Oracle® Hierarchical Storage Manager and StorageTek QFS Software

보안 설명서

릴리스 6.0

E62078-01

2015년 3월

ORACLE

Oracle® Hierarchical Storage Manager and StorageTek QFS Software
보안 설명서

E62078-01

차례

머리말

Oracle Hierarchical Storage Manager and StorageTek QFS Software 보안 설명서는 Oracle Hierarchical Storage Manager 및 QFS 제품에 대한 정보를 제공하고 응용 프로그램 보안에 대한 일반적인 원칙을 설명합니다.

대상

이 설명서는 Oracle Hierarchical Storage Manager and StorageTek QFS Software의 보안 설치/구성 및 보안 기능 사용과 관련된 모든 사람을 대상으로 합니다.

설명서 접근성

Oracle의 접근성 개선 노력에 대한 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스
지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info를 참조하거나, 청각 장애가 있는 경우 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs를 방문하십시오.

표기 규약

다음 표는 이 책에 사용되는 표기 규약에 대해 설명합니다.

활자체	의미	예
AaBbCc123	명령 이름 및 컴퓨터 화면 출력	*ls -a*를 사용하여 모든 파일의 목록을 표시합니다.
AaBbCc123	컴퓨터 화면 출력과 함께 표시되는 사용자 입력 내용	*machine_name%* **su** *Password:*
aabbcc123	위치 표시자로, 실제 이름이나 값으로 대체됩니다.	파일을 제거하는 명령은 *rm filename*입니다.
AaBbCc123	책 제목, 새로 나오는 용어, 강조 표시할 단어입니다.	사용자 설명서의 6장을 참조하십시오. 캐시는 로컬에 저장된 복사본입니다. 파일을 저장하지 마십시오 . 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

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

셸	프롬프트
Bashshell, Kornshell 및 Bourneshell	$
수퍼유저의 경우 Bashshell, Kornshell 및 Bourneshell	#
Cshell	machine_name%
수퍼유저의 경우 Cshell	machine_name#

1

개요

이 장에서는 Oracle Hierarchical Storage Manager and StorageTek QFS Software 제품에 대한 개요와 응용 프로그램 보안에 대한 일반적인 원칙을 설명합니다.

1.1. 제품 개요

Oracle Hierarchical Storage Manager and StorageTek QFS Software는 계층적인 스토리지 관리자가 포함된 공유 파일 시스템입니다. 이 제품은 다음 주요 구성 요소로 구성됩니다.

StorageTek QFS 패키지
독립형 또는 공유 중 하나로 구성할 수 있는 고성능 QFS 파일 시스템을 포합합니다. 독립형으로 구성될 경우 QFS는 공유 클라이언트 없이 단일 시스템에 구성됩니다. QFS는 표준 VFS vnode 작업을 사용하여 Oracle Solaris 및 Linux 운영 체제와 상호 작용합니다.

QFS 설치 패키지는 SUNWqfsr 및 SUNWqfsu입니다. 이러한 패키지에는 Oracle Hierarchical Storage Manager(HSM) 구성 요소가 포함되지 않습니다.

공유 클라이언트 없이 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.

Oracle HSM 패키지
Oracle HSM을 실행하는 데 필요한 QFS 파일 시스템 및 코드가 포함됩니다. Oracle HSM 설치 패키지는 SUNWsamfsr 및 SUNWsamfsu입니다. 계층적 스토리지 관리가 필요하지 않을 경우 StorageTek QFS 패키지만 설치하십시오.

SAM-Remote
TCP/IP WAN(Wide Area Network) 연결을 통한 원격 테이프 라이브러리 및 드라이브에 대한 액세스를 허용합니다. StorageTek SAM-Remote는 원격으로 테이프 설비를 찾아 일종의 재해 복구 기능을 제공합니다. QFS 또는 SAM-QFS 패키지와 함께 SAM-Remote를 설치할 수 있지만 SAM-Remote는 별도로 사용으로 설정하고 구성해야 합니다. SAM-Remote에 대한 자세한 내용은 `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

Manager 그래픽 사용자 인터페이스
Manager 그래픽 사용자 인터페이스(GUI)인 fsmgr은 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. Manager GUI 설치 및 구성에 대한 자세한 내용은 http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

1.2. 일반적인 보안 원칙

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

1.2.1. 소프트웨어를 최신으로 유지

실행하는 Oracle HSM 버전을 최신으로 유지하십시오. 최신 버전의 소프트웨어는 Oracle Software Delivery Cloud(https://edelivery.oracle.com/)에서 다운로드할 수 있습니다.

1.2.2. 중요 서비스에 대한 네트워크 액세스 제한

Oracle HSM에서는 다음 TCP/IP 포트를 사용합니다.

- tcp/7105는 클라이언트와 MDS 사이에 메타 데이터 트래픽에 사용됩니다.
- tcp/1000은 SAM-Remote에 사용됩니다.
- tcp/6789는 브라우저가 fsmgr에 연결하는 데 사용하는 HTTP 포트입니다.
- tcp/5012는 sam-rpcd에 사용됩니다.

주:

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

1.2.3. 최소 권한 원칙 준수

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

Manager GUI 사용에 대한 자세한 내용은 http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

1.2.4. 시스템 작업 모니터링

시스템 작업을 모니터링하여 Oracle HSM이 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, see /etc/opt/SUNWsamfs/archiver.cmd
- /var/opt/SUNWsamfs/recycler.log, see /etc/opt/SUNWsamfs/recycler.cmd
- /var/opt/SUNWsamfs/releaser.log, see /etc/opt/SUNWsamfs/releaser.cmd
- /var/opt/SUNWsamfs/stager.log, see /etc/opt/SUNWsamfs/stager.cmd
- /var/opt/SUNWsamfs/trace/*

1.2.5. 최신 보안 정보 유지

여러 소스의 보안 정보에 액세스할 수 있습니다. 다양한 소프트웨어 제품에 대한 보안 정보 및 경보는 http://www.us-cert.gov를 참조하십시오. SAM-QFS 관련 정보는 https://communities.oracle.com/portal/server.pt/community/sam_qfs_storage_archive_manager_and_sun_qfs/401을 참조하십시오. 보안 사항을 최신으로 유지하는 기본적인 방법은 최신 버전의 Oracle HSM 소프트웨어를 실행하는 것입니다.

2

보안 설치

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

2.1. 사용자 환경 이해

보안 요구 사항을 더 잘 이해하려면 다음과 같은 질문을 해야 합니다.

2.1.1. 어떤 리소스를 보호해야 하는가?

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

Oracle HSM을 사용하는 경우 다음과 같은 리소스를 보호합니다.

메타 데이터 및 기본 데이터 디스크
이러한 디스크 리소스는 Oracle HSM 파일 시스템을 구축하는 데 사용됩니다. 일반적으로 광섬유 채널(FC)로 연결됩니다. 이러한 디스크에 대한 (Oracle HSM을 통하지 않은) 독립적인 액세스는 정상적인 Oracle HSM 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.

Oracle HSM 테이프
Oracle HSM 파일 시스템에서 스테이징될 때 파일 데이터가 쓰여지는 테이프(대개 테이프 라이브러리에 있음)에 대한 독립적인 액세스는 보안 위험을 가져옵니다.

Oracle HSM 덤프 테이프
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.

Oracle HSM 메타 데이터 서버(MDS)
Oracle HSM 클라이언트는 TCP/IP를 통해 MDS에 액세스할 수 있어야 합니다. 하지만 클라이언트는 외부 WAN 액세스로부터 보호되어야 합니다.

구성 파일 및 설정
Oracle HSM 구성 설정은 관리자 이외의 사용자가 액세스할 수 없도록 보호되어야 합니다. 일반적으로 이러한 설정은 Manager GUI를 사용하는 경우 Oracle HSM에 의해 자동으로 보호됩니다. 비관리 사용자에게 구성 파일을 쓸 수 있도록 허용할 경우 보안 위험에 노출됩니다.

2.1.2. 누구로부터 리소스를 보호하는가?

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.

2.1.3. 전략 리소스에 대한 보호를 실패할 경우 어떻게 되는가?

전략 리소스에 대한 보호 실패는 부적절한 액세스(정상적인 Oracle HSM POSIX 파일 권한을 벗어나는 데이터에 대한 액세스)부터 데이터 손상(정상적인 권한을 벗어나는 디스크나 테이프에 쓰기)에 이르기까지 다양합니다.

2.2. 권장되는 배치 토폴로지

이 절에서는 기반구조 구성 요소를 안전하게 설치 및 구성하는 방법에 대해 설명합니다. Oracle HSM 설치에 대한 자세한 내용은 `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`에서 *Oracle Hierarchical Storage Manager Release 6.0 Customer Documentation Library*를 참조하십시오.

Oracle HSM을 설치하고 구성할 때 다음 사항을 고려하십시오.

별도의 메타 데이터 네트워크
Oracle HSM 클라이언트를 MDS 서버에 연결하는 경우 어떤 WAN에도 연결되어 있지 않은 별도의 TCP/IP 네트워크 및 스위치 하드웨어를 제공하십시오. 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 Oracle HSM 포트에 대한 트래픽을 거부하십시오. 1.2.2절. “중요 서비스에 대한 네트워크 액세스 제한” [8]을 참조하십시오.

FC 영역 분할
FC 영역 분할을 사용하여 디스크에 대한 액세스가 필요하지 않은 모든 서버로부터 Oracle HSM 디스크에 대한 액세스를 거부합니다. 가능하면 별도의 FC 스위치를 사용하여 액세스가 필요한 서버에 만 물리적으로 연결하는 것이 좋습니다.

SAN 디스크 구성 액세스 보호
일반적으로 SAN RAID 디스크는 주로 HTTP, 아니면 TCP/IP를 통해 관리 목적으로 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.

Oracle HSM 패키지 설치
먼저, 필요한 패키지만 설치합니다. 예를 들어, 계층적 스토리지 관리가 필요하지 않을 경우 QFS 패키지만 설치합니다. 설치 후에는 보안에 미칠 영향을 고려하지 않고 기본 Oracle HSM 파일 및 디렉토리 권한과 소유자를 변경해서는 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 OS를 강화하는 방법은 Oracle Solaris 10 보안 지침 및 Oracle Solaris 11 보안 지침을 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.

Oracle HSM 테이프 보안
Oracle HSM 외부에서 Oracle HSM 테이프에 액세스할 수 없도록 하거나 이러한 액세스를 관리자로만 제한합니다. FC 영역 분할을 사용하여 테이프 드라이브에 대한 액세스를 MDS(또는 백업 MDS가 구성된 경우 잠재적인 MDS)로만 제한합니다. 분산 I/O를 사용하도록 구성될 Solaris 클라이언트에게는 테이프 드라이브에 대한 액세스 권한이 필요합니다. 또한 root 전용 권한을 부여하여 테이프 장치 파일 액세스를 제한합니다. Oracle HSM 테이프에 대한 허용되지 않은 액세스는 사용자 데이터를 조작하거나 삭제할 수 있습니다.

백업
samfsdump 또는 qfsdump 명령을 사용하여 Oracle HSM 데이터의 백업을 설정하고 수행합니다. Oracle HSM 테이프에 권장되는 대로 덤프 테이프에 대한 액세스를 제한합니다.

2.2.1. SAM-Remote 설치

SAM-Remote 소프트웨어의 보안 설치에 대한 자세한 내용은 `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

2.2.2. Manager GUI 설치

Manager GUI의 보안 설치에 대한 자세한 내용은 `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

2.2.3. 사후 설치 구성

Oracle HSM 패키지를 설치한 후에는 부록 A. 보안 배치 점검 목록 [19]의 보안 점검 목록을 확인하십시오.

3

보안 기능

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

- 정책 위반 시 파일 시스템 데이터의 노출
- 데이터 손실
- 감지되지 않은 데이터 수정

이러한 보안 위협은 적절한 구성 및 부록 A. 보안 배치 점검 목록 [19]의 사후 설치 점검 목록을 준수하여 최소화할 수 있습니다.

3.1. 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.

3.1.1. 인증

Oracle HSM에서는 호스트 기반 사용자 인증을 사용하여 관리 작업을 수행할 수 있는 사용자를 제어합니다. Manager GUI를 사용한 관리는 주로 다양한 사용자에게 지정된 역할로 제어됩니다. 명령줄을 사용한 관리는 root 사용자로 제한됩니다.

3.1.2. 액세스 제어

Oracle HSM에서 액세스 제어는 두 부분으로 나누어집니다.

- 관리 액세스 제어 – Oracle HSM에 대한 관리 작업을 수행할 수 있는 사용자를 제어합니다. 이 제어는 Manager GUI를 통해 사용자에게 지정된 역할을 기준으로 합니다. 명령줄 작업에서 제어는 root 권한을 기준으로 합니다. Manager GUI에 대한 자세한 내용은 `http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#samqfs`에서 *Oracle Hierarchical Storage Manager and StorageTek QFS Software Release 6.0 Customer Documentation Library*를 참조하십시오.

- 파일/디렉토리 액세스 제어 – Oracle HSM은 풍부한 액세스 제어 기능이 있는 POSIX 호환 파일 시스템을 구현합니다. 자세한 내용은 Oracle HSM 설명서를 참조하십시오.

4

개발자에 대한 보안 고려 사항

개발자는 일반적으로 Oracle HSM과 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 *intro_libsam(3)* 및 *intro_libsamrpc(3)* 매뉴얼 페이지를 참조하십시오.

부록 A

보안 배치 점검 목록

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

1. root 계정 및 Oracle HSM 역할이 지정된 기타 다른 계정에 대해 강력한 암호를 설정합니다. 이 지침에는 다음 내용이 포함되어 있습니다.
   - Manager GUI로 관리 역할이 부여된 모든 계정.
   - *acsss*, *acsdb* 및 *acssa* 사용자 ID(사용되는 경우).
   - 모든 디스크 어레이 관리 계정.
2. Manager GUI에서 기본 사용자 *samadmin*을 사용하는 경우 기본 설치된 암호에서 강력한 암호로 즉시 암호를 변경하십시오. Manager GUI에서는 root를 사용하지 말고 다른 사용자 계정에 필요에 맞게 역할을 지정합니다. 다른 계정 또한 강력한 암호로 보호합니다.
3. WAN 에지 라우터에서 포트 필터링을 설치하여 SAM-Remote에 필요한 경우를 제외하고 1.2절. “일반적인 보안 원칙” [8]에 나열된 포트의 트래픽이 MDS 또는 클라이언트로 들어가지 않도록 막습니다.
4. 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.
5. root 이외의 사용자가 테이프 및 디스크 장치 파일에 액세스할 수 없도록 */dev*를 확인합니다. 이 방식은 Oracle HSM 데이터가 부적절하게 액세스되거나 삭제되지 않도록 예방합니다.
6. Oracle HSM은 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 Oracle HSM 설명서를 참조하십시오.
7. 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 Oracle HSM 테이프 및 백업과 동일한 수준으로 보호해야 합니다.