaforme hardware e software per carichi di lavoro mission-critical possono contare sulla capacità del sistema modulare di impedire o ridurre al minimo i danni causati da azioni accidentali e non autorizzate eseguite da utenti interni o esterni. Le best practice indicate di seguito, incluse in Oracle Maximum Availability Architecture, migliorano la capacità di sopravvivenza.
  - Garantisce che i componenti utilizzati siano stati progettati, costruiti e testati per funzionare correttamente insieme a supporto delle architetture per la distribuzione sicura. Il sistema modulare supporta l'isolamento sicuro, il controllo dell'accesso, la qualità del servizio e la gestione sicura.
  - La riduzione della superficie di attacco predefinita dei relativi prodotti costituenti contribuisce a ridurre l'esposizione generale del sistema.
  - Garantisce la protezione del sistema, incluse le interfacce operative e di gestione, con un insieme di protocolli aperti e controllati e di interfacce API in grado di supportare gli obiettivi di sicurezza tradizionali di autenticazione complessa, controllo dell'accesso, riservatezza, integrità e disponibilità.
  - Verifica che i componenti software e hardware contengano funzioni in grado di garantire la disponibilità del servizio anche in caso di errori o guasti. Queste funzionalità sono di aiuto in caso di attacchi volti a disabilitare uno o più singoli componenti del sistema.
- Difesa avanzata per la protezione dell'ambiente operativo: il sistema modulare utilizza più controlli di sicurezza indipendenti e che si rafforzano a vicenda, che contribuiscono a creare un ambiente operativo sicuro per carichi di lavoro e dati. Il sistema modulare supporta il principio di difesa avanzata nei modi indicati di seguito.
  - Offre un insieme di valide protezioni per garantire la sicurezza delle informazioni in transito, in uso e archiviate. I controlli di sicurezza sono disponibili ai livelli di server e di rete. I controlli di sicurezza univoci per ciascun livello possono essere integrati con gli altri per consentire la creazione di architetture di sicurezza affidabili su più livelli.
  - Supporta l'uso di standard, protocolli e interfacce aperti e ben definiti. Il sistema modulare può essere integrato in criteri, architetture, procedure e standard di sicurezza esistenti.

# Funzioni di sicurezza

I componenti hardware e software del sistema modulare sono stati potenziati. Oracle fornisce anche configurazioni sicure consigliate per servizi come NTP e SSH. L'architettura del sistema modulare, inoltre, offre funzionalità di sicurezza ai componenti principali. Tali funzionalità vengono spesso applicate dalle organizzazioni che distribuiscono una strategia di sicurezza su più livelli. Le funzionalità sono raggruppate nelle categorie riportate di seguito.

- sezione chiamata «Isolamento del traffico di rete» [9]
- sezione chiamata «Oracle ILOM per la gestione sicura» [9]

## Isolamento del traffico di rete

Se si desidera consolidare l'infrastruttura IT, implementare le architetture dei servizi condivisi e offrire servizi multi-tenant sicuri, considerare l'isolamento del traffico di rete. Il sistema modulare offre la flessibilità necessaria per implementare i criteri e le strategie di isolamento in base alle proprie esigenze.

A livello di rete fisica, l'accesso al client è isolato dalla gestione del dispositivo e dalla comunicazione tra dispositivi. Il client e la gestione del traffico di rete sono isolati su reti separate. L'accesso al client viene fornito su una rete Ethernet ridondante da 10 Gbps che garantisce un accesso affidabile ad alta velocità ai servizi in esecuzione sul sistema. L'accesso alla gestione viene fornito su una rete Ethernet da 1 Gbps separata fisicamente. In questo modo si ottiene una separazione tra reti operative e reti di gestione.

Le organizzazioni possono scegliere di isolare ulteriormente il traffico di rete sulla rete Ethernet di accesso al client configurando LAN virtuali (VLAN). Le VLAN isolano il traffico di rete in base agli specifici requisiti. Per garantire la riservatezza e l'integrità delle comunicazioni, Oracle consiglia di utilizzare protocolli cifrati nelle VLAN.

## Oracle ILOM per la gestione sicura

Per proteggere in modo appropriato le singole applicazioni e i singoli servizi, sono necessarie raccolte di controlli e funzionalità di sicurezza. Per sostenere la sicurezza dei servizi e dei sistemi distribuiti, è ugualmente importante disporre di funzionalità di gestione complete. Il sistema modulare utilizza le funzionalità di gestione di sicurezza di Oracle ILOM.

Oracle ILOM è un SP incorporato nei nodi di calcolo del sistema modulare. Oracle ILOM viene utilizzato per eseguire attività di gestione fuori banda, come quelle elencate di seguito.

- Offrire accesso sicuro per eseguire una gestione lights-out sicura del database e dei server di memorizzazione. 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 di controllo dell'accesso basato su ruoli. Ai singoli utenti vengono assegnati ruoli specifici che limitano le funzioni che è possibile eseguire.
- Fornire un log di controllo di tutte le modifiche a login e configurazione. Ciascuna voce del log di controllo mostra l'utente che esegue l'azione e un indicatore di data e ora. Il record di controllo consente alle organizzazioni di rilevare attività o modifiche non autorizzate e attribuisce queste azioni a utenti specifici.

Per ulteriori informazioni sulla sicurezza di Oracle ILOM, fare riferimento al manuale *Oracle ILOM Security Guide* all'indirizzo `http://www.oracle.com/goto/ILOM/docs`.

# Pianificazione di un ambiente sicuro

Prima dell'arrivo di Sistema modulare Netra, implementare le linee guida sulla sicurezza. Una volta installato il sistema, esaminare e modificare periodicamente le linee guida sulla sicurezza in modo da renderle conformi ai requisiti di sicurezza correnti dell'organizzazione.

Negli argomenti riportati di seguito vengono illustrate le linee guida sulla sicurezza per l'installazione di Sistema modulare Netra.

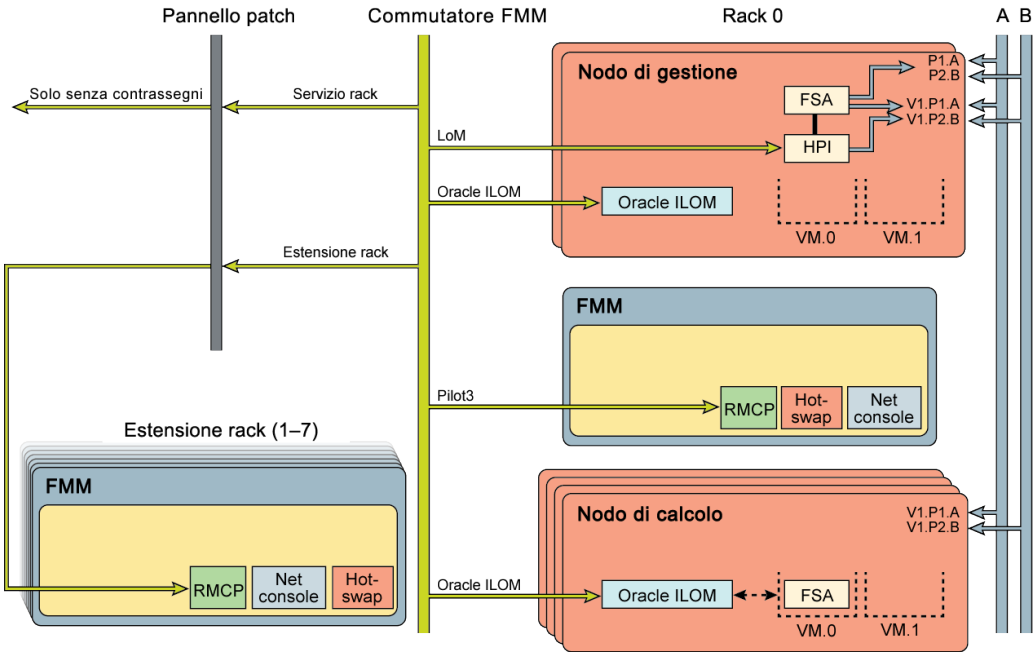

- sezione chiamata «Rete predefinita» [11]
- sezione chiamata «Account utente» [12]
- sezione chiamata «Impostazioni di sicurezza predefinite» [12]


Per i requisiti di sicurezza aggiuntivi relativi al sistema e all'ambiente specifico, contattare il responsabile della sicurezza IT.

## Rete predefinita

Nella figura e nelle descrizioni seguenti viene illustrata la rete predefinita per Sistema modulare Netra.

- La rete di sistema/telemetria (rete verde chiaro) include la porta LoM del nodo di gestione sulla VLAN 4090 con switch FMM.
- La rete ILOM di telemetria su una VLAN 4094 interna con FMM include Oracle ILOM nei nodi di calcolo e nei nodi di rete con switch FMM.
- Il pannello delle patch estende la rete di telemetria ai rack 1-7. Una configurazione con più rack supporta le stesse sottoreti e VLAN con un ID di rack diverso.
- La VLAN(1) fornisce altri servizi alla rete di telemetria tramite un'appropriata autenticazione.
- Le reti di dati (A e B) offrono l'accesso in banda al nodo FSA.
- L'applicazione HA può gestire i rack tramite le interfacce esposte del sistema modulare (JMX, C- API e così via).




# Account utente

In questa tabella sono elencati gli utenti e le password predefiniti per i componenti del sistema modulare. Modificare tutte le password predefinite dopo avere installato Sistema modulare Netra.

| Componente | Nome utente e password |
|---|---|
| Switch Ethernet | `root/changeme`<br>**Nota -** Proteggere i valori `enable mode password` e `secret` per l'utente `admin`. |
| Nodi di gestione e di calcolo | `root/changeme` |

# Impostazioni di sicurezza predefinite

Il sistema modulare viene installato con molte impostazioni di sicurezza predefinite. Se possibile e realizzabile, configurare le impostazioni predefinite sicure. Fare riferimento alle impostazioni predefinite nella propria versione di Oracle ILOM all'indirizzo `http://www.oracle.com/goto/ILOM/docs`.

# Protezione dell'hardware

L'isolamento fisico e il controllo dell'accesso costituiscono gli elementi di base per la creazione dell'architettura di sicurezza. L'installazione in un ambiente sicuro protegge il sistema dagli accessi non autorizzati. Allo stesso modo, la registrazione di tutti i numeri di serie aiuta a evitare l'uso di componenti hardware non autorizzati.

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



## Limitazioni di accesso

- Installare i sistemi e le apparecchiature correlate in una stanza chiusa a chiave con accesso limitato.
- Se le apparecchiature sono installate in un rack dotato di sportello, chiudere sempre lo sportello finché non sarà necessario effettuare un intervento sui componenti contenuti nel rack. La chiusura degli sportelli limita anche l'accesso ai dispositivi con collegamento o swapping a caldo.
- Conservare tutte le parti di ricambio in un cabinet chiuso. Consentire l'accesso a tale armadietto solo al personale autorizzato.
- Verificare periodicamente lo stato e l'integrità delle serrature nel rack e dell'armadietto dei ricambi per evitare o rilevare eventuali tentativi di manomissione o sportelli lasciati inavvertitamente aperti.
- Conservare le chiavi dell'armadietto in un luogo sicuro con accesso limitato.
- Limitare l'accesso alle console USB. Dispositivi quali i controller di sistema, le PDU e gli switch di rete possono essere dotati di connessioni USB. L'accesso fisico è il metodo di accesso a un componente più sicuro, in quanto non è soggetto ad attacchi che sfruttano la rete.
- Connettere la console a un dispositivo KVM esterno per abilitare l'accesso remoto alla console. I dispositivi KVM supportano spesso l'autenticazione basata su due fattori: il controllo dell'accesso centralizzato e l'audit. Per ulteriori informazioni sulle istruzioni

di sicurezza e sulle procedure ottimali per i dispositivi KVM, fare riferimento alla documentazione fornita con il dispositivo KVM in uso.

# Numeri di serie

Per impedire l'uso di componenti hardware non autorizzati, registrare attentamente tutti i numeri di serie quando si ricevono i componenti e se ne esegue l'inventario. Prima di installare o utilizzare qualsiasi componente, verificarne l'autenticità confrontandone il numero di serie con quello registrato al momento della ricezione. Attenersi alle procedure indicate di seguito per proteggere i componenti hardware.

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

I reader wireless RFID (Radio Frequency Identification) consentono di semplificare ulteriormente la registrazione degli asset. Fare riferimento al white paper Oracle *How to Track Your Oracle Sun System Assets by Using RFID*, all'indirizzo `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`.

# Unità disco rigido

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

- 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.

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

# Protezione del software

La sicurezza dell'hardware viene garantita principalmente tramite l'implementazione di misure software. Nelle sezioni indicate vengono fornite le linee guida generali relative alla sicurezza del software per Sistema modulare Netra.



## Prevenzione dell'accesso non autorizzato (Oracle Linux)

- **Utilizzare i comandi del sistema operativo Oracle Linux per limitare l'accesso al software, rafforzare il sistema operativo, utilizzare le funzioni di sicurezza e proteggere le applicazioni.**
  Fare riferimento al manuale *Oracle Linux Security Guide for Release 6* all'indirizzo `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`.

## Prevenzione dell'accesso non autorizzato (Oracle ILOM)

- **Utilizzare i comandi Oracle ILOM per limitare l'accesso al firmware di Oracle ILOM, modificare la password impostata in fabbrica, limitare l'utilizzo dell'account superutente root e proteggere la rete privata presso il processore di servizi.**
  Fare riferimento alla propria versione del manuale *Oracle ILOM Security Guide* all'indirizzo `http://www.oracle.com/goto/ILOM/docs`.

## Prevenzione dell'accesso non autorizzato (Oracle VM Server con Oracle Linux)

- **Utilizzare i comandi del sistema operativo Oracle Linux per limitare l'accesso al software Oracle VM Server, utilizzare le funzioni di sicurezza e proteggere le applicazioni.**

Fare riferimento al manuale *Oracle VM Security Guide for Release 3.3* all'indirizzo http://docs.oracle.com/cd/E50245_01/E50254/html/index.html.

# Sicurezza di Oracle Hardware Management Pack

Oracle Hardware Management Pack include due componenti: un agente di monitoraggio SNMP e una gamma di strumenti CLI (Command Line Interface, interfaccia a riga di comando) per la gestione del sistema.

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

  I plugin SNMP possono essere eseguiti sul sistema operativo host dei sistemi Oracle. Il plugin SNMP estende l'agente SNMP nativo nel sistema operativo host per fornire funzionalità aggiuntive di Oracle MIB. Oracle Hardware Management Pack stesso non contiene un agente SNMP. Per Oracle Linux, viene aggiunto un modulo all'agente `net-snmp`. Per Microsoft Windows, il plugin estende il servizio SNMP nativo. Tutte le impostazioni di sicurezza relative a SNMP per Oracle Hardware Management Pack vengono determinate dalle impostazioni dell'agente o servizio SNMP nativo e non dal plugin.

  SNMPv1 e SNMPv2c non forniscono alcuna cifratura e utilizzano stringhe comunità come metodo di autenticazione. SNMPv3 è più sicuro ed è la versione consigliata poiché utilizza la cifratura per fornire un canale sicuro, nonché password e nomi utente singoli.
- Documentazione di Oracle Hardware Management Pack: per le linee guida di sicurezza specifiche di Oracle Hardware Management Pack, fare riferimento al manuale *Oracle Hardware Management Pack (HMP) Security Guide* all'indirizzo http://www.oracle.com/goto/OHMP/docs.

# Ricerca delle guide per la sicurezza correlate

## Guida per la sicurezza

Nelle guide riportate di seguito sono descritti i criteri e le procedure per proteggere i prodotti correlati.

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Oracle Linux Security Guide for Release 6* all'indirizzo `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- *Oracle ILOM Security Guide* all'indirizzo `http://www.oracle.com/goto/ILOM/docs`
- *Oracle VM Security Guide for Release 3.3* all'indirizzo `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- *Oracle Hardware Management Pack (HMP) Security Guide* all'indirizzo `http://www.oracle.com/goto/OHMP/docs`