Guida per la sicurezza di Sun QFS e Sun Storage Archive Manager 5.3

N. di parte: E36004
Giugno 2012

120817@25097

Indice

Prefazione 5

1 Panoramica di Sun QFS e Sun Storage Archive Manager 7
Panoramica del prodotto 7
Principi di sicurezza generali 8
Mantenere aggiornato il software 8
Limitare accesso di rete a servizi fondamentali 8
Seguire il principio dei privilegi minimi 9
Monitorare l'attività del sistema 9
Restare aggiornati per quanto riguarda le informazioni di sicurezza più recenti 9

2 Configurazione e installazione sicure 11
Panoramica dell'installazione 11
Informazioni sull'ambiente 11
Topologie di distribuzione raccomandate 12
Installazione di SAM-QFS 12
Installazione di Sun SAM-Remote 14
Installazione di SAM-QFS Manager 14
Configurazione post-installazione 14

3 Funzioni di sicurezza di Sun QFS e Sun Storage Archive Manager 15
Modello di sicurezza 15
Autenticazione 15
Controllo degli accessi 16
Considerazioni di sicurezza per gli sviluppatori 16

A Lista di controllo di distribuzione sicura 17
Lista di controllo di distribuzione 17
Riferimenti 18

Prefazione

Guida per la sicurezza di Sun QFS e Sun Storage Archive Manager include informazioni relative al prodotto Sun QFS e Storage Archive Manager (SAM-QFS) e spiegazioni dei principi generali di sicurezza delle applicazioni.

Accesso a Oracle Support

I clienti Oracle hanno accesso al supporto elettronico mediante My Oracle Support. Per informazioni, visitare il sito `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oppure il sito `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` per utenti con problemi di udito.

Convenzioni tipografiche

Nella seguente tabella vengono descritte le convenzioni tipografiche utilizzate in questo manuale.

TABELLA P–1 Convenzioni tipografiche

Carattere tipografico	Descrizione	Esempio
`AaBbCc123`	Nomi di comandi, file e directory, nonché messaggi del sistema sullo schermo	Modificare il file `.login`. Utilizzare `ls -a` per elencare tutti i file. `machine_name% Nuovi messaggi.`
`AaBbCc123`	Comandi digitati dall'utente, in contrasto con l'output del sistema sullo schermo	`machine_name%` **`su`** `Password:`
aabbcc123	Segnaposto: da sostituire con nomi o valori reali	Il comando per la rimozione di un file è `rm` *filename* .

TABELLA P–1 Convenzioni tipografiche *(Continua)*

Carattere tipografico	Descrizione	Esempio
AaBbCc123	Titoli di manuali, termini citati per la prima volta, termini particolarmente importanti nel contesto	Vedere il Capitolo 6 del *Manuale utente*. La *cache* è una copia memorizzata localmente. *Non* salvare il file. **Nota:** alcuni termini compaiono in grassetto nella visualizzazione online.

Prompt delle shell in esempi di comandi

Nella tabella seguente sono riportati i prompt di sistema UNIX e superutente predefiniti per le shell incluse nel sistema operativo Oracle Solaris. Il prompt di sistema predefinito visualizzato negli esempi di comandi varia in base alla release di Oracle Solaris.

TABELLA P–2 Prompt delle shell

Shell	Prompt
Shell Bash, shell Korn e shell Bourne	`$`
Shell Bash, shell Korn e shell Bourne per superutenti	`#`
C shell	`machine_name%`
C shell, superutente	`machine_name#`

◆ ◆ ◆ CAPITOLO 1

1 Panoramica di Sun QFS e Sun Storage Archive Manager

In questo capitolo viene fornita una panoramica del prodotto Sun QFS e Storage Archive Manager (SAM-QFS) e vengono descritti i principi generali di sicurezza delle applicazioni.

Panoramica del prodotto

SAM-QFS è un file system condiviso caratterizzato da una gestione archivi gerarchica. SAM-QFS è suddiviso nei seguenti componenti principali:

- **Pacchetto Sun QFS –** Include il file system Sun QFS a elevate prestazioni configurabile in modalità standalone o condivisa. Quando viene utilizzata la configurazione standalone, Sun QFS viene configurato su un singolo sistema e non con client condivisi. Sun QFS utilizza operazioni vnode VFS standard per interfacciarsi con i sistemi operativi Linux e Oracle Solaris.

  I pacchetti di installazione Sun QFS sono `SUNWqfsr` e `SUNWqfsu`. In questi pacchetti *non* è incluso il componente SAM (gestione archivio memorizzazione) gerarchico.

  La configurazione di Sun QFS in modalità standalone senza client condivisi è la più sicura. In questa configurazione non vengono eseguiti daemon e non sono disponibili connessioni remote diverse da quelle da Fibre Channel (FC) a disco. La configurazione di QFS in modalità condivisa include connessioni FC a disco e una connessione TCP/IP tra il client e il server di metadati (MDS).

- **Pacchetto SAM-QFS –** Include il file system Sun QFS e il codice necessario per l'esecuzione di SAM.

  I pacchetti di installazione SAM-QFS sono `SUNWsamfsr` e `SUNWsamfsu`. Se SAM non è necessario, installare *solo* il pacchetto Sun QFS.

- **Sun SAM-Remote –** Consente di accedere alle librerie di nastri remote e alle unità mediante connessioni WAN (Wide Area Network) TCP/IP. Sun SAM-Remote fornisce una forma di ripristino di emergenza tramite individuazione remota di risorse nastro. È possibile installare Sun SAM-Remote con i pacchetti Sun QFS o SAM-QFS, ma è necessario attivare e

configurare Sun SAM-Remote separatamente. Per maggiori informazioni su Sun SAM-Remote, vedere Capitolo 18, "Using the Sun SAM-Remote Software" in *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*.

- **Pacchetto strumenti SAM-QFS –** Consente di installare strumenti e pagine man nella directory `/opt/SUNWsamfs/tools`. Nessuno di questi strumenti dispone di privilegi particolari, ma per utilizzarli è necessario un accesso root. Il pacchetto di installazione è `SUNWsamtp`.
- **SAM-QFS Manager –** SAM-QFS Manager, `fsmgr`, viene eseguito su MDS ed è accessibile da remoto mediante un browser Web. L'accesso è consentito mediante la porta 6789 (`https://`*hostname*`:6789`).

  Per utilizzare `fsmgr`, è necessario eseguire il login come utente valido su MDS e aggiungere determinati ruoli all'account utente. Per informazioni sull'installazione e configurazione di SAM-QFS Manager, vedere Capitolo 6, "Installing and Configuring SAM-QFS Manager" in *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Principi di sicurezza generali

Le seguenti sezioni descrivono i principi fondamentali necessari per utilizzare in maniera sicura qualsiasi applicazione.

Mantenere aggiornato il software

Mantenere aggiornata la versione di SAM-QFS in esecuzione. È possibile trovare versioni correnti del software da scaricare sul sito Oracle Software Delivery Cloud (`https://edelivery.oracle.com/`).

Limitare accesso di rete a servizi fondamentali

SAM-QFS utilizza le seguenti porte TCP/IP:

- `tcp/7105` è utilizzata per il traffico di metadati tra il client e MDS
- `tcp/1000` è utilizzata per Sun SAM-Remote
- `tcp/6789` è la porta HTTPS utilizzata da un browser per eseguire la connessione a `fsmgr`
- `tcp/5012` è utilizzato per `sam-rpcd`

Nota – Per il traffico client MDS, prendere in considerazione l'impostazione di una rete separata senza interconnessione con la WAN esterna. Questa configurazione impedisce l'esposizione a rischi esterni e garantisce inoltre che il traffico esterno non limiti le prestazioni MDS.

Seguire il principio dei privilegi minimi

Fornire all'utente o all'amministratore i privilegi minimi necessari per portare a termine le attività da eseguire. In SAM-QFS Manager sono disponibili diversi ruoli da assegnare agli utenti. Questi ruoli garantiscono privilegi di diverso tipo e quantità. L'esecuzione di attività di amministrazione di SAM-QFS dalla riga di comando richiede un'autorizzazione root.

Per maggiori informazioni sull'utilizzo di SAM-QFS Manager, vedere Capitolo 6, "Installing and Configuring SAM-QFS Manager" in *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Monitorare l'attività del sistema

Monitorare l'attività del sistema per stabilire la corretta esecuzione di SAM-QFS e la presenza di attività anomale. Verificare i seguenti file di log:

- `/var/adm/messages`
- `/var/opt/SUNWsamfs/sam-log`
- `/var/opt/SUNWsamfs/archiver.log`, vedere `/etc/opt/SUNWsamfs/archiver.cmd`
- `/var/opt/SUNWsamfs/recycler.log`, vedere `/etc/opt/SUNWsamfs/recycler.cmd`
- `/var/opt/SUNWsamfs/releaser.log`, vedere `/etc/opt/SUNWsamfs/releaser.cmd`
- `/var/opt/SUNWsamfs/stager.log`, vedere `/etc/opt/SUNWsamfs/stager.cmd`
- `/var/opt/SUNWsamfs/trace/*`

Restare aggiornati per quanto riguarda le informazioni di sicurezza più recenti

È possibile accedere a diverse fonti di informazioni di sicurezza. Per avvisi e informazioni sulla sicurezza relativi a un'ampia varietà di prodotti software, vedere `http://www.us-cert.gov`. Per informazioni specifiche su SAM-QFS, vedere `http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss`. Il metodo principale per essere sempre aggiornati sulle questioni relative alla sicurezza è quello di utilizzare la versione più aggiornata del software SAM-QFS

◆ ◆ ◆ CAPITOLO 2

2 Configurazione e installazione sicure

In questo capitolo viene presentato il processo di pianificazione di un'installazione sicura e sono descritte alcune topologie di distribuzione raccomandate per i sistemi.

Panoramica dell'installazione

Informazioni sull'ambiente

Per comprendere al meglio le proprie esigenze di sicurezza, è necessario porsi le seguenti domande:

- **Quali risorse voglio proteggere?**

  È possibile proteggere tutte le risorse presenti nell'ambiente di produzione. Considerare il tipo di risorse che si desidera proteggere quando si stabilisce il livello di sicurezza da fornire.

  Quando si utilizza SAM-QFS, proteggere le seguenti risorse:

  - **Disco dati principali e metadati –** Queste risorse dati sono utilizzate per creare file system SAM-QFS. Sono solitamente collegate tramite Fibre Channel (FC). Un accesso indipendente a questi dischi (non tramite SAM-QFS) presenta rischi per la sicurezza poiché solitamente vengono ignorate le autorizzazioni di file e directory SAM-QFS. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue lettura o scrittura dei dischi FC, o da un sistema interno che può accidentalmente fornire accesso non root a file dispositivo raw.
  - **Nastri SAM –** L'accesso indipendente ai nastri, solitamente in una libreria di nastri, in cui i dati del file sono scritti durante la fase di disinstallazione da un file system SAM, è un rischio per la sicurezza.

- **File dump SAM-QFS –** Dump file system creati da `samfsdump` che contengono dati e metadati. Questi dati e metadati dovrebbero essere protetti dall'accesso eseguito da utenti diversi dall'amministratore di sistema nel corso di un dump di routine o di attività di ripristino.
- **Server metadati SAM-QFS (MDS) –** I client SAM-QFS necessitano di accesso TCP/IP a MDS. Tuttavia, è necessario garantire che i client siano protetti da accesso WAN esterno.
- **Impostazioni e file di configurazione –** Le impostazioni di configurazione SAM-QFS *devono* essere protette da accessi eseguiti da utenti senza diritti di amministratore. In generale, queste impostazioni sono automaticamente protette da SAM-QFS quando si utilizza SAM-QFS Manager. Tenere presente che rendere i file di configurazione modificabili da parte di utenti senza diritti di amministrazione costituisce un rischio per la sicurezza.

- **Da chi desidero proteggere le risorse?**

  In generale, le risorse descritte nella sezione precedente *devono* essere protette da tutti gli accessi non root e non di amministratore su un sistema configurato, o da un sistema esterno non autorizzato con accesso a queste risorse mediante fabric WAN o FC.

- **Cosa accade se la protezione delle risorse strategiche fallisce?**

  Gli errori nella protezione delle risorse strategiche possono comprendere accesso non appropriato (accesso ai dati non conforme alle autorizzazioni dei file POSIX SAM-QFS ordinarie) e danneggiamento dei dati (scrittura su disco o nastro non conforme alle autorizzazione ordinarie).

Topologie di distribuzione raccomandate

Installazione di SAM-QFS

In questa sezione viene descritto come installare e configurare in maniera sicura un componente dell'infrastruttura.

Per informazioni sull'installazione di SAM-QFS, consultare il Capitolo 5, “Installing Sun QFS and SAM-QFS” in *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Considerare i seguenti punti quando si installa e configura SAM-QFS:

- **Rete metadati separata –** Per connettere i client SAM-QFS ai server MDS, fornire una rete TCP/IP separata e scollegare qualsiasi hardware non collegato a WAN. Poiché il traffico dei metadati è implementato mediante TCP/IP, un attacco esterno ai danni di questo traffico è teoricamente possibile. Configurando una rete di metadati separata è possibile ridurre i rischi e ottenere prestazioni migliori. È possibile ottenere prestazioni migliorate fornendo un percorso dati garantito ai metadati. Se non è possibile ottenere una rete di metadati separata, bloccare il traffico alle porte SAM-QFS da WAN esterno e da qualsiasi host non attendibile sulla rete. Vedere "Limitare accesso di rete a servizi fondamentali" a pagina 8.
- **Suddivisione in zone FC –** Utilizzare la suddivisione in zone FC per impedire l'accesso ai dischi SAM-QFS da qualsiasi server che non necessita di accesso ai dischi. È preferibile utilizzare un Fibre Channel switch separato per eseguire il collegamento fisico *solo* ai server che necessitano di accesso.
- **Proteggere l'accesso alla configurazione dei dischi SAN –** È solitamente possibile accedere ai dischi RAID SAN per scopi amministrativi mediante TCP/IP o, più spesso, HTTP. È necessario proteggere i dischi dagli accessi esterni limitando l'accesso per scopi amministrativi ai dischi RAID SAN ai soli sistemi con un dominio attendibile. Inoltre, modificare la password predefinita negli array del disco.
- **Installare il pacchetto SAM-QFS –** Installare come prima cosa solo i pacchetti necessari. Ad esempio, se non si desidera utilizzare SAM, installare *solo* i pacchetti QFS.

  I proprietari e le autorizzazioni di file e directory SAM-QFS predefiniti *non* dovrebbero essere modificati dopo l'installazione senza aver preso in esame le implicazioni di tali modifiche a carico della sicurezza.
- **Accesso client –** Se si desidera configurare client condivisi, stabilire quali client devono avere accesso ai file system nel file `hosts`. Consultare la pagina man `hosts.fs`(4). Configurare *solo* gli host che necessitano di accesso allo specifico file system configurato.
- **Impostare la protezione avanzata del server di metadati Oracle Solaris –** Per informazioni sull'impostazione della protezione avanzata di Sistema operativo Oracle Solaris, consultare le *linee guida sulla sicurezza di Oracle Solaris 10* e le *linee guida sulla sicurezza di Oracle Solaris 11*. Come precauzioni minime, scegliere una buona password root, installare una versione aggiornata di Sistema operativo Oracle Solaris e mantenere aggiornate le patch, specialmente quelle di sicurezza.
- **Impostare la protezione avanzata dei client Linux –** Verificare la documentazione di Linux per informazioni sull'impostazione della protezione avanzata dei client Linux. Come precauzioni minime, scegliere una buona password root, installare una versione aggiornata del sistema operativo Linux e mantenere aggiornate le patch, specialmente quelle di sicurezza.
- **Sicurezza nastro SAM-QFS –** Impedire l'accesso esterno ai nastri SAM da posizioni esterne a SAM o limitare tale accesso ai soli amministratori. Utilizzare la suddivisione in zone FC per limitare l'accesso alle unità nastro solo a MDS (o a MDS potenziale se è configurato un

MDS di backup). Inoltre, limitare l'accesso al file dispositivo a nastro consentendo solo le autorizzazioni root. Accessi non autorizzati ai nastri SAM possono compromettere o distruggere i dati dell'utente.

- **Backup –** Impostare ed eseguire backup di dati SAM-QFS mediante i comandi `samfsdump` o `qfsdump`. Limitare l'accesso ai file dump come raccomandato per i nastri SAM.

Installazione di Sun SAM-Remote

Per informazioni sull'installazione sicura del software Sun SAM-Remote, vedere Capitolo 18, "Using the Sun SAM-Remote Software" in *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*.

Installazione di SAM-QFS Manager

Per informazioni sull'installazione sicura di SAM-QFS Manager, vedere Capitolo 6, "Installing and Configuring SAM-QFS Manager" in *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.

Configurazione post-installazione

Dopo aver installato i pacchetti SAM-QFS, consultare la lista di controllo di sicurezza in Appendice A, "Lista di controllo di distribuzione sicura".

◆ ◆ ◆ CAPITOLO 3

Funzioni di sicurezza di Sun QFS e Sun Storage Archive Manager

Per evitare potenziali rischi di sicurezza, è necessario che i clienti con file system condiviso prestino attenzione ai seguenti elementi:

- Diffusione di dati di file system in violazione dei criteri
- Perdita di dati
- Modifiche non rilevate ai dati

È possibile minimizzare questi rischi per la sicurezza eseguendo una corretta configurazione e consultando la lista di controllo in seguito all'installazione in Appendice A, "Lista di controllo di distribuzione sicura".

Modello di sicurezza

Le funzioni di sicurezza fondamentali per la protezione dai rischi sono:

- **Autenticazione** – Consente di garantire che solo gli utenti autorizzati abbiano accesso al sistema e ai dati.
- **Autorizzazione** – Controllo dell'accesso a dati e privilegi di sistema. Questa funzione consente di creare l'autenticazione, così da garantire che gli utenti dispongano unicamente dell'accesso appropriato.
- **Audit** – Consente agli amministratori di rilevare tentativi di violazione del meccanismo di autenticazione o violazioni del controllo degli accessi.

Autenticazione

SAM-QFS utilizza l'autenticazione dell'utente basata su host per verificare quali utenti dispongono dell'autorizzazione per eseguire attività di amministrazione. L'amministrazione mediante SAM-QFS Manager è controllata principalmente da ruoli assegnati a vari utenti. L'amminsitrazione mediante la riga di comando è limitata all'utente root.

Controllo degli accessi

Il controllo degli accessi in SAM-QFS è diviso in due parti:

- **Controllo degli accessi amministrativi** – Consente di controllare gli utenti che possono eseguire attività amministrative per SAM-QFS. I controlli sono basati su ruoli assegnati a utenti mediante SAM-QFS Manager. Per le operazioni della riga di comando, i controlli sono basati su autorizzazioni root. Per maggiori informazioni su SAM-QFS Manager, vedere Capitolo 6, "Installing and Configuring SAM-QFS Manager" in *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*.
- **Controllo degli accessi file/directory** – SAM-QFS consente di implementare un file system conforme a POSIX con un'ampia scelta di controlli degli accessi. Per maggiori dettagli, vedere la documentazione di SAM-QFS.

Considerazioni di sicurezza per gli sviluppatori

Gli sviluppatori generalmente non utilizzano direttamente SAM-QFS. Due eccezioni sono riscontrabili nell'API `libsam` e nell'API `libsamrpc`. Questi due API forniscono la stessa funzionalità. `libsam` è solo per un computer locale, mentre `libsamrpc` consente la comunicazione con MDS mediante `rpc(3)` per l'implementazione delle azioni richieste. L'autenticazione di richieste eseguite da uno dei due metodi è basata su UID e GID del processo chiamante. Le autorizzazioni sono le stesse utilizzate dalle richieste eseguite mediante la riga di comando. Assicurarsi di avere a disposizione uno spazio UID e GID comune per MDS e sistemi client.

Per maggiori informazioni, vedere `intro_libsam(3)` e `intro_libsamrpc`(3) in *Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual*.

◆ ◆ ◆ APPENDICE A

Lista di controllo di distribuzione sicura

Utilizzare la lista di controllo fornita in appendice per la distribuzione sicura del software SAM-QFS.

Lista di controllo di distribuzione

La lista di controllo di sicurezza include linee guida per proteggere il database.

- Impostare password sicure per l'account root e per tutti gli account a cui sono assegnati ruoli SAM-QFS. Questa linea guida include:
  - Qualsiasi account con ruoli amministrativi assegnati da SAM-QFS Manager.
  - ID utente `acsss`, `acsdb` e `acssa` (se utilizzati).
  - Qualsiasi account amministrativo array di dischi.
- Se si utilizza l'utente predefinito `samadmin` con SAM-QFS Manager, modificare immediatamente la password predefinita installata con una più sicura. Non utilizzare account root con SAM-QFS Manager, assegnare piuttosto ruoli quando necessario ad altri account utente. Proteggere anche questi account con password sicure.
- Installare il filtro applicato alle porte su edge router WAN per evitare il traffico sulle porte elencate nei "Principi di sicurezza generali" a pagina 8 da MDS o client, tranne quando necessario per Sun SAM-Remote.
- Separare i dischi FC e i nastri fisicamente o attraverso la suddivisione in zone FC, così da rendere i dischi accessibili solo da MDS e client e i nastri da MDS e MDS potenziali. In questo modo si previene la perdita di dati provocata dalla sovrascrittura accidentale di nastri o dischi.
- Verificare `/dev` per garantire che i file dispositivo disco e nastro non siano accessibili a utenti diversi da quellI root. In questo modo si previene l'accesso non appropriato o la distruzione dei dati SAM-QFS.

- SAM-QFS è un file system POSIX e fornisce un ampio set di autorizzazioni directory/file, tra cui liste di controllo dell'accesso (ACL, Access Control List). Utilizzarli quando necessario per proteggere i dati utente nel file system. Per maggiori informazioni, consultare la documentazione SAM-QFS.
- Impostare un set di dump di backup appropriato basato sui criteri locali. I backup sono fondamentali per la sicurezza e forniscono una soluzione per il ripristino dei dati accidentalmente smarriti o violati. Il backup dovrebbe includere alcuni criteri durante il trasporto in un'altra posizione. È necessario proteggere i backup allo stesso livello di dischi e nastri SAM-QFS.

Riferimenti

- *Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide*
- *Sun QFS File System 5.3 Configuration and Administration Guide*
- *Sun Storage Archive Manager 5.3 Configuration and Administration Guide*
- *Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual*