

Sun QFS 및 Sun Storage Archive Manager

5.3 보안 설명서

Copyright © 2011, 2012, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 계약서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록 상표입니다.

본 소프트웨어 혹은 하드웨어와 관련 문서(설명서)는 제 3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다.

목차

머리말	5
1 Sun QFS 및 Sun Storage Archive Manager 개요	7
제품 개요	7
일반적인 보안 원칙	8
소프트웨어를 최신으로 유지	8
중요 서비스에 대한 네트워크 액세스 제한	8
최소 권한 원칙 준수	8
시스템 작업 모니터링	9
최신 보안 정보 유지	9
2 보안 설치 및 구성	11
설치 개요	11
작업 환경 파악	11
권장되는 배치 토폴로지	12
SAM-QFS 설치	12
Sun SAM-Remote 설치	13
SAM-QFS Manager 설치	13
사후 설치 구성	14
3 Sun QFS 및 Sun Storage Archive Manager 보안 기능	15
보안 모델	15
인증	15
액세스 제어	15
개발자에 대한 보안 고려 사항	16

A	보안 배치 점검 목록	17
	배치 점검 목록	17
	참조 자료	18

머리말

Sun QFS 및 Sun Storage Archive Manager 보안 설명서에서는 Sun QFS 및 Storage Archive Manager(SAM-QFS) 제품에 대한 정보를 제공하며 응용 프로그램 보안의 일반적인 원칙을 설명합니다.

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

표기 규약

다음 표는 이 책에 사용되는 표기 규약에 대해 설명합니다.

표 P-1 표기 규약

활자체	설명	예
AaBbCc123	명령, 파일 및 디렉토리의 이름, 그리고 컴퓨터 화면에 출력되는 내용입니다.	.login 파일을 편집하십시오. 모든 파일을 나열하려면 <code>ls -a</code> 를 사용합니다. machine_name% you have mail.
AaBbCc123	컴퓨터 화면 상의 출력과는 달리 사용자가 직접 입력하는 사항입니다.	machine_name% su Password:
aabbcc123	자리 표시자: 실제 이름이나 값으로 대체됩니다.	<code>rm filename</code> 명령을 사용하여 파일을 제거합니다.

표 P-1 표기 규약 (계속)		
활자체	설명	예
AaBbCc123	책 제목, 새로 나오는 용어, 강조 표시할 단어입니다.	사용자 설명서 의 6장을 참조하십시오. 캐시 는 로컬에 저장된 복사본입니다. 파일을 저장하지 마십시오. 주: 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에서는 Oracle Solaris OS에 포함된 셸에 대한 기본 UNIX 시스템 프롬프트와 슈퍼유저 프롬프트를 보여 줍니다. 명령 예에서 표시되는 기본 시스템 프롬프트는 Oracle Solaris 릴리스에 따라 달라집니다.

표 P-2 셸 프롬프트	
셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	\$
슈퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	#
C 셸	machine_name%
슈퍼유저용 C 셸	machine_name#

Sun QFS 및 Sun Storage Archive Manager 개요

이 장에서는 Sun QFS 및 Storage Archive Manager(SAM-QFS) 제품에 대한 개요와 응용 프로그램 보안에 대한 일반적인 원칙을 설명합니다.

제품 개요

SAM-QFS는 계층적 저장소 관리자를 갖춘 공유 파일 시스템입니다. SAM-QFS는 다음과 같은 주요 구성 요소로 구성됩니다.

- **Sun QFS 패키지** - 독립형이나 공유로 구성할 수 있는 고성능 Sun QFS 파일 시스템이 포함됩니다. 독립형으로 구성할 경우 Sun QFS는 공유 클라이언트 없이 단일 시스템으로 구성됩니다. Sun QFS는 표준 VFS vnode 작업을 사용하여 Oracle Solaris 및 Linux 운영 체제와 상호 작용합니다.

Sun QFS 설치 패키지는 SUNWqfsr 및 SUNWqfsu입니다. 이러한 패키지에는 계층적 저장소 아카이브 관리자(SAM) 구성 요소가 포함되지 **않습니다**.

공유 클라이언트 없이 Sun QFS 독립형으로 구성하면 보안 위험이 가장 적게 노출됩니다. 이 구성에서는 데몬을 실행하지 않으며 디스크에 대한 광섬유 채널(FC) 이외의 원격 연결은 없습니다. QFS 공유 구성에는 디스크에 대한 FC 연결 및 클라이언트와 메타 데이터 서버(MDS) 사이의 TCP/IP 연결이 포함됩니다.

- **SAM-QFS 패키지** - SAM을 실행하는 데 필요한 Sun QFS 파일 시스템 및 코드가 포함됩니다.

SAM-QFS 설치 패키지는 SUNwsamfsr 및 SUNwsamfsu입니다. SAM이 필요하지 않은 경우 Sun QFS 패키지 **만** 설치하십시오.

- **Sun SAM-Remote** - TCP/IP WAN(wide area network) 연결을 통한 원격 테이프 라이브러리 및 드라이브에 대한 액세스를 허용합니다. Sun SAM-Remote는 원격으로 테이프 설비를 찾아 일종의 재해 복구 기능을 제공합니다. Sun QFS 또는 SAM-QFS 패키지와 함께 Sun SAM-Remote를 설치할 수 있지만, Sun SAM-Remote는 별도로 사용으로 설정하고 구성해야 합니다. Sun SAM-Remote에 대한 자세한 내용은 **Sun Storage Archive Manager 5.3 Configuration and Administration Guide**의 18 장, “Using the Sun SAM-Remote Software”를 참조하십시오.

- **SAM-QFS 도구 패키지** - /opt/SUNWsamfs/tools 디렉토리에 도구 및 매뉴얼 페이지를 설치합니다. 이러한 도구에는 특수한 권한이 없지만 사용하려면 모두 root 액세스 권한이 필요합니다. 설치 패키지는 SUNWsamtp입니다.
- **SAM-QFS Manager** - SAM-QFS Manager(fsmgr)는 MDS에서 실행되고 웹 브라우저를 통해 원격으로 액세스됩니다. 액세스는 포트 6789(<https://hostname:6789>)를 통해 부여됩니다.

fsmgr을 사용하려면 MDS에서 유효한 사용자로 로그인하고 사용자 계정에 특정 역할을 추가해야 합니다. SAM-QFS Manager 설치 및 구성에 대한 자세한 내용은 [Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide](#)의 6 장, “Installing and Configuring SAM-QFS Manager”를 참조하십시오.

일반적인 보안 원칙

다음 절에서는 응용 프로그램을 안전하게 사용하는 데 필요한 기본적인 원칙을 설명합니다.

소프트웨어를 최신으로 유지

사용하는 SAM-QFS를 항상 최신 버전으로 유지하십시오. 최신 버전의 소프트웨어는 [Oracle Software Delivery Cloud \(https://edelivery.oracle.com/\)](https://edelivery.oracle.com/)에서 다운로드할 수 있습니다.

중요 서비스에 대한 네트워크 액세스 제한

SAM-QFS에서는 다음 TCP/IP 포트를 사용합니다.

- tcp/7105는 클라이언트와 MDS 사이에 메타 데이터 트래픽에 사용됩니다.
- tcp/1000은 Sun SAM-Remote에 사용됩니다.
- tcp/6789는 fsmgr에 연결하는 브라우저에 사용되는 HTTPS 포트입니다.
- tcp/5012는 sam-rpcd에 사용됩니다.

주 - MDS 클라이언트 트래픽의 경우, 외부 WAN과 상호 연결되지 않는 별도의 네트워크를 설정하십시오. 이 구성은 외부 위협으로부터 노출을 막고 외부 트래픽이 MDS 성능을 제한하지 않도록 합니다.

최소 권한 원칙 준수

사용자나 관리자에게 작업을 수행하는 데 필요한 최소한의 권한을 부여합니다. SAM-QFS Manager에는 사용자에게 부여할 수 있는 다양한 역할이 있습니다. 이러한 역할은 다양한 유형과 수준의 권한을 부여합니다. 명령줄에서 SAM-QFS 관리 작업을 수행하려면 root 권한이 필요합니다.

SAM-QFS Manager 사용에 대한 자세한 내용은 **Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide**의 6 장, “Installing and Configuring SAM-QFS Manager”를 참조하십시오.

시스템 작업 모니터링

시스템 작업을 모니터링하여 SAM-QFS가 제대로 작동하고 있는지 및 비정상적인 작업이 기록되고 있는지 여부를 확인합니다. 다음 로그 파일을 확인하십시오.

- /var/adm/messages
- /var/opt/SUNWsamfs/sam-log
- /var/opt/SUNWsamfs/archiver.log(/etc/opt/SUNWsamfs/archiver.cmd 참조)
- /var/opt/SUNWsamfs/recycler.log(/etc/opt/SUNWsamfs/recycler.cmd 참조)
- /var/opt/SUNWsamfs/releaser.log(/etc/opt/SUNWsamfs/releaser.cmd 참조)
- /var/opt/SUNWsamfs/stager.log(/etc/opt/SUNWsamfs/stager.cmd 참조)
- /var/opt/SUNWsamfs/trace/*

최신 보안 정보 유지

여러 소스의 보안 정보에 액세스할 수 있습니다. 다양한 소프트웨어 제품에 대한 보안 정보 및 경고는 <http://www.us-cert.gov>를 참조하십시오. SAM-QFS에 대한 특정 정보는 <http://mail.opensolaris.org/mailman/listinfo/sam-qfs-discuss>를 참조하십시오. 보안 사항을 최신으로 유지하는 기본적인 방법은 최신 버전의 SAM-QFS 소프트웨어를 실행하는 것입니다.

보안 설치 및 구성

이 장에서는 보안 설치를 위한 계획 과정을 간략하게 알아보고 시스템에 권장되는 여러 배치 토폴로지에 대해 설명합니다.

설치 개요

작업 환경 파악

보안 요구사항을 제대로 파악하기 위해 다음과 같은 질문에 스스로 답해보십시오.

- 어떤 리소스를 보호해야 하는가?

운영 환경의 여러 가지 많은 리소스를 보호할 수 있습니다. 제공할 보안 수준을 결정할 때 보호하고자 하는 리소스의 유형을 고려합니다.

SAM-QFS를 사용하는 경우 다음과 같은 리소스를 보호합니다.

- **메타 데이터 및 기본 데이터 디스크** - 이러한 디스크 리소스는 SAM-QFS 파일 시스템을 작성하는 데 사용됩니다. 일반적으로 광섬유 채널(FC)로 연결됩니다. 이러한 디스크에 대한 (SAM-QFS를 통하지 않은) 독립적인 액세스는 정상적인 SAM-QFS 파일 및 디렉토리 권한을 우회하므로 보안 위험을 가져옵니다. 이 유형의 외부 액세스는 FC 디스크를 읽거나 쓰는 악의적인 시스템 또는 원시 장치 파일에 대한 비root 액세스를 실수로 제공하는 내부 시스템에서 발생할 수 있습니다.
- **SAM 테이프** - SAM 파일 시스템을 준비할 때 파일 데이터가 쓰여지는 대개 테이프 라이브러리의 테이프에 대한 독립적인 액세스는 보안 위험을 가져옵니다.
- **SAM-QFS 덤프 파일** - samfsdump에서 만들어지는 파일 시스템 덤프에는 데이터 및 메타 데이터가 포함됩니다. 이 데이터 및 메타 데이터는 일상적인 덤프나 복원 작업 중 시스템 관리자 이외의 다른 사용자 액세스로부터 보호해야 합니다.

- **SAM-QFS 메타 데이터 서버(MDS)** - SAM-QFS 클라이언트에는 MDS에 대한 TCP/IP 액세스가 필요합니다. 하지만 클라이언트는 외부 WAN 액세스로부터 보호되어야 합니다.
- **구성 파일 및 설정** - SAM-QFS 구성 설정은 비관리자 액세스로부터 **반드시** 보호되어야 합니다. 일반적으로 이러한 설정은 SAM-QFS Manager를 사용하는 경우 SAM-QFS에 의해 자동으로 보호됩니다. 비관리 사용자에게 구성 파일을 쓸 수 있도록 허용할 경우 보안 위험에 노출됩니다.
- **누구로부터 리소스를 보호해야 하는가?**
일반적으로 위의 절에서 설명한 리소스는 구성된 시스템의 모든 비root 또는 비관리자 액세스나 WAN 또는 FC 패브릭으로 이러한 리소스에 액세스할 수 있는 악의적인 외부 시스템으로부터 **반드시** 보호해야 합니다.
- **전략 리소스에 대한 보호를 실패할 경우 어떻게 되는가?**
전략 리소스에 대한 보호 실패는 부적절한 액세스(정상적인 SAM-QFS POSIX 파일 권한을 벗어나는 데이터에 대한 액세스)부터 데이터 손상(정상적인 권한을 벗어나는 디스크나 테이프에 쓰기)에 이르기까지 다양합니다.

권장되는 배치 토폴로지

SAM-QFS 설치

이 절에서는 기반구조 구성 요소를 안전하게 설치하고 구성하는 방법에 대해 설명합니다.

SAM-QFS 설치에 대한 자세한 내용은 [Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide](#)의 5 장, “Installing Sun QFS and SAM-QFS”를 참조하십시오.

SAM-QFS를 설치하고 구성할 때 다음 사항을 고려하십시오.

- **별도의 메타 데이터 네트워크** - SAM-QFS 클라이언트가 MDS 서버에 연결할 수 있도록 별도의 TCP/IP 네트워크 및 WAN에 연결되지 않은 스위치 하드웨어를 제공합니다. 메타 데이터 트래픽은 TCP/IP를 사용하여 구현되므로 이론적으로 이 트래픽에 대한 외부 공격이 가능합니다. 별도의 메타 데이터 네트워크를 구성하면 이 위험이 줄어들고 성능도 향상됩니다. 성능 향상은 메타 데이터에 대한 데이터 경로 보장으로 얻게 됩니다. 별도의 메타 데이터 네트워크가 불가능한 경우 적어도 외부 WAN 및 네트워크의 신뢰할 수 없는 모든 호스트로부터 SAM-QFS 포트에 대한 트래픽을 거부하십시오. 8 페이지 “중요 서비스에 대한 네트워크 액세스 제한”을 참조하십시오.
- **FC 영역 분할** - FC 영역 분할을 사용하여 디스크에 대한 액세스가 필요하지 않은 모든 서버로부터 SAM-QFS 디스크에 대한 액세스를 거부합니다. 가능하면 별도의 FC 스위치를 사용하여 액세스가 필요한 서버에 **만** 물리적으로 연결하는 것이 좋습니다.

- **SAN 디스크 구성 액세스 보호** - SAN RAID 디스크는 관리를 위해 대개 TCP/IP 또는 더욱 일반적으로는 HTTP로 액세스할 수 있습니다. SAN RAID 디스크에 대한 관리 액세스를 신뢰할 수 있는 도메인 내의 시스템으로만 제한하여 외부 액세스로부터 디스크를 보호해야 합니다. 또한 디스크 어레이에 대한 기본 암호를 변경하십시오.
- **SAM-QFS 패키지 설치** - 먼저 필요한 패키지만 설치합니다. 예를 들어, SAM을 실행할 계획이 없는 경우 QFS 패키지만 설치합니다.
설치 후 기본 SAM-QFS 파일 및 디렉토리 권한과 소유자는 이러한 변경의 보안 구현을 고려하지 않고는 변경하면 **안됩니다**.
- **클라이언트 액세스** - 공유 클라이언트를 구성할 계획이 있는 경우 어떤 클라이언트가 hosts 파일의 파일 시스템에 대한 액세스 권한을 가져야 하는지 결정합니다.
hosts.fs(4) 매뉴얼 페이지를 참조하십시오. 구성 중인 특정 파일 시스템에 대한 액세스가 필요한 호스트만 구성하십시오.
- **Oracle Solaris 메타 데이터 서버 강화** - Oracle Solaris OS 강화에 대한 자세한 내용은 **Oracle Solaris 10 Security Guidelines** 및 **Oracle Solaris 11 Security Guidelines**를 참조하십시오. 최소한 강력한 root 암호를 선택하고 최신 버전의 Oracle Solaris OS를 설치하며 패치(특히, 보안 패치)를 최신으로 유지하십시오.
- **Linux 클라이언트 강화** - Linux 클라이언트를 강화하는 방법은 Linux 설명서를 참조하십시오. 최소한 강력한 root 암호를 선택하고 최신 버전의 Linux 운영 체제를 설치하며 패치(특히, 보안 패치)를 최신으로 유지하십시오.
- **SAM-QFS 테이프 보안** - SAM 외부로부터 SAM 테이프에 대한 외부 액세스를 막거나 이러한 액세스를 관리자만 제한합니다. FC 영역 분할을 사용하여 테이프 드라이브에 대한 액세스를 MDS(또는 백업 MDS가 구성된 경우 잠재적인 MDS)로만 제한합니다. 또한 root 전용 권한을 부여하여 테이프 장치 파일 액세스를 제한합니다. SAM 테이프에 대한 무단 액세스는 사용자 데이터를 조작하거나 삭제할 수 있습니다.
- **백업** - samfsdump 또는 qfsdump 명령을 사용하여 SAM-QFS 데이터의 백업을 설정하고 수행합니다. SAM 테이프에 권장되는 대로 덤프 파일에 대한 액세스를 제한합니다.

Sun SAM-Remote 설치

Sun SAM-Remote 소프트웨어를 안전하게 설치하는 방법에 대한 자세한 내용은 [Sun Storage Archive Manager 5.3 Configuration and Administration Guide](#)의 18 장, “Using the Sun SAM-Remote Software”를 참조하십시오.

SAM-QFS Manager 설치

SAM-QFS Manager를 안전하게 설치하는 방법에 대한 자세한 내용은 [Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide](#)의 6 장, “Installing and Configuring SAM-QFS Manager”를 참조하십시오.

사후 설치 구성

SAM-QFS 패키지를 설치한 후에는 [부록 A](#), “보안 배치 점검 목록”의 보안 점검 목록을 확인하십시오.

Sun QFS 및 Sun Storage Archive Manager 보안 기능

잠재적인 보안 위협을 피하기 위해서 공유 파일 시스템을 운영하는 고객은 다음 사항을 유의해야 합니다.

- 정책 위반시 파일 시스템 데이터의 노출
- 데이터 손실
- 감지되지 않은 데이터 수정

이러한 보안 위협은 적절한 구성 및 [부록 A, “보안 배치 점검 목록”](#)의 사후 설치 점검 목록을 준수하여 최소화할 수 있습니다.

보안 모델

보안 위협으로부터 보호하는 중요 보안 기능은 다음과 같습니다.

- **인증** - 권한이 부여된 사용자만 시스템 및 데이터에 액세스할 수 있도록 합니다.
- **권한 부여** - 시스템 권한 및 데이터에 대한 액세스 제어입니다. 이 기능은 인증을 기반으로 사용자가 적절한 액세스 권한만 가지도록 합니다.
- **감사** - 관리자가 인증 방식의 무력화 시도 및 액세스 제어의 무력화 시도 또는 성공을 감지할 수 있습니다.

인증

SAM-QFS에서는 호스트 기반 사용자 인증을 사용하여 관리 작업을 수행할 수 있는 사용자를 제어합니다. SAM-QFS Manager를 사용한 관리는 주로 다양한 사용자에게 지정된 역할로 제어됩니다. 명령줄을 사용한 관리는 root 사용자로 제한됩니다.

액세스 제어

SAM-QFS에서 액세스 제어는 두 부분으로 나누어집니다.

- **관리 액세스 제어** - SAM-QFS에 대한 관리 작업을 수행할 수 있는 사용자를 제어합니다. 이 제어는 SAM-QFS Manager를 통해 사용자에게 지정된 역할을 기준으로 합니다. 명령줄 작업에서 제어는 root 권한을 기준으로 합니다. SAM-QFS Manager에 대한 자세한 내용은 [Sun QFS and Sun Storage Archive Manager 5.3 Installation Guide](#)의 6 장, “Installing and Configuring SAM-QFS Manager”를 참조하십시오.
- **파일/디렉토리 액세스 제어** - SAM-QFS는 풍부한 액세스 제어 기능이 있는 POSIX 호환 파일 시스템을 구현합니다. 자세한 내용은 SAM-QFS 설명서를 참조하십시오.

개발자에 대한 보안 고려 사항

개발자는 일반적으로 SAM-QFS와 직접 상호 작용하지 않습니다. 하지만 `libsam` API 및 `libsamrpc` API의 두 가지 예외 사항이 있습니다. 이러한 두 API는 동일한 기능을 제공합니다. `libsam`은 로컬 시스템 전용이고, `libsamrpc`는 `rpc(3)`를 통해 MDS와 통신하여 요청된 작업을 구현합니다. 이러한 두 가지 메소드로 이루어진 요청의 인증은 호출 프로세스의 UID 및 GID를 기준으로 합니다. 명령줄을 통해 이루어진 요청과 동일한 권한을 가집니다. MDS 및 클라이언트 시스템에 대해 공통 UID 및 GID 공간을 가지고 있는지 확인하십시오.

자세한 내용은 [Sun QFS and Sun Storage Archive Manager 5.3 Reference Manual](#)의 `intro_libsam(3)` 및 `intro_libsamrpc(3)`를 참조하십시오.

보안 배치 점검 목록

이 부록의 점검 목록을 참조하여 SAM-QFS 소프트웨어를 안전하게 배치하십시오.

배치 점검 목록

이 보안 점검 목록에는 데이터베이스 보안 유지에 도움이 되는 지침이 포함되어 있습니다.

- root 계정 및 SAM-QFS 역할이 지정된 기타 다른 계정에 대해 강력한 암호를 설정합니다. 이 지침에는 다음 내용이 포함되어 있습니다.
 - SAM-QFS Manager로 관리 역할이 부여된 모든 계정.
 - acsss, acsdb 및 acssa 사용자 ID(사용되는 경우).
 - 모든 디스크 어레이 관리 계정.
- SAM-QFS Manager에서 기본 사용자 samadmin을 사용하는 경우 기본 설치된 암호에서 강력한 암호로 즉시 암호를 변경하십시오. SAM-QFS Manager에서는 root를 사용하지 말고 다른 사용자 계정에 필요에 맞게 역할을 지정합니다. 이러한 계정 또한 강력한 암호로 보호합니다.
- WAN 에지 라우터에서 포트 필터링을 설치하여 Sun SAM-Remote에 필요한 경우를 제외하고 8 페이지 “일반적인 보안 원칙”에 나열된 포트의 트래픽이 MDS 또는 클라이언트로 들어가지 않도록 막습니다.
- FC 디스크 및 테이프를 물리적으로 또는 FC 영역 분할을 통해 분리하여 디스크는 MDS 및 클라이언트에서만 액세스 가능하고 테이프는 MDS 및 잠재적 MDS에서만 액세스 가능하도록 합니다. 이 보안 방식은 테이프나 디스크의 우발적 덮어쓰기로 인한 데이터 손실 사고를 예방하는 데 도움이 됩니다.
- root 이외의 사용자가 테이프 및 디스크 장치 파일에 액세스할 수 없도록 /dev를 확인합니다. 이 방식은 SAM-QFS 데이터가 부적절하게 액세스되거나 삭제되지 않도록 예방합니다.

- SAM-QFS는 POSIX 파일 시스템이며, 액세스 제어 목록(ACL)을 포함하여 풍부한 파일/디렉토리 권한을 제공합니다. 필요에 따라 이러한 권한을 사용하여 파일 시스템에서 사용자 데이터를 보호하십시오. 자세한 내용은 SAM-QFS 설명서를 참조하십시오.
- 로컬 정책에 따라 적절한 백업 덤프 세트를 설정합니다. 백업은 보안의 일부이며 실수나 침입으로 손실된 데이터를 복구하는 방법을 제공합니다. 멀리 떨어진 위치로 전송되는 경우 백업에 어떤 정책이 포함되어야 합니다. 백업은 SAM-QFS 테이프 및 백업과 동일한 수준으로 보호해야 합니다.

참조 자료

- [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](#)