Sun Server X3-2 (precedentemente Sun Fire X4170 M3)

Guida per la sicurezza

N. di parte: E35510-02
Settembre 2013

Indice

• • • Capitolo 1

Guida per la sicurezza di Sun Server X3-2

In questo documento vengono fornite le linee guida di sicurezza generali per garantire la sicurezza di Oracle Sun Server X3-2, delle relative interfacce di rete e dei commutatori di rete ai quali è connesso.

Nota

Sun Server X3-2 era precedentemente denominato server Sun Fire X4170 M3. Il nome precedente potrebbe ancora comparire all'interno del software. Il nuovo nome del prodotto non indica alcuna modifica a funzionalità o funzioni di sistema.

Nel capitolo sono disponibili le seguenti sezioni:

Panoramica del sistema

Sun Server X3-2 è un server unità a un rack (1U) per le imprese. Questo server supporta i seguenti componenti:

- Fino a due processori Intel. Sono inoltre supportati i processori con le funzionalità seguenti:
  - 2,4 GHz, 4 core, 80 W
  - 2,5 GHz, 6 core, 95 W
  - 2,2 GHz, 8 core, 95 W
  - 2,9 GHz, 8 core, 135 W
- Fino a 8 DIMM per processore per un massimo di 16 DIMM DDR3 e un massimo di 512 GB di memoria su sistemi con doppio processore. Sono supportate dimensioni DIMM di 8 GB, 16 GB e 32 GB.

Nota

Sono supportati un massimo di 8 DIMM per un massimo di 256 GB su sistemi con processore singolo.

- Quattro slot PCIe Gen3 in sistemi con doppio processore, di cui tre esterne e una interna. La slot PCIe 1 esterna non è operativa nei sistemi con processore singolo.
- Le configurazioni dell'unità di archiviazione possono includere sia unità disco rigido (HDD, hard disk drives) sia unità stato solido (SSD, solid state disk). Le configurazioni unità di archiviazione supportate includono:
  - Fino a quattro HDD SAS hot-pluggable da 3,5 pollici
  - Fino a quattro HDD/SSD SAS/SATA hot-pluggable da 2,5 pollici con DVD
  - Fino a otto HDD/SSD SAS/SATA hot-pluggable da 2,5 pollici
- Due alimentatori ridondanti hot-pluggable.
- Un processore di servizio Oracle Integrated Lights Out Manager (Oracle ILOM) integrato basato sul chip AST2300 che fornisce una gestione locale e remota sicura.
- Lo strumento di impostazione server Oracle System Assistant, integrato in un'unità flash USB preinstallata.

Principi di sicurezza

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

- **Accesso**

  L'accesso fa riferimento all'accesso fisico all'hardware o all'accesso fisico o virtuale al software.
  - Eseguire controlli fisici e al software per proteggere il proprio hardware e i dati da eventuali intrusioni.
  - Fare riferimento alla documentazione fornita con il software per attivare le funzionalità di sicurezza disponibili per il software.
  - Installare i server e le apparecchiature relative in una stanza il cui accesso è riservato.
  - Se l'apparecchiatura è installata in uno scaffale dotato di sportello, non lasciare mai lo sportello aperto, tranne quando è necessario agire sui componenti al suo interno.
  - Limitare l'accesso a connettori o porte, che costituiscono un migliore punto di accesso rispetto alle connessioni SSH. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU, power distribution unit) e i commutatori di rete forniscono connettori e porte.
  - Limitare l'accesso in particolare a dispositivi con collegamento o swapping a caldo, in quanto possono essere facilmente rimossi.
  - Conservare le unità sostituibili sul campo (FRU, field-replaceable units) e le unità sostituibili dall'utente (CRU, customer-replaceable unit) di riserva in un armadietto chiuso a chiave. Consentire l'accesso all'armadietto solo al personale autorizzato.
- **Autenticazione**

  L'autenticazione garantisce la convalida degli utenti hardware o software.
  - Impostare funzionalità di autenticazione, come ad esempio un sistema di password, nei sistemi operativi della piattaforma per garantire la convalida degli utenti.
  - Verificare che tutto il personale utilizzi correttamente i badge per accedere alla sala computer.

- Per gli account utente: utilizzare, se necessario, le liste di controllo degli accessi; impostare time-out per sessioni troppo prolungate; impostare livelli di privilegi per gli utenti.

- **Autorizzazione**

  L'autorizzazione fa riferimento alle limitazioni per il personale in merito all'utilizzo di hardware o software.

  - Consentire al personale di utilizzare l'hardware e il software solo se correttamente formato a tale scopo.
  - Impostare un sistema di autorizzazioni di lettura, scrittura ed esecuzione per controllare l'accesso utente a comandi, spazio su disco, dispositivi e applicazioni.

- **Accounting**

  L'accounting fa riferimento a funzionalità software e hardware utilizzate per monitorare l'attività di login e la manutenzione degli inventari hardware.

  - Utilizzare i registri di sistema per monitorare i login utente. Monitorare gli account di servizio e amministratore di sistema in particolare, in quanto forniscono importanti comandi.
  - Conservare un record dei numeri di serie dell'intero hardware. Utilizzare i numeri di serie del componente per monitorare gli asset di sistema. I codici parte di Oracle sono registrati elettronicamente su schede, moduli e schede madri.
  - Per rilevare e monitorare i componenti, fornire un contrassegno di sicurezza per tutti gli elementi significativi dell'hardware del computer, come le FRU. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.

Uso degli strumenti di gestione e configurazione server

Seguire le linee guida di sicurezza durante l'utilizzo di strumenti firmware e software per configurare e gestire il server.

- sezione chiamata «Sicurezza di Oracle System Assistant» [7]
- sezione chiamata «Sicurezza di Oracle ILOM» [8]
- sezione chiamata «Sicurezza di Oracle Hardware Management Pack» [9]

Sicurezza di Oracle System Assistant

Oracle System Assistant è uno strumento preinstallato che consente di aggiornare e configurare localmente o in remoto l'hardware server e di installare i sistemi operativi supportati. Per informazioni sull'utilizzo di Oracle System Assistant, fare riferimento alla *guida di amministrazione di Sun Server X3-2*, all'indirizzo:

http://www.oracle.com/pls/topic/lookup?ctx=SunServerX3-2

Le seguenti informazioni consentono di analizzare i problemi di sicurezza di Oracle System Assistant.

- **Oracle System Assistant contiene un ambiente root di boot**

Oracle System Assistant è un'applicazione eseguita in un'unità flash USB interna e preinstallata ed è situata in un ambiente root Linux di boot. Oracle System Assistant garantisce inoltre la possibilità di accedere a una shell root sottostante. Gli utenti con accesso fisico al sistema o che dispongono dell'accesso remoto a tastiera, video, mouse e archiviazione tramite Oracle ILOM, potranno accedere a Oracle System Assistant e alla shell root.

È possibile utilizzare un ambiente di root per modificare i criteri e la configurazione di sistema, nonché per accedere ai dati su altri dischi. Si consiglia di proteggere l'accesso fisico al server e assegnare privilegi console e amministratore agli utenti Oracle ILOM con moderazione.

- **In Oracle System Assistant è disponibile un dispositivo di memorizzazione USB accessibile dal sistema operativo**

Oltre a essere un ambiente di boot, Oracle System Assistant prevede inoltre un dispositivo di memorizzazione USB (unità flash) accessibile dal sistema operativo host dopo l'installazione. Tutto ciò è utile quando si accede agli strumenti e ai driver per attività di manutenzione e riconfigurazione. Il dispositivo di memorizzazione USB Oracle System Assistant è leggibile e scrivibile e può essere soggetto all'attacco di virus.

Si consiglia di utilizzare gli stessi metodi di protezione dei dischi nel dispositivo di memorizzazione Oracle System Assistant, compresi scansione regolare dei virus e verifica dell'integrità.

- **È possibile disattivare Oracle System Assistant**

Oracle System Assistant è un utile strumento per l'impostazione del server, l'aggiornamento e la configurazione del firmware e l'installazione del sistema operativo host. Tuttavia, se non è possibile accettare le limitazioni di sicurezza descritte sopra o se lo strumento non è necessario, Oracle System Assistant può essere disattivato. Disattivando Oracle System Assistant non sarà più possibile accedere al dispositivo di memorizzazione USB dal sistema operativo host. Inoltre, non sarà possibile eseguire il boot di Oracle System Assistant.

È possibile disattivare Oracle System Assistant dallo strumento stesso o da BIOS. Una volta disattivato, Oracle System Assistant può essere attivato nuovamente solo dall'utilità di impostazione del BIOS. Si consiglia di proteggere con una password l'impostazione del BIOS, in modo che solo gli utenti autorizzati possano attivare nuovamente Oracle System Assistant. Per informazioni su come disabilitare o abilitare nuovamente Oracle System Assistant, fare riferimento alla *guida di amministrazione di Sun Server X3-2*.

Sicurezza di Oracle ILOM

È possibile proteggere, gestire e monitorare attivamente i componenti di sistema mediante il firmware di gestione di Oracle ILOM (Oracle Integrated Lights Out Manager), preinstallato su Sun Server X3-2, altri server basati su Oracle x86 e su alcuni server basati su SPARC Oracle.

Utilizzare una rete interna dedicata per il processore di servizio per separarlo dalla rete generale. Oracle ILOM fornisce agli amministratori di sistema funzioni di controllo e monitoraggio del server. A seconda del livello di autorizzazione concesso agli amministratori, queste funzioni possono includere la possibilità di spegnere il server, creare account utente, installare dispositivi di memorizzazione remoti e così via. Pertanto, per mantenere un ambiente il più affidabile e sicuro possibile per Oracle ILOM, la porta di gestione di rete dedicata o la porta di gestione di banda laterale sul server deve essere sempre collegata a una rete affidabile interna o a una rete di gestione/privata sicura dedicata.

Limitare l'utilizzo dell'account amministratore predefinito (**root**) al login iniziale a Oracle ILOM. Questo account amministratore predefinito viene fornito solo per facilitare l'installazione iniziale del server. Pertanto, per garantire un ambiente il più sicuro possibile, è necessario modificare la password predefinita dell'amministratore (**changeme**) durante l'impostazione iniziale del sistema. Per ogni nuovo utente Oracle ILOM è necessario definire nuovi account utente con password univoche e livelli di autorizzazione assegnati, oltre alla possibilità di modificare la password per l'account amministratore predefinito.

Fare riferimento alla documentazione di Oracle ILOM per ottenere maggiori informazioni sull'impostazione di password, la gestione degli utenti e l'applicazione di funzionalità relative alla sicurezza, comprese l'autenticazione Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS. Per le linee guida relative alla sicurezza specifiche per Oracle ILOM, fare riferimento alla *guida per la sicurezza di Oracle Integrated Lights Out Manager (ILOM) 3.1*, che fa parte della libreria della documentazione di Oracle ILOM 3.1. È possibile reperire la documentazione Oracle ILOM 3.1 all'indirizzo:

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

Sicurezza di Oracle Hardware Management Pack

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

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

È possibile utilizzare gli strumenti CLI di Oracle Server per configurare i server Oracle. Gli strumenti CLI sono compatibili con Oracle Solaris, Oracle Linux, Oracle VM, altre varianti di Linux e sistemi operativi Microsoft Windows.

Fare riferimento alla documentazione Oracle Hardware Management Pack per maggiori informazioni su queste funzionalità. Per le linee guida relative alla sicurezza specifiche per Oracle Hardware Management Pack, fare riferimento alla *guida per la sicurezza di Oracle Hardware Management Pack (HMP)*, che fa parte della libreria della documentazione di Oracle Hardware Management Pack. È possibile reperire la documentazione di Oracle Hardware Management Pack all'indirizzo:

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

Pianificazione di un ambiente sicuro

Utilizzare le seguenti informazioni durante l'installazione e la configurazione del server e della relativa apparecchiatura.

- sezione chiamata «Linee guida del sistema operativo Oracle» [9]
- sezione chiamata «Commutatori e porte di rete» [10]
- sezione chiamata «Sicurezza VLAN» [10]
- sezione chiamata «Sicurezza di Infiniband» [11]
- sezione chiamata «Sicurezza fisica dell'hardware» [11]
- sezione chiamata «Sicurezza del software» [11]

Linee guida del sistema operativo Oracle

Fare riferimento ai documenti del sistema operativo Oracle per informazioni su:

- Come utilizzare le funzionalità di sicurezza durante la configurazione dei sistemi.

- Come eseguire operazioni in maniera sicura durante l'aggiunta di applicazioni e utenti a un sistema.
- Come proteggere le applicazioni basate sulla rete.

I documenti della guida di sicurezza per i sistemi operativi Oracle supportati sono parte della libreria della documentazione del sistema operativo. Per consultare il documento della guida di sicurezza di un sistema operativo Oracle, individuare la libreria della documentazione del sistema operativo Oracle:

- **Oracle Solaris 10 1/13** - http://www.oracle.com/goto/Solaris10/docs
- **Oracle Solaris 11.1** - http://www.oracle.com/goto/Solaris11/docs
- **Oracle Linux** - http://www.oracle.com/technetwork/documentation/ol-1861776.html
- **Oracle VM** - http://www.oracle.com/technetwork/documentation/vm-096300.html

  Per informazioni sui sistemi operativi di altri fornitori, ad esempio Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows e VMware ESXi, fare riferimento alla documentazione del fornitore.

Commutatori e porte di rete

Diversi commutatori offrono differenti livelli di funzionalità di sicurezza delle porte. Fare riferimento alla documentazione relativa ai commutatori per maggiori informazioni sulle operazioni seguenti.

- Utilizzare funzionalità di autenticazione, autorizzazione e accounting per l'accesso locale e remoto al commutatore.
- Modificare tutte le password dei commutatori di rete che potrebbero presentare, per impostazione predefinita, più password e account utente.
- Eseguire la gestione fuori banda dei commutatori (separati dal traffico dati). Se non è possibile eseguire la gestione fuori banda, predisporre un numero VLAN (rete locale virtuale) per la gestione in banda.
- Utilizzare la funzionalità di uso di copie sincronizzate del commutatore di rete per accedere all'IDS (intrusion detection system).
- Conservare offline un file di configurazione del commutatore e limitarne l'accesso solo agli amministratori autorizzati. Nel file di configurazione dovrebbero essere contenuti commenti descrittivi per ciascuna impostazione.
- Implementare la sicurezza della porta per limitare l'accesso basato su indirizzi MAC. Disattivare il trunking automatico in tutte le porte.
- Utilizzare queste funzionalità di sicurezza della porta se disponibili nel commutatore in uso:
  - La funzione di **bloccaggio MAC** prevede l'associazione di un indirizzo MAC (Media Access Control) di uno o più dispositivi connessi a una porta fisica su un commutatore. Se viene bloccata una porta commutatore di uno specifico indirizzo MAC, ai superutenti non sarà consentito creare backdoor nella rete con punti di accesso rogue.
  - La funzione di **blocco MAC** consente di disattivare la connessione di un indirizzo MAC a un commutatore.
  - La funzione di **apprendimento MAC** consente di utilizzare le informazioni su ciascuna connessione diretta della porta commutatore, in modo che sia possibile per il commutatore di rete impostare la sicurezza in base alle connessioni correnti.

Sicurezza VLAN

Se viene impostata una rete locale virtuale (VLAN), tenere presente che le VLAN condividono la larghezza di banda della rete e richiedono misure di sicurezza aggiuntive.

- Definire le reti VLAN per separare i cluster sensibili dei sistemi dal resto della rete. In questo modo viene limitata la possibilità che gli utenti possano accedere alle informazioni su questi client e server.
- Assegnare un numero VLAN nativo univoco alle porte trunk.
- Limitare le reti VLAN trasportabili tramite trunk unicamente a quelle strettamente necessarie.
- Disattivare il protocollo VTP (VLAN Trunking Protocol), se possibile. In alternativa, impostare le seguenti opzioni per VTP: eliminazione, password e dominio di gestione. Quindi, impostare il protocollo VTP in modalità trasparente.

Sicurezza di Infiniband

Proteggere gli host Infiniband. Un fabric Infiniband è sicuro quanto il relativo host Infiniband meno sicuro.

- Il partizionamento non protegge un fabric Infiniband. Il partizionamento offre solo l'isolamento del traffico Infiniband tra macchine virtuali su un host.
- Utilizzare una configurazione VLAN statica, ove possibile.
- Disattivare le porte commutatore non utilizzate e assegnare loro un numero VLAN non utilizzato.

Sicurezza fisica dell'hardware

I componenti hardware fisici possono essere protetti in modo relativamente semplice limitando l'accesso e registrando i numeri di serie.

- **Limitazione dell'accesso**
  - Installare i server e le apparecchiature relative in una stanza il cui accesso è riservato.
  - Se l'apparecchiatura è installata in uno scaffale dotato di sportello, non lasciare mai lo sportello aperto, tranne quando è necessario agire sui componenti al suo interno. Chiudere lo sportello dopo qualsiasi intervento sull'apparecchiatura.
  - Limitare l'accesso alle connessioni USB, che costituiscono un migliore punto di accesso rispetto alle connessioni SSH. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU, Power Distribution Unit) e i commutatori di rete possono essere dotati di connessioni USB.
  - Limitare l'accesso in particolare a dispositivi con collegamento o swapping a caldo, in quanto possono essere facilmente rimossi.
  - Conservare le unità sostituibili sul campo (FRU, field-replaceable units) o le unità sostituibili dall'utente (CRU, customer-replaceable unit) di riserva in un armadietto chiuso a chiave. Consentire l'accesso all'armadietto solo al personale autorizzato.
- **Registrazione dei numeri di serie**
  - Posizionare un contrassegno di sicurezza su tutti gli elementi significativi dell'hardware del computer, come le FRU. Utilizzare speciali penne a luce ultravioletta o etichette in rilievo.
  - Conservare un record dei numeri di serie dell'intero hardware.
  - Conservare le chiavi di attivazione hardware e le 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.

Sicurezza del software

La sicurezza dell'hardware viene garantita principalmente tramite l'implementazione di misure software.

- Modificare tutte le password predefinite durante l'installazione di un nuovo sistema. Molti tipi di apparecchiature utilizzano password predefinite, come **changeme**, conosciute a livello globale e per questo motivo non sicure contro gli accessi non autorizzati.
- Modificare tutte le password dei commutatori di rete che potrebbero presentare, per impostazione predefinita, più password e account utente.
- Limitare l'utilizzo dell'account amministratore predefinito (**root**) a un unico utente amministratore. Creare sempre un nuovo account Oracle ILOM per ogni nuovo utente. Assicurarsi che a ciascun account utente Oracle ILOM siano sempre assegnati una password univoca e un livello appropriato di privilegi di autorizzazione (operatore, amministratore e così via).
- Utilizzare una rete dedicata per i processori di servizio per separarli dalla rete generale.
- Proteggere l'accesso alle connessioni USB. Dispositivi quali i controller di sistema, le unità di distribuzione dell'alimentazione (PDU) e i commutatori di rete possono essere dotati di connessioni USB, che costituiscono un migliore punto di accesso rispetto alle connessioni SSH.
- Fare riferimento alla documentazione fornita con il software per attivare le funzionalità di sicurezza disponibili per il software.
- Implementare la sicurezza delle porte per limitare l'accesso basato su indirizzi MAC. Disattivare il trunking automatico in tutte le porte.

Mantenimento di un ambiente sicuro

Dopo aver eseguito l'installazione e la configurazione, utilizzare le funzionalità di sicurezza software e hardware Oracle per mantenere il controllo sull'hardware e tracciare gli asset di sistema.

- sezione chiamata «Controllo alimentazione hardware» [12]
- sezione chiamata «Tracciabilità dell'asset» [12]
- sezione chiamata «Aggiornamenti per software e firmware» [13]
- sezione chiamata «Accesso di rete» [13]
- sezione chiamata «Protezione e sicurezza dei dati» [14]
- sezione chiamata «Mantenimento del registro» [14]

Controllo alimentazione hardware

È possibile utilizzare il software per attivare o disattivare l'alimentazione di alcuni sistemi Oracle. È possibile attivare e disattivare da remoto le unità di distribuzione dell'alimentazione (PDU) per alcuni cabinet di sistema. L'autorizzazione per tali comandi è solitamente impostata durante la configurazione del sistema ed è limitata agli amministratori di sistema e al personale di servizio. Fare riferimento alla documentazione relativa a cabinet o sistema per ulteriori informazioni.

Tracciabilità dell'asset

Utilizzare i numeri di serie per tenere traccia dell'inventario. In Oracle vengono incorporati i numeri di serie nel firmware in schede opzione e schede madri di sistema. È possibile leggere questi numeri di serie mediante connessioni di rete locali.

È inoltre possibile utilizzare lettori wireless di identificazione a radiofrequenza (RFID, radio frequency identification) per semplificare ulteriormente il rilevamento dell'asset. Il white paper Oracle relativo al *tracciamento degli asset del sistema Oracle Sun mediante RFID*, è disponibile all'indirizzo:

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

Aggiornamenti per software e firmware

Mantenere sempre aggiornate le versioni di software e firmware nell'apparecchiatura server.

- Verificare con regolarità la presenza di aggiornamenti.
- Installare sempre la versione più recente di software o firmware.
- Installare tutte le patch di sicurezza necessarie per il software.
- Tenere presente che i dispositivi come i commutatori di rete contengono inoltre firmware e potrebbero richiedere aggiornamenti firmware e patch.

Accesso di rete

Seguire queste linee guida per proteggere l'accesso locale e remoto ai sistemi.

- Limitare la configurazione remota a indirizzi IP specifici utilizzando SSH anziché Telnet. I nomi utente e le password vengono trasmesse mediante Telnet in testo non cifrato, consentendo potenzialmente a chiunque sul segmento LAN di visualizzare le credenziali di login. Impostare una password sicura per SSH.
- Utilizzare la versione 3 del protocollo SNMP per garantire trasmissioni sicure. Versioni precedenti di SNMP non sono sicure e trasmettono i dati di autenticazione come testo non cifrato.
- Modificare la stringa comunità SNMP predefinita in una stringa comunità sicura se SNMP è necessario. In alcuni prodotti è impostato il valore PUBLIC nella stringa comunità SNMP predefinita. Gli autori di attacchi possono inviare query a una comunità per ottenere una mappa di rete molto complessa e, se possibile, modificare i valori di base delle informazioni di gestione (MIB).
- Eseguire sempre il logout dopo aver utilizzato il controller di sistema, se questo utilizza un'interfaccia browser.
- Disattivare i servizi di rete non necessari, come il protocollo TCP (Transmission Control Protocol) o quello HTTP (Hypertext Transfer Protocol). Attivare i servizi di rete necessari e configurarli in maniera sicura.
- Adottare le misure di sicurezza LDAP quando si utilizza il protocollo LDAP per l'accesso al sistema. Fare riferimento alla *Guida per la sicurezza di Oracle ILOM* all'indirizzo: http://www.oracle.com/goto/ILOM/docs
- Creare un banner che dichiari che l'accesso non autorizzato è proibito.
- Ove possibile, utilizzare le liste di controllo dell'accesso.
- Impostare timeout per le sessioni prolungate e livelli di privilegi.
- Utilizzare le funzioni di autenticazione, autorizzazione e accounting (AAA) per l'accesso locale e remoto a un commutatore.
- Se possibile, utilizzare i protocolli di sicurezza RADIUS e TACACS+:
  - RADIUS (Remote Authentication Dial In User Service) è un protocollo client/server che protegge le reti dall'accesso non autorizzato.
  - TACACS+ (Terminal Access Controller Access-Control System) è un protocollo che consente a un server di accesso remoto di comunicare con un server di autenticazione per determinare se un utente può accedere alla rete.
- Utilizzare la funzionalità di mirroring delle porte del commutatore per l'accesso al sistema di rilevamento delle intrusioni IDS (Intrusion Detection System).
- Implementare la sicurezza delle porte per limitare l'accesso basato su un indirizzo MAC. Disattivare il trunking automatico in tutte le porte.

Protezione e sicurezza dei dati

Seguire queste linee guida per ottimizzare la protezione e la sicurezza dei dati.

- Eseguire il backup dei dati importanti utilizzando dispositivi quali dischi rigidi esterni o dispositivi di memorizzazione USB. Memorizzare i dati acquisiti in una seconda posizione sicura in remoto.
- Utilizzare il software di cifratura dei dati per proteggere le informazioni confidenziali sui dischi rigidi.
- Quando si sostituisce un disco rigido obsoleto, distruggerlo fisicamente o eliminare totalmente tutti i dati al suo interno. È comunque possibile recuperare le informazioni da un disco dopo che tutti i file sono stati eliminati o il disco è stato riformattato. L'eliminazione dei file o la riformattazione del disco consentono di rimuovere solo le tabelle di indirizzi sul disco. Utilizzare il software di cancellazione del disco per eliminare completamente tutti i dati da un disco.

Mantenimento del registro

Verificare ed eseguire la manutenzione dei file di registro con regolarità. Utilizzare i seguenti metodi per proteggere i file di registro.

- Attivare il log e inviare i registri di sistema a un host di registro sicuro dedicato.
- Configurare il log per includere informazioni temporali accurate, mediante NTP (Network Time Protocol) e data/ora.
- Riesaminare i registri per visualizzare possibili problemi e archiviarli rispettando i criteri di sicurezza.
- Archiviare periodicamente i file di registro quando superano una determinata dimensione. Conservare copie dei file archiviati per riferimenti futuri o analisi statistiche.