Oracle SuperCluster M7 시리즈 보안 설명서

부품 번호: **E69650-01**
2016년 2월

부품 번호: E69650-01

설명서 접근성

오라클의 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.

목차

이 설명서 사용

- **개요** – Oracle SuperCluster M7 시리즈 시스템에 대한 보안 환경 계획, 구성 및 유지 관리에 대한 정보를 제공합니다.
- **대상** - 기술자, 시스템 관리자 및 공인 서비스 공급자
- **필요한 지식** – UNIX 및 데이터베이스 관리에 대한 고급 지식이 필요합니다.

제품 설명서 라이브러리

이 제품과 관련 제품들에 대한 설명서 및 리소스는 http://www.oracle.com/goto/sc-m7/docs에서 사용할 수 있습니다.

피드백

http://www.oracle.com/goto/docfeedback에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

보안 주체 이해

이 설명서에서는 Oracle SuperCluster M7 시리즈 시스템에 대한 보안 환경 계획, 구성 및 유지 관리에 대한 정보를 제공합니다.

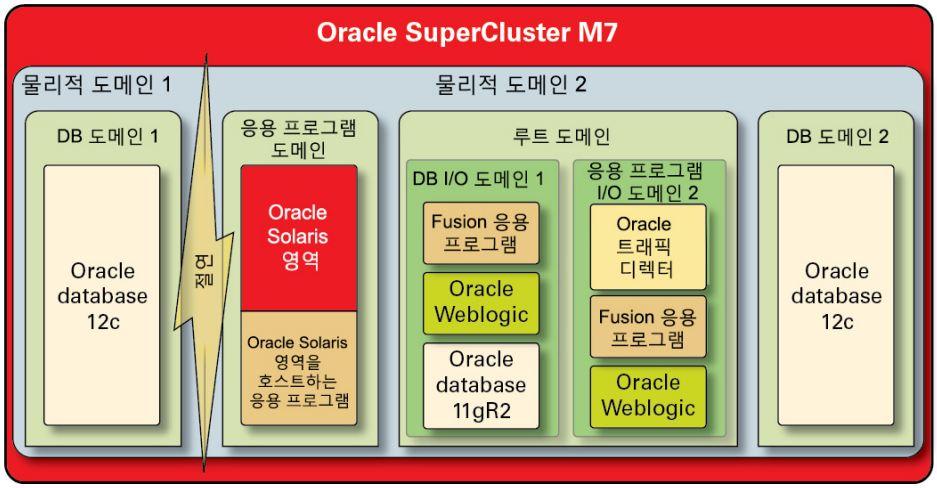
이 절에서는 다음 항목을 다룹니다.

보안 격리

SuperCluster M7은 해당 보안 및 보증 요구 사항에 따라 클라우드 공급자가 선택할 수 있는 다양한 격리 전략을 지원합니다. 이러한 유연성 덕분에 클라우드 공급자는 해당 비즈니스에 따라 맞춤화된 사용자 정의된 보안 다중 테넌트 기반구조를 만들 수 있습니다.

SuperCluster M7은 각각 고유한 기능 세트가 포함된 여러 작업 부하 격리 전략을 지원합니다. 각 구현 전략은 개별적으로 사용할 수 있지만, 하이브리드 접근 방법에 따라 함께 사용하여 클라우드 공급자가 보안, 성능, 가용성 요구 및 기타 요구 균형을 보다 효과적으로 조정할 수 있는 기반구조를 배치할 수 있습니다.

그림 1 동적 테넌트 구성을 포함하는 보안 격리



클라우드 공급자는 해당 테넌트 호스트가 다른 작업 부하와 물리적으로 격리되어야 하는 응용 프로그램 및 데이터베이스를 실행 중인 경우 물리적 도메인(PDomain이라고도 부름)을 사용할 수 있습니다. 조직에 대한 배치의 중요도, 조직에 포함된 정보의 중요도, 준수 요구 사항으로 인해 또는 단순히 데이터베이스 또는 응용 프로그램 작업 부하가 전체 물리적 시스템의 리소스를 완전히 사용하게 되기 때문에 전용 물리적 리소스가 배치에 필요할 수 있습니다.

하이퍼바이저로 조정되는 격리가 필요한 조직의 경우, 전용 도메인으로 참조되는 Oracle VM Server for SPARC 도메인은 응용 프로그램 및/또는 데이터베이스 인스턴스를 격리하는 가상 환경을 만드는 데 사용됩니다. SuperCluster 설치의 일부로 생성되는 전용 도메인은 각각 Oracle Solaris OS의 고유 인스턴스를 실행합니다. 물리적 리소스에 대한 액세스는 SPARC 프로세서에 구축된 하드웨어 지원 하이퍼바이저에 의해 조정됩니다.

또한 SuperCluster는 루트 도메인이라고 부르는 SR-IOV(단일 루트 I/O 가상화) 기술을 사용하는 추가 도메인을 만들 수 있게 해줍니다. 루트 도메인은 1개 또는 2개의 IB HCA와 10GbE NIC를 소유합니다. 사용자는 I/O 도메인으로 참조되는 추가 도메인을 루트 도메인 위에 동적으로 만들 수 있습니다. SuperCluster M7에는 이를 만들고 관리하기 위한 브라우저 기반 도구가 포함됩니다.

이러한 각 도메인 내에서 클라우드 소비자 테넌트는 Oracle Solaris 영역 기술을 활용해서 추가 격리 환경을 만들 수 있습니다. 영역을 사용하면 개별 응용 프로그램 또는 데이터베이스 인스턴스나 응용 프로그램 또는 데이터베이스 인스턴스 그룹을 단일 OS 커널에서 총체적으로 실행되는 하나 이상의 가상화된 컨테이너에 배치할 수 있습니다. 가상화에 대한 이러한 경량 접근 방법은 배치된 서비스 주위에 보다 강력한 보안 경계를 만들기 위해 사용됩니다.

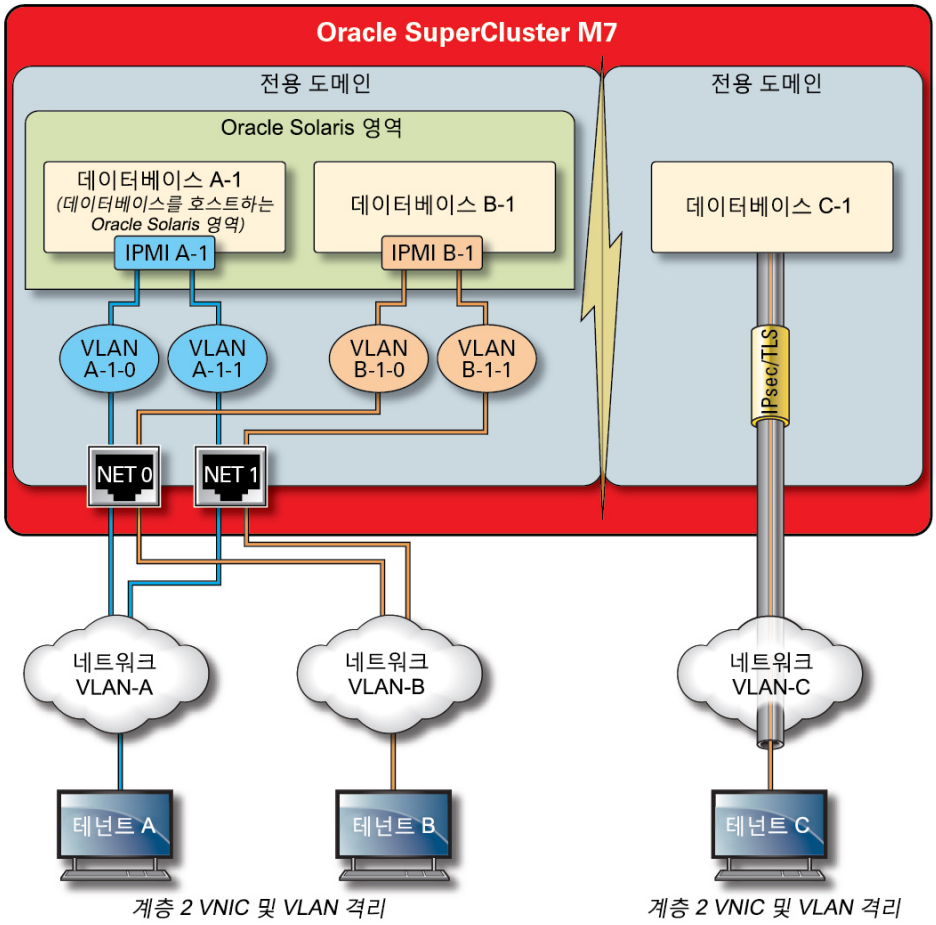
SuperCluster에서 여러 응용 프로그램 및 데이터베이스를 호스트하는 테넌트는 또한 Oracle Solaris 영역, I/O 도메인 및 전용 도메인 기반의 격리 전략 조합을 사용하는 하이브리드 접근 방법을 사용하여 해당 클라우드 기반구조 요구에 맞는 유연하지만 탄력적인 기반구조를 만들 수 있습니다. 다양한 가상화 옵션을 통해 SuperCluster는 클라우드 호스트 테넌트가 하드웨어 계층에서 안전하게 격리될 수 있게 해주며, 런타임 환경에서 향상된 보안 및 추가적인 격리를 위해 Oracle Solaris 영역을 제공합니다.

이러한 개별 응용 프로그램, 데이터베이스, 사용자 및 프로세스가 해당 호스트 OS에서 올바르게 격리되도록 보장하는 것이 올바른 첫 단계입니다. 하지만, SuperCluster에서 사용되는 3개의 기본 네트워크와 네트워크 격리 기능 및 네트워크를 통해 전송되는 통신의 보호 방법도 고려하는 것이 중요합니다.

- 10GbE 클라이언트 액세스 네트워크
- 개인 IB 서비스 네트워크
- 관리 네트워크

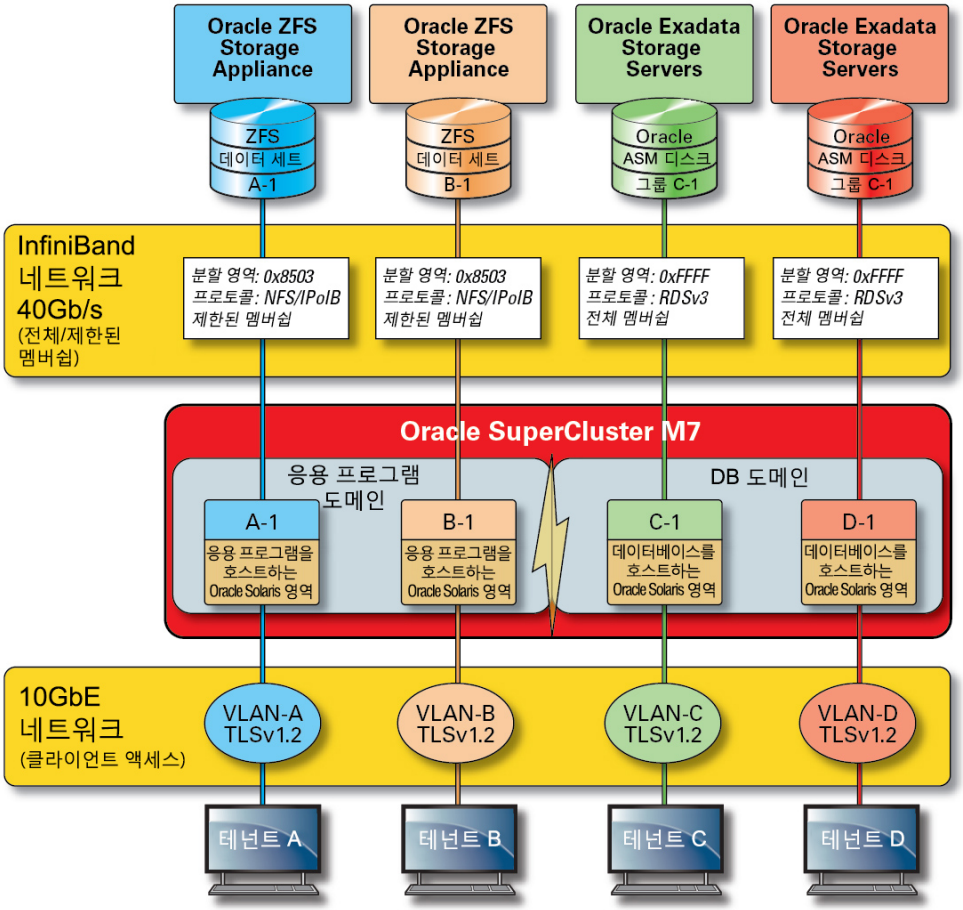
SuperCluster 클라이언트 액세스 네트워크를 통해 전송되는 네트워크 트래픽은 여러 기술을 사용해서 격리시킬 수 있습니다. 이 그림에서는 4개의 데이터베이스 인스턴스가 3개의 고유한 VLAN(가상 LAN)에서 작동하도록 구성된 한 가지 가능한 구성을 보여줍니다. SuperCluster의 네트워크 인터페이스가 VLAN을 사용하도록 구성하면 Oracle Solaris 영역 사이는 물론 Oracle VM Server for SPARC 전용 도메인 사이에 네트워크 트래픽을 격리시킬 수 있습니다.

그림 2 클라이언트 액세스 네트워크를 통한 보안 네트워크 격리



SuperCluster에는 데이터베이스 인스턴스가 Exadata Storage Server와 ZFS Storage Appliance에 저장된 정보에 액세스하고 클러스터화 및 고가용성을 위해 필요한 내부 통신을 수행하기 위해 사용되는 개인 IB 네트워크가 포함되어 있습니다. 이 그림은 SuperCluster M7에 대한 보안 네트워크 격리를 보여줍니다.

그림 3 40Gbs IB 네트워크의 보안 네트워크 격리



기본적으로 SuperCluster IB 네트워크는 설치 및 구성 중에 6개의 고유 분할 영역으로 분할됩니다. 기본 분할 영역은 변경할 수 없지만, Oracle에서는 IB 네트워크의 추가 세그먼트화가 필요한 경우 추가 전용 분할 영역 만들기 및 사용이 지원되지 않습니다. 또한 IB 네트워크에서는 제한된 영역 멤버쉽 및 전체 분할 영역 멤버쉽 표기가 지원됩니다. 제한된 멤버는 전체 멤버와만 통신할 수 있으며, 전체 멤버는 분할 영역의 모든 노드와 통신할 수 있습니다. 응용 프로그램 I/O 도메인 및 Oracle Solaris 11 영역은 전체 멤버로 구성된 ZFS Storage Appliance와만 통신하고 동일 분할 영역에 존재할 수 있는 다른 제한된 멤버쉽 노드와는 통신할 수 없도록 해당 IB 분할 영역의 제한된 멤버로 구성할 수 있습니다.

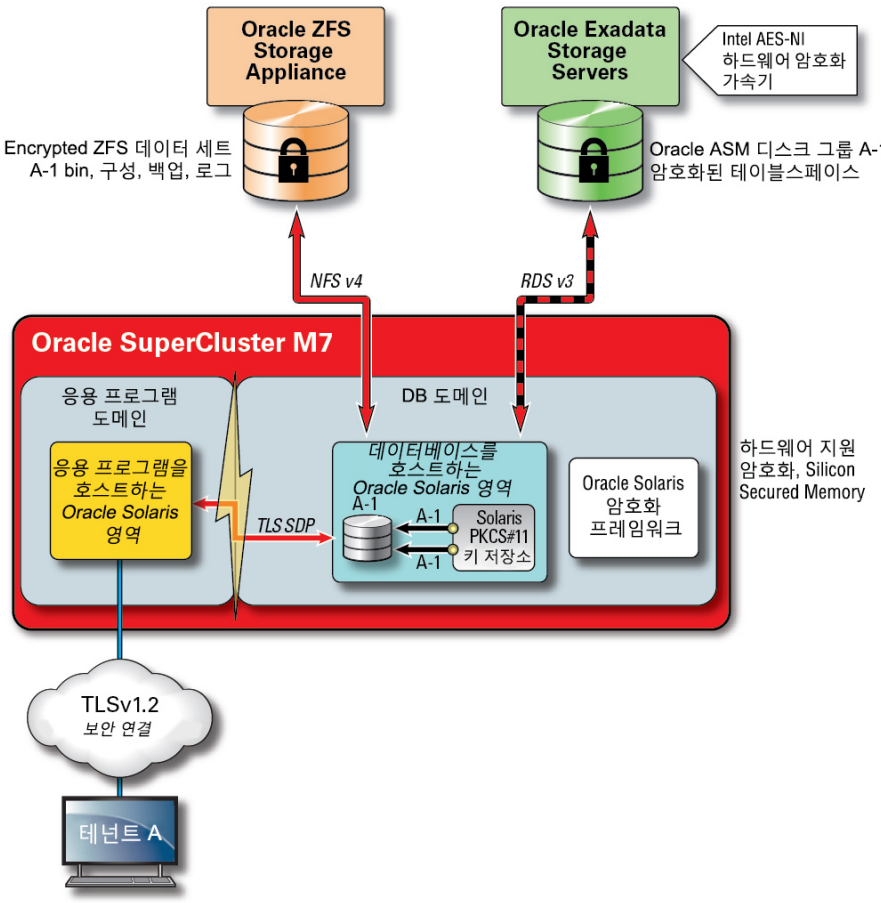
SuperCluster에는 또한 모든 핵심 구성 요소를 관리 및 모니터할 수 있는 전용 관리 네트워크가 포함됩니다. 이 전략은 클라이언트 요청을 처리하는 데 사용되는 네트워크 경로로부터 중요한 관리 및 모니터링 기능을 격리시킵니다. 이러한 관리 네트워크에 대해 관리 기능을 격리 상태로 유지함으로써 SuperCluster는 클라이언트 액세스 및 IB 네트워크를 통해 노출되는 네트워크 공격 영역을 더 줄일 수 있습니다. 클라우드 공급자는 이 권장 방식 및 격리 관리, 모니터링 및 관련 기능을 따라서 관리 네트워크에서만 액세스할 수 있도록 하는 것이 좋습니다.

데이터 보호

클라우드 공급자에게 데이터 보호는 보안 전략의 핵심입니다. 개인 정보 보호 및 준수 요구의 중요성에 비춰볼 때 다중 테넌트 기반구조를 고려 중인 조직은 데이터베이스 간에 전송되는 정보의 보호를 위해 암호화 사용을 중요하게 고려해야 합니다. 데이터 보호를 위한 암호화 서비스 사용은 네트워크 간에 전송되고 디스크에 상주하는 정보의 기밀성 및 무결성을 보장하기 위해 대칭적으로 적용됩니다.

SuperCluster의 SPARC M7 프로세서에는 보안에 민감한 IT 환경의 데이터 보호 요구를 위해 하드웨어 지원 고성능 암호화 기술이 사용됩니다. SPARC M7 프로세서에는 또한 메모리 스크래핑, 은밀한 메모리 손상, 버퍼 오버런 및 관련 공격과 같은 악의적인 응용 프로그램 레벨 공격을 방지할 수 있는 Silicon Secured Memory 기술이 사용됩니다.

그림 4 하드웨어 지원 암호화 가속화 및 메모리 침입 방지로 제공되는 데이터 보호



데이터 보호가 거의 모든 기반구조에 포함되어 있는 보안 다중 테넌트 기반구조에서 SuperCluster 및 해당 지원 소프트웨어는 조직이 성능을 희생하지 않으면서도 보안 및 준수 목적을 달성할 수 있게 해줍니다. SuperCluster에는 암호화 작업 가속화 및 성능에 영향이 없는 메모리 침입 방지를 보장하기 위해 SPARC M7 프로세서에 포함되도록 설계된 온코어 기반 암호화 명령 및 Silicon Secured Memory 기능이 사용됩니다. 이러한 기능은 향상된 암호화 성능은 물론 메모리 침입 확인 기능을 제공하며, 테넌트 작업 부하를 서비스하는 데 더 많은 전용 리소스를 지정할 수 있으므로 전반적인 성능 향상에도 도움이 됩니다.

SPARC 프로세서는 16개 이상의 산업 표준 암호화 알고리즘에 대해 하드웨어 지원 암호화 가속화 지원을 제공합니다. 이러한 알고리즘은 공개 키 암호화, 대칭 키 암호화, 난수 생성, 디지

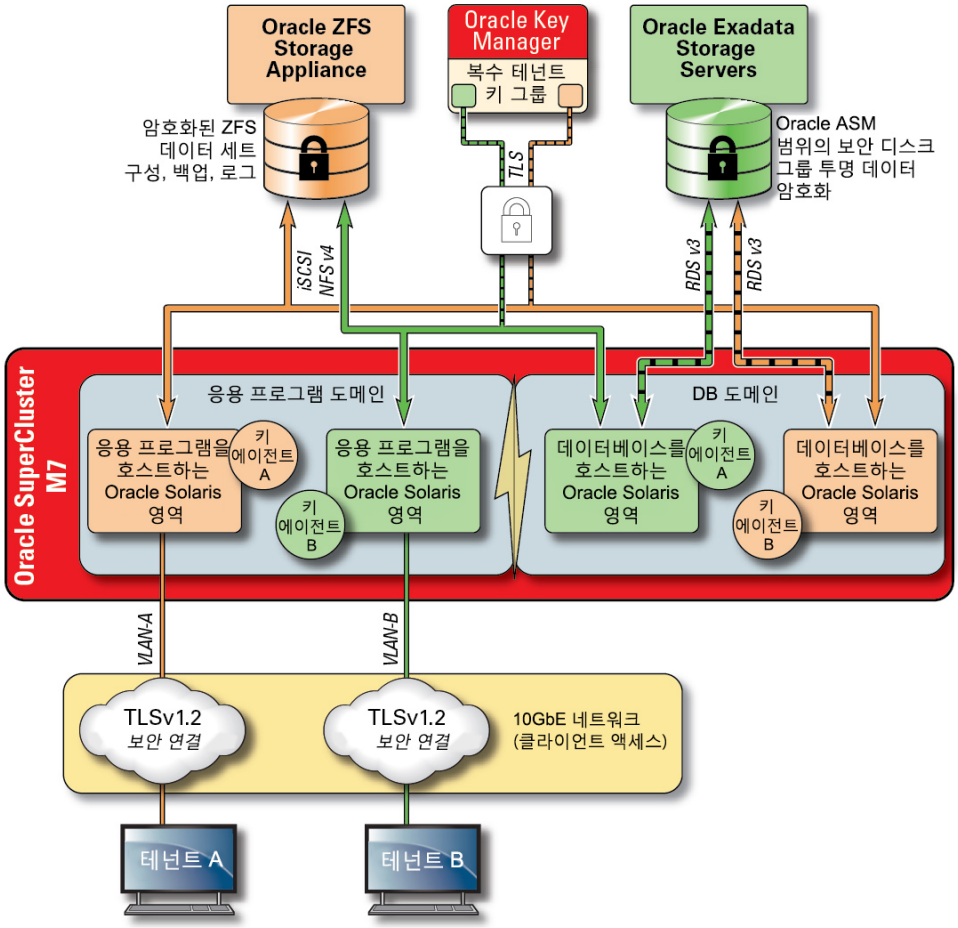
털 서명 및 메시지 다이제스트의 계산 및 확인을 포함해서 대부분의 현대적인 암호화 요구를 지원합니다. 또한 OS 레벨에서 암호화 하드웨어 가속화는 보안 셸, IPSec/IKE 및 암호화된 ZFS 데이터 세트에 대해 기본적으로 사용으로 설정되어 있습니다.

Oracle Database 및 Oracle Fusion Middleware는 SuperCluster에서 사용되는 Oracle Solaris OS 및 SPARC 프로세서를 자동으로 식별합니다. 이렇게 하면 데이터베이스 및 미들웨어가 TLS, WS-Security, 테이블스페이스 암호화 작업을 위해 플랫폼의 하드웨어 암호화 가속화 기능을 자동으로 사용할 수 있습니다. 또한 메모리 보호를 위해 Silicon Secured Memory 기능도 사용할 수 있고, 최종 사용자 구성을 필요로 하지 않아도 응용 프로그램 데이터 무결성을 보장합니다. IB 네트워크를 통해 전송되는 테넌트 특정의 영역 간 IP 기반 통신의 기밀성 및 무결성을 보호하려면 IPSec(IP 보안) 및 IKE(인터넷 키 교환)를 사용합니다.

암호화 키의 관리 방법에 대한 논의 없이는 어떠한 암호화 토론도 완전한 것이 될 수 없습니다. 특히 대규모 서비스 모음에서 암호화 키 생성 및 관리는 전통적으로 조직의 중요 과제였으며, 클라우드 기반 다중 테넌트 환경에서는 이러한 과제가 더욱 중요해지고 있습니다. SuperCluster에서 ZFS 데이터 세트 암호화 및 Oracle Database 투명한 데이터 암호화는 Oracle Solaris PKCS#11 키 저장소를 활용해서 마스터 키를 안전하게 보호할 수 있습니다. Oracle Solaris PKCS#11 키 저장소를 사용하면 모든 마스터 키 작업에 대해 SPARC 하드웨어 지원 암호화 가속화가 자동으로 사용됩니다. 이를 통해 SuperCluster는 ZFS 데이터 세트, Oracle Database 테이블스페이스 암호화, 암호화된 데이터베이스 백업(Oracle Recovery Manager [Oracle RMAN] 사용), 암호화된 데이터베이스 내보내기(Oracle Database의 Data Pump 기능 사용) 및 리두 로그(Oracle Active Data Guard 사용)와 연관된 암호화 및 암호 해독 작업의 성능을 크게 향상시킬 수 있습니다.

공유 전자 지갑 접근 방법을 사용하는 테넌트는 ZFS Storage Appliance를 활용해서 클러스터의 모든 노드 간에 공유할 수 있는 디렉토리를 만들 수 있습니다. 공유되는 중앙화된 키 저장소를 사용하면 키가 클러스터의 각 노드 간에 동기화되기 때문에 테넌트가 Oracle RAC(Real Application Cluster)와 같은 클러스터화된 데이터베이스 기반구조에서 키 관리, 유지 관리 및 순환을 보다 효과적으로 수행할 수 있습니다.

그림 5 Oracle Key Manager를 사용하여 다중 테넌트 키 관리 시나리오를 통해 데이터 보호



클라우드 기반 다중 테넌트 환경에서 여러 호스트 및 응용 프로그램과 연관된 키 관리의 복잡성 및 문제를 해결하기 위해서는 관리 네트워크 통합된 어플라이언스로서 선택적인 Oracle Key Manager를 사용합니다. Oracle Key Manager는 Oracle Database, Oracle Fusion Applications, Oracle Solaris 및 ZFS Storage Appliance에서 사용되는 암호화 키에 대한 액세스를 중앙에서 권한 부여, 보안 설정 및 관리합니다. Oracle Key Manager는 또한 Oracle StorageTek 암호화 테이프 드라이브를 지원합니다. ZFS 데이터 세트(파일 시스템) 레벨에서 암호화 정책 및 키 관리를 사용하면 키 파괴를 통해 테넌트 파일 시스템에 대한 삭제가 보장됩니다.

Oracle Key Manager는 키 수명 주기 관리 작업 및 신뢰할 수 있는 키 저장소를 지원하는 완벽한 키 관리 어플라이언스입니다. Oracle에서 제공되는 추가적인 Sun Crypto Accelerator 6000 PCIe 카드로 구성된 경우, Oracle Key Manager는 FIPS 186-2 호환 난수 생성은 물론 AES 256비트 암호화 키의 FIPS 140-2 레벨 3 인증 키 저장소를 제공합니다. SuperCluster 내에서 모든 데이터베이스 및 응용 프로그램 도메인은 해당 전역 영역 및 비전역 영역을 포함해서 응용 프로그램, 데이터베이스 및 암호화된 ZFS 데이터 세트와 연관된 키 관리를 위해 Oracle Key Manager를 사용하도록 구성할 수 있습니다. 실제로 Oracle Key Manager는 개별 또는 여러 데이터베이스 인스턴스, Oracle RAC, Oracle Active Data Guard, Oracle RMAN 및 Oracle Database의 Data Pump 기능과 연관된 키 관리 작업을 지원할 수 있습니다.

마지막으로 Oracle Key Manager로 강제 적용되는 책임 구분을 통해 각 테넌트는 모든 키 관리 작업에 대한 일관된 가시성을 확보하여 해당 암호화 키를 완벽하게 제어할 수 있습니다. 정보 보호에 있어서 키가 얼마나 중요한지를 생각한다면, 사용 기간 전반에 걸쳐 키가 올바르게 보호되도록 보장하기 위해 테넌트가 역할 기반 액세스 제어 및 감사에 필요한 레벨을 구현하는 것이 필수적입니다.

관련 정보

- “Oracle Key Manager” [116]

액세스 제어

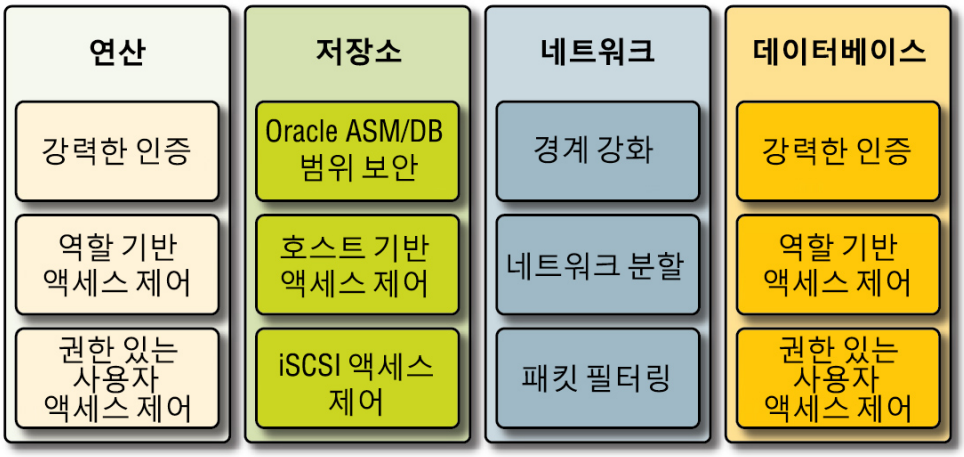
클라우드 호스팅 환경 전략을 채택하는 조직에게 있어서 액세스 제어는 풀어야 할 가장 중요한 과제 중 하나입니다. 테넌트는 공유된 기반구조에 저장된 정보가 보호되고 권한 부여된 호스트, 서비스, 개인, 그룹 및 역할에만 제공된다는 것을 확신할 수 있어야 합니다. 권한 부여된 호스트, 개인 및 서비스는 또한 특정 작업에 필요한 권한만 가질 수 있도록 최소 권한의 원칙에 따라 추가적인 제한을 받아야 합니다.

SuperCluster는 스택의 모든 계층을 포함하는 유연하고 계층화된 액세스 제어 기반구조를 사용해서 최종 사용자, 데이터베이스 관리자 및 시스템 관리자를 포함한 다양한 역할을 지원합니다. 이를 통해 조직은 호스트, 응용 프로그램 및 데이터베이스를 개별적으로 보호하는 정책을 정의하고 이러한 서비스가 실행되는 기본 연산, 저장소 및 네트워크 기반구조를 보호할 수 있습니다.

가상화 및 OS 계층에서 액세스 제어는 네트워크에 노출되는 서비스 수를 줄이는 것으로부터 시작됩니다. 이렇게 하면 Oracle VM Server for SPARC 콘솔, 도메인 및 영역에 대한 액세스를 제어하는 데 도움이 됩니다. 시스템이 액세스될 수 있는 시작점의 수를 줄임으로써 액세스 제어 정책의 수도 줄일 수 있으며, 시스템 수명 전반에 걸쳐 보다 쉽게 유지 관리할 수 있습니다.

Oracle Solaris OS 내에서 액세스 제어는 Oracle Solaris RBAC(역할 기반 액세스 제어) 기능과 POSIX 권한의 조합을 통해 구현됩니다. SuperCluster에서 실행되는 호스트, 응용 프로그램, 데이터베이스 및 관련 서비스를 네트워크 기반 공격으로부터 보호하는 기능도 똑같이 중요합니다. 이를 위해서는 테넌트가 먼저 승인된 네트워크 서비스만 실행 중이고 들어오는 네트워크 연결을 수신 중인지 확인해야 합니다. 네트워크 공격 표면을 최소화한 다음에는 승인된 네트워크 및 인터페이스에서만 들어오는 연결을 수신하도록 테넌트가 남은 서비스를 구성해야 합니다. 이러한 간단한 방식은 보안 셸과 같은 관리 프로토콜을 관리 네트워크 이외의 다른 위치에서 액세스할 수 없도록 보장하는 데 도움이 됩니다.

그림 **6** 종단간 액세스 제어 요약



또한 테넌트는 Oracle Solaris의 IP 필터 서비스와 같은 호스트 기반 방화벽을 구현하도록 선택할 수도 있습니다. 호스트 기반 방화벽은 네트워크 서비스에 대해 보다 다양한 액세스 제어 방식을 호스트에 제공하기 때문에 유용합니다. 예를 들어, IP 필터는 stateful 패킷 필터링을 지원하며, 이 기능은 IP 주소, 포트, 프로토콜, 네트워크 인터페이스 및 트래픽 방향에 따라 패킷을 필터링할 수 있습니다. 이러한 기능은 여러 네트워크 인터페이스를 작동하고 다양한 인바운드 및 아웃바운드 네트워크 통신을 지원하는 SuperCluster와 같은 플랫폼에 중요합니다.

SuperCluster에서 IP 필터는 Oracle VM Server for SPARC 도메인 내에 구성하거나, Oracle Solaris 영역 내에서 작동할 수 있습니다. 이를 통해 데이터베이스 서비스가 제공된 동일한 OS 컨테이너에 네트워크 액세스 제어 정책을 강제 적용할 수 있습니다. 다중 테넌트 시나리오에서 아웃바운드 네트워크 작업의 양은 최소한으로만 유지될 가능성이 높으며, 특정 네트워크 인터페이스 및 대상으로 통신을 제한하는 정책을 만들 수 있도록 쉽게 분류할 수 있습니다. 다른 모든 트래픽은 거부되고 "기본 거부" 정책에 따라 기록되어 인바운드 및 아웃바운드 모두 허용되지 않은 통신이 차단됩니다.

Oracle End User Security를 통해 테넌트는 SSO(Single Sign-On) 및 중앙화된 사용자 및 역할 관리를 지원하기 위해 기존 ID 관리 서비스와 자신의 응용 프로그램 및 데이터베이스를 통합할 수 있습니다. 특히, Oracle End User Security는 (1) 데이터베이스 사용자 및 관리자에 대한 프로비전 및 프로비전 해제, (2) 암호 관리 및 셀프 서비스 암호 재설정, (3) 전역 데이터베이스 역할을 사용한 권한 부여 관리를 중앙화하여 도움을 줍니다. Kerberos 또는 PKI와 같은 다중 요소 인증 방법이 필요한 조직은 Oracle Advanced Security를 활용할 수 있습니다.

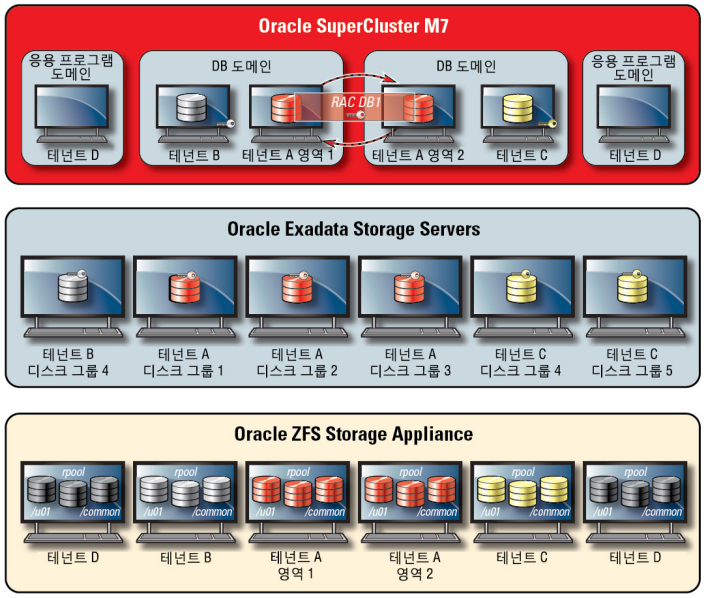
Oracle Exadata Storage Server 기술은 각각 고유한 권한을 포함하는 사전 정의된 사용자 계정 세트를 지원합니다. Oracle Exadata Storage Server 관리를 수행하는 관리자는 시스템에 액세스하기 위해 이러한 사전 정의된 역할 중 하나를 사용해야 합니다. 반면에 ZFS Storage Appliance는 역할 및 권한의 개별 지정을 지원하는 로컬 및 원격 관리 계정을 만들 수 있도록 지원합니다.

기본적으로 SuperCluster에 사용되는 Oracle Exadata Storage Server는 Oracle Automatic Storage Management 기능을 사용해서 데이터베이스에 의해 액세스됩니다. 이 기능을 통해 클라우드 공급자는 각 테넌트에 대해 해당 용량, 성능 및 가용성 요구 사항을 충족시킬 수 있는 고유한 디스크 그룹을 만들 수 있습니다. 액세스 제어 측면에서 Oracle Automatic Storage Management는 개방형 보안, Oracle Automatic Storage Management 범위 보안 및 데이터베이스 범위 보안이라는 세 가지 액세스 제어 모드를 지원합니다.

다중 테넌트 시나리오에서는 가장 미세한 레벨의 액세스 제어를 제공하는 데이터베이스 범위 보안이 권장됩니다. 이 모드에서는 단일 데이터베이스에서만 액세스할 수 있는 정도로 디스크 그룹을 구성할 수 있습니다. 즉, 데이터베이스 관리자와 사용자 모두 자신이 액세스 권한이 있는 정보가 포함된 그리드 디스크에만 액세스하도록 제한할 수 있습니다. 개별 데이터베이스가 여러 조직 및 테넌트를 지원할 수 있는 데이터베이스 통합 시나리오의 경우에는 각 테넌트가 자신이 소유하는 저장소만 액세스하고 조작할 수 있도록 하는 것이 중요합니다. 특히, 앞에서 논의한 작업 부하 및 데이터베이스 격리 전략과 결합하면, 테넌트가 개별 데이터베이스에 대한 액세스를 효과적으로 분류할 수 있게 하는 것이 가능합니다.

데이터베이스 범위 보안은 Oracle ASM 그리드 디스크에 대한 액세스를 제한하는 데 효과적인 도구입니다. 이 그림은 ZFS 보안과 함께 Oracle ASM 범위 보안을 보여줍니다. SuperCluster 플랫폼에 대량의 Oracle Database 인스턴스가 배치되는 경우에는 생성, 지정 및 관리해야 하는 키 수를 크게 줄여주는 테넌트별 Oracle ASM 범위 보안 전략이 보다 효과적일 수 있습니다. 또한 데이터베이스 범위 보안을 위해서는 각 데이터베이스에 대해 별도의 디스크 그룹을 만들어야 하기 때문에 이 접근 방법은 Exadata Storage Server에서 만들어야 하는 개별 그리드 디스크의 수도 크게 줄일 수 있습니다.

그림 7 테넌트별 Oracle ASM 범위 보안



SuperCluster는 Oracle Solaris 데이터 링크 보호를 활용해서 악의적인 테넌트 가상 시스템이 네트워크에 일으킬 수 있는 잠재적인 손상을 방지합니다. 이 통합된 Oracle Solaris 기능은 IP 및 MAC 주소 스푸핑은 물론 L2 프레임 스푸핑(예: Bridge Protocol Data Unit 공격)과 같은 기본적인 위협에 대한 보호 기능을 제공합니다. Oracle Solaris 데이터 링크 보호는 다중 테넌트 환경 내에 배치된 모든 Oracle Solaris 비전역 영역에 개별적으로 적용되어야 합니다.

개별 테넌트는 Exadata Storage Server에 대한 관리 또는 호스트 레벨의 액세스 권한이 필요하지 않으므로, 이러한 액세스 권한을 제한하는 것이 좋습니다. Exadata Storage Server는 SuperCluster 데이터베이스 도메인(클라우드 공급자가 운영하는)의 액세스를 허용하면서도 테넌트 비전역 영역 및 데이터베이스 I/O 도메인에 대한 직접 액세스를 방지하도록 구성해야 합니다. 이렇게 하면 관리 네트워크의 신뢰할 수 있는 위치에서만 Exadata Storage Server를 관리할 수 있습니다.

테넌트의 보안 구성이 정의 및 구현된 다음에는 서비스 공급자가 테넌트 특정 전역 및 비전역 영역을 읽기 전용 환경으로 변경할 수 없도록 구성하는 추가적인 단계를 고려할 수 있습니다. 변경할 수 없는 영역은 테넌트가 자신의 고유 서비스를 운영하는 탄력적이고 무결성이 높은 작동 환경을 만들 수 있습니다. Oracle Solaris의 기본 보안 기능을 기반으로 작성되는 변경할 수 없는 영역은 일부(또는 모든) OS 디렉토리 및 파일을 클라우드 서비스 공급자의 개입 없이 변경할 수 없도록 보장합니다. 이렇게 읽기 전용 방식을 강제로 적용하면 허용되지 않은 변경을 방지하고, 보다 강력한 변경 관리 절차를 촉진시키고, 커널 및 사용자 기반 악성 프로그램의 삽입을 방해하는 데 도움이 됩니다.

모니터링 및 준수 감사

클라우드 환경에서 사전적인 모니터링 및 로깅은 매우 중요하며, 많은 경우에 보안 허점 및 취약점으로부터 시작되는 공격을 완화하는 데 도움이 됩니다. 준수 보고 또는 사고 대응에 관계없이 모니터링 및 감사는 클라우드 공급자에게 중요한 기능이며, 테넌트 조직은 자신의 호스팅 환경에 대해 향상된 가시성을 얻기 위해 잘 정의된 로깅 및 감사 정책을 강제 적용해야 합니다. 모니터링 및 감사는 보호되는 환경의 위험 또는 치명적인 특성에 따라 적용 강도가 결정되는 경우가 많습니다.

SuperCluster 클라우드 기반구조는 Oracle Solaris 감사 부속 시스템을 사용해서 감사 이벤트 정보를 수집, 저장 및 처리합니다. 각 테넌트 특정 비전역 영역은 각 SuperCluster 전용 도메인(전역 영역)에 로컬로 저장되는 감사 레코드를 생성합니다. 이 접근 방법은 개별 테넌트가 자신의 감사 정책, 구성 또는 기록된 데이터를 변경할 수 없도록 보장합니다. 이러한 작업의 책임은 클라우드 서비스 공급자에게 속하기 때문입니다. Oracle Solaris 감사 기능은 테넌트 영역 및 도메인 모두에서 모든 관리 작업, 명령 호출 및 심지어 개별 커널 레벨의 시스템 호출까지 모니터합니다. 이 기능은 세부적인 구성이 가능하며, 전역, 영역별 및 사용자별 감사 정책까지 제공합니다. 테넌트 영역을 사용하도록 구성된 경우, 각 영역의 감사 레코드는 전역 영역에 저장하여 훼손되지 않도록 보호할 수 있습니다. 전용 도메인 및 I/O 도메인도 또한 고유 Oracle Solaris 감사 기능을 사용해서 가상화 이벤트 및 도메인 관리와 연관된 작업 및 이벤트를 기록합니다.

Exadata Storage Server 및 ZFS Storage Appliance는 로그인, 하드웨어 및 구성 감사를 지원합니다. 이를 통해 조직은 장치에 액세스한 사용자 및 수행된 작업을 확인할 수 있습니다. 최종 사용자에게 직접적으로 노출되지는 않지만, Oracle Solaris 감사는 ZFS Storage Appliance에서 제공되는 정보에 대한 기본 컨텐츠를 제공합니다.

마찬가지로, Exadata Storage Server 감사는 Exadata Storage Server 소프트웨어에서 제공되는 하드웨어 및 구성 경보 정보와 함께 사용할 수 있는 다양한 시스템 이벤트의 모음입니다. Oracle Solaris의 IP 필터 기능을 통해 클라우드 공급자는 인바운드 및 아웃바운드 네트워크 통신을 선택적으로 기록할 수 있으며, 이러한 기능을 도메인 및 비전역 영역 레벨 모두에 적용할 수 있습니다. 이를 통해 조직은 자신의 네트워크 정책을 세그먼트화하고 작업 레코드를 확인할 수 있습니다. 선택적으로, Oracle Solaris의 감사 정보는 물론 다양한 Oracle 및 비Oracle 데이터베이스로부터 감사 정보를 안전하게 집계 및 분석할 수 있도록 Oracle Audit Vault and Database Firewall 어플라이언스를 배치할 수 있습니다.

Oracle Enterprise Manager와의 통합을 통해 SuperCluster는 다양한 클라우드 셀프 서비스 작업을 지원할 수 있습니다. 클라우드 공급자는 리소스 풀을 정의하고, 개별 테넌트에 풀 및 할당량을 지정하고, 서비스 카탈로그를 식별 및 게시하고, 궁극적으로 응용 프로그램 및 데이터베이스 리소스의 모니터링 및 로깅을 지원할 수 있습니다.

관련 정보

- “준수 감사” [109] [109]

- “보안 모니터링” [119]

SuperCluster 보안 모범 사례를 위한 추가 리소스

SuperCluster 보안, 기반구조 및 모범 사례에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- Oracle SuperCluster M7 - 플랫폼 보안 원칙 및 기능

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7 - 보안 사설 클라우드 기반구조

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Oracle SuperCluster에 대한 종합 데이터 보호

  https://community.oracle.com/docs/DOC-918251
- Oracle SuperCluster에 대한 보안 데이터 통합

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster 및 PCI 준수

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - STIG(보안 기술 구현 설명서) 검증 및 모범 사례

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Developer’s Guide to Oracle Solaris 11 Security

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 및 PCI 준수

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 감사 빠른 시작

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Oracle Solaris 11 보안 지침

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database 보안 설명서 12c 릴리스 1(12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

기본 보안 구성 검토

이 항목에서는 SuperCluster M7에 대한 기본 보안 구성에 대해 설명합니다.

기본 보안 설정

SuperCluster M7 소프트웨어는 여러 기본 보안 설정으로 설치됩니다. 가능한 모든 경우에 기본 보안 설정을 사용하십시오.

- 암호 정책은 최소한의 암호 복잡성을 강제 적용합니다.
- 로그인 시도가 실패할 경우, 실패한 시도의 특정 횟수 이후 잠금이 설정됩니다.
- OS의 모든 기본 시스템 계정이 잠기고 로그인이 금지됩니다.
- `su` 명령 사용을 위한 제한된 기능이 구성됩니다.
- 불필요한 프로토콜 및 모듈은 OS 커널에서 사용 안함으로 설정됩니다.
- 부트 로더는 암호로 보호됩니다.
- `inetd`(인터넷 서비스 데몬)를 포함해서 모든 불필요한 시스템 서비스가 사용 안함으로 설정됩니다.
- 소프트웨어 방화벽은 저장소 셸에 구성되어 있습니다.
- 중요 보안 관련 구성 파일 및 실행 파일에는 제한적인 파일 권한이 설정됩니다.
- SSH 수신 포트는 관리 및 개인 네트워크로 제한됩니다.
- SSH는 v2 프로토콜로 제한됩니다.
- SSH 인증 방식이 사용 안함으로 설정되었는지 확인합니다.
- 특정 암호화 암호가 구성됩니다.
- 시스템에서 스위치는 네트워크의 데이터 트래픽과 구분됩니다.

기본 사용자 계정 및 암호

이 표에서는 SuperCluster M7에 대한 기본 사용자 계정 및 암호를 보여줍니다. 기본 암호 변경을 위한 추가 지침은 각 구성 요소에 대한 이후 장에 제공되어 있습니다.

구성 요소	사용자 이름	암호	사용자 계정 및 암호 정보
Oracle ILOM: ■ SPARC M7 시리즈 서버 ■ Exadata Storage Server ■ ZFS Storage Appliance	■ root	welcome1	Oracle ILOM 설명서 모음(http://docs.oracle.com/cd/E24707_01/html/E24528)에서 "Configuration and Maintenance"를 참조하십시오.
SPARC M7 시리즈 서버	■ root ■ oracle ■ grid	welcome1 welcome1 welcome1	연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오. 또한 다음 리소스를 참조하십시오. ■ **Oracle Solaris 11** – 다음 위치에서 Oracle Solaris 11에 대한 보안 설명서를 참조하십시오. http://www.oracle.com/goto/Solaris11/docs ■ **Oracle Solaris 10** – 다음 위치에서 *Oracle Solaris* 관리: 기본 관리를 참조하십시오. http://docs.oracle.com/cd/E26505_01
Exadata Storage Server	■ root ■ celladmin ■ cellmonitor	welcome1 Welcome Welcome	저장소 서버 암호 변경 [86]을 참조하십시오.
Oracle ZFS Storage ZS3-ES	■ root	welcome1	ZFS Storage Appliance root 암호 변경 [76]을 참조하십시오. 또한 다음 위치의 *Oracle ZFS Storage Appliance* 관리 설명서에서 “사용자” 절을 참조하십시오. http://www.oracle.com/goto/ZS3-ES/docs
InfiniBand 스위치	■ root ■ nm2user	welcome1 changeme	root 및 nm2user 암호 변경 [101]을 참조하십시오. 또한 다음 위치에서 *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1*의 “Controlling the Chassis”를 참조하십시오. http://docs.oracle.com/cd/E36265_01
InfiniBand Oracle ILOM	■ ilom-admin ■ ilom-operator	ilom-admin ilom-operator	IB 스위치 암호 변경(Oracle ILOM) [101]을 참조하십시오. 또한 InfiniBand 설명서(http://docs.oracle.com/cd/E36265_01)를 참조하십시오.
이더넷 관리 스위치	■ admin	welcome1	이더넷 스위치 암호 변경 [108]을 참조하십시오.
Oracle I/O 도메인 만들기 도구	■ admin	welcome1	http://www.oracle.com/goto/sc-m7/docs에서 제공되는 *Oracle I/O* 도메인 관리 설명서를 참조하십시오.

구성 요소	사용자 이름	암호	사용자 계정 및 암호 정보
Oracle Engineered Systems Hardware Manager	■ admin ■ service	welcome1 welcome1	자세한 내용은 *Oracle SuperCluster M7* 시리즈 소유자 안내서*:* 관리(http://www.oracle.com/goto/sc-m7/docs)를 참조하십시오.

주 - 이 구성 요소에 대한 root 또는 admin 암호가 변경된 경우에는 Oracle Engineered Systems Hardware Manager에서도 변경되어야 합니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 소유자 안내서*:* 관리를 참조하십시오. 또한 “Oracle Engineered Systems Hardware Manager에서 알려진 암호” [31]를 참조하십시오.

Oracle Engineered Systems Hardware Manager에서 알려진 암호

Oracle Engineered Systems Hardware Manager는 이 표에 있는 구성 요소에 대한 계정 및 암호로 구성되어야 합니다.

주 - Oracle Engineered Systems Hardware Manager는 모든 논리적 도메인 또는 영역에 대한 암호를 확인할 필요가 없습니다.

구성 요소	계정
모든 Oracle ILOM	root
Exadata Storage Server OS	root
ZFS 저장소 컨트롤러 OS	root
IB 스위치	root
이더넷 관리 스위치	admin
PDU	admin

Oracle Engineered Systems Hardware Manager에 대한 자세한 내용은 “Oracle Engineered Systems Hardware Manager” [117] 및 http://www.oracle.com/goto/sc-m7/docs에서 *Oracle SuperCluster M7* 시리즈 관리 설명서를 참조하십시오.

하드웨어 보안

다음 절에서는 하드웨어 보안을 위한 보안 지침에 대해 설명합니다.

액세스 제한

- Oracle SuperCluster M7 시리즈 시스템 및 관련 장비를 잠겨 있고 액세스가 제한된 실내 공간에 설치합니다.
- 랙 내 구성 요소에 대한 서비스가 필요하지 않는 한 랙 도어를 잠가 두십시오. 이렇게 하면 핫 플러그 가능 또는 핫 스왑 가능 장치 및 USB 포트, 네트워크 포트 및 시스템 콘솔에 대한 액세스를 제한할 수 있습니다.
- 예비 FRU(현장 교체 가능 장치) 또는 CRU(자가 교체 가능 장치)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.
- 랙 및 예비 장치 캐비닛의 잠금 상태 및 무결성을 주기적으로 확인하여 변조되거나 실수로 문 잠금이 해제되는 상황을 방지하거나 감지합니다.
- 액세스가 제한된 안전한 위치에 캐비닛 키를 보관합니다.
- USB 콘솔에 대한 액세스를 제한합니다. 시스템 컨트롤러, PDU(전원 분배 장치), 네트워크 스위치 등의 장치가 USB 연결을 제공할 수 있습니다. 물리적 액세스 제한은 네트워크 기반 공격에 노출되지 않으므로 구성 요소에 액세스할 수 있는 보다 안전한 방법입니다.

일련 번호

- SuperCluster M7 시리즈 시스템에 있는 구성 요소의 일련 번호를 기록합니다.

- 교체 부품과 같은 컴퓨터 하드웨어의 모든 중요한 항목에 보안 표시를 합니다. 특수 자외선 펜 또는 돌출된 레이블을 사용합니다.
- 시스템 긴급 상황 시 시스템 관리자가 쉽게 액세스할 수 있는 보안 위치에 하드웨어 활성화 키 및 라이센스를 기록합니다. 인쇄된 문서만 소유권 증명이 될 수 있습니다.
- 시스템에 제공된 모든 정보 안내서를 안전하게 보관합니다.

드라이브

하드 드라이브 및 반도체 드라이브는 중요한 정보를 저장하는 데 사용되는 경우가 많습니다. 이 정보가 무단으로 공개되지 않도록 보호하려면 드라이브를 재사용하거나, 구성 해제하거나, 폐기하기 전에 정리합니다.

- Oracle Solaris `format(1M)` 명령 등 디스크 완전 삭제 도구를 사용하여 드라이브에서 모든 데이터를 완전히 지원됩니다.
- 조직에서는 관련 데이터 보호 정책을 참조하여 가장 적절한 하드 드라이브 정리 방법을 결정해야 합니다.
- 필요한 경우 Oracle의 고객 데이터 및 장치 보존 서비스를 활용합니다. `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf` 문서를 참조하십시오.

주의 - 데이터 액세스 관리 방식으로 인해 디스크 완전 삭제 소프트웨어를 사용하여 최신 드라이브의 일부 데이터를 삭제하지 못할 수도 있습니다.

OBP

기본적으로 SPARC M7 시리즈 OBP는 암호로 보호되지 않습니다. 다음 작업을 수행하여 OBP에 대한 액세스를 제한해서 시스템 보안을 향상시킬 수 있습니다.

- 암호 보호를 구현합니다.
- 실패한 OBP 로그인을 확인합니다.
- OBP 전원 켜기 배너를 제공합니다.

추가 하드웨어 리소스

*SPARC M7 Series Servers Security Guide*에 설명된 모든 보안 원칙은 SuperCluster의 SPARC M7 서버에 적용됩니다. 이 보안 설명서는 `http://www.oracle.com/goto/M7/docs`에서 제공됩니다.

Oracle ILOM 보안

Oracle ILOM은 연산 서버, 저장소 서버, ZFS Storage Appliance 및 IB 스위치를 포함하여 Oracle SuperCluster 구성 요소를 관리 및 모니터하는 데 사용되는 고급 서비스 프로세서 하드웨어 및 소프트웨어를 제공합니다.

Oracle ILOM은 사용자가 OS 상태와 별개로 기본 서버 및 장치를 직접 관리 및 모니터할 수 있게 해주며, 신뢰할 수 있는 정전 관리 기능을 제공합니다.

SuperCluster M7에서 Oracle ILOM 보안을 완전히 설정하려면 모든 Oracle ILOM 지원 구성 요소에 대해 개별적으로 구성 설정을 적용해야 합니다. Oracle ILOM이 포함된 구성 요소는 다음과 같습니다.

- 연산 서버
- 저장소 서버
- ZFS Storage Appliance
- IB 스위치

Oracle ILOM 보안을 위해 다음 작업을 수행합니다.

▼ Oracle ILOM CLI에 로그인

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   이 예에서는 *ILOM_SP_ipaddress*를 액세스하려는 구성 요소에 대한 Oracle ILOM의 IP 주소로 바꿉니다.

- 연산 서버
- 저장소 서버
- ZFS Storage Appliance
- IB 스위치

사용자 구성의 IP 주소는 오라클 담당자가 제공한 배치 요약에 나열됩니다.

```
% ssh root@ILOM_SP__ipaddress
```

2. **Oracle ILOM 루트 암호를 입력합니다.**
   "기본 계정 및 암호(Oracle ILOM)" [38]를 참조하십시오.

Oracle ILOM 버전 확인

최신 기능 및 보안 개선 사항을 활용하기 위해서는 Oracle ILOM 소프트웨어를 지원되는 최신 버전으로 업데이트합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **Oracle ILOM 버전을 표시합니다.**
   이 예에서 Oracle ILOM 소프트웨어 버전은 3.2.4.1.b입니다.

```
-> version
SP firmware 3.2.4.1.b
SP firmware build number: 94529
SP firmware date: Thu Nov 13 16:41:19 PST 2014
SP filesystem version: 0.2.10
```

주 - SuperCluster 구성 요소의 Oracle ILOM 버전을 업데이트하려면 My Oracle Support(https://support.oracle.com)에서 제공되는 최신 SuperCluster 분기별 전체 스택 다운로드 패치를 설치합니다.

주 - SuperCluster와 같은 Oracle Engineered System은 사용할 수 있는 Oracle ILOM 버전 및 이러한 버전의 업데이트 방법에 따라 제한됩니다. 자세한 내용은 오라클 담당자에게 문의하십시오.

(필요한 경우) FIPS-140 호환 작업 사용으로 설정(Oracle ILOM)

미국 연방 정부 고객의 경우 FIPS 140 검증 암호화 사용이 필요합니다.

기본적으로 Oracle ILOM은 FIPS 140 검증 암호화를 사용해서 작동하지 않습니다. 하지만 FIPS 140 검증 암호 사용은 필요에 따라 사용으로 설정할 수 있습니다.

FIPS 140 호환 작업에 맞게 구성된 경우에는 일부 Oracle ILOM 기능을 사용할 수 없습니다. 이러한 기능 목록은 *Oracle ILOM* 보안 설명서의 "FIPS 모드가 사용으로 설정된 경우에 지원되지 않는 기능" 절에 포함되어 있습니다(“추가 Oracle ILOM 리소스” [49] 참조).

또한 “FIPS-140-2 레벨 1 준수” [112]를 참조하십시오.

주의 - 이 작업을 위해서는 Oracle ILOM을 재설정해야 합니다. 재설정하면 모든 사용자 구성 설정이 삭제됩니다. 따라서 Oracle ILOM에서 사이트 특정 항목을 추가로 변경하기 전에 FIPS 140 호환 작업을 사용으로 설정해야 합니다. 사이트 특정 구성이 변경된 시스템에서는 Oracle ILOM 재설정 후 복원할 수 있도록 Oracle ILOM 구성을 백업해야 합니다. 그렇지 않으면 해당 구성 변경사항이 손실됩니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **Oracle ILOM이 FIPS 140 호환 작업에 대해 구성되어 있는지 확인합니다.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

   Oracle ILOM에서 FIPS 140 호환 모드는 `state` 및 `status` 등록 정보로 표시됩니다. `state` 등록 정보는 Oracle ILOM에서 구성된 모드를 나타내고, `status` 등록 정보는 Oracle ILOM의 작동 모드를 나타냅니다. FIPS `state` 등록 정보가 변경된 경우 다음에 Oracle ILOM을 재부트할 때까지 작동 모드 FIPS `status` 등록 정보에 변경사항이 적용되지 않습니다.

3. **FIPS 140 호환 작업을 사용으로 설정합니다.**

```
-> set /SP/services/fips state=enabled
```

4. **Oracle ILOM 서비스 프로세서를 다시 시작합니다.**

   이 변경사항을 적용하려면 Oracle ILOM SP를 다시 시작해야 합니다.

```
-> reset /SP
```

기본 계정 및 암호(Oracle ILOM)

계정	유형	기본 암호	설명
`root`	관리자	`welcome1`	이 구성 요소에 대해 제공 및 사용으로 설정된 기본 계정입니다. 이 계정은 초기 구성을 수행하고 공유되지 않는 추가 관리 계정을 만들 수 있도록 허용하는 데 사용됩니다. 보안을 위해 기본 암호를 변경하십시오.

기본 노출된 네트워크 서비스(Oracle ILOM)

이 표에서는 Oracle ILOM에서 노출되는 기본 네트워크 서비스를 보여줍니다.

이러한 서비스에 대한 자세한 내용은 *Oracle ILOM* 보안 설명서를 참조하십시오("추가 Oracle ILOM 리소스" [49] 참조).

서비스 이름	프로토콜	포트	설명
SSH	TCP	22	CLI를 사용해서 Oracle ILOM에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 보안 셸 서비스에서 사용됩니다.
HTTP (BUI)	TCP	80	브라우저 인터페이스를 사용하여 Oracle ILOM에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTP 서비스에서 사용됩니다. TCP/80은 일반적으로 일반 텍스트 액세스에 사용되지만, 기본적으로 Oracle ILOM은 수신되는 요청을 TCP/443에서 실행되는 서비스의 보안 버전으로 자동으로 재지정합니다.
NTP	UDP	123	로컬 시스템 시계를 하나 이상의 외부 시간 소스와 동기화하기 위해 사용되는 통합된 NTP(Network Time Protocol)(클라이언트 전용) 서비스에서 사용됩니다.
SNMP	UDP	161	Oracle ILOM의 건전성을 모니터하고 수신된 트랩 알림을 모니터할 수 있는 관리 인터페이스를 제공하기 위해 통합된 SNMP 서비스에서 사용됩니다.
HTTPS (BUI)	TCP	443	브라우저 인터페이스를 사용해서 암호화된(SSL/TLS) 채널을 통해 Oracle ILOM에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTPS 서비스에서 사용됩니다.
IPMI	TCP	623	통합된 IPMI(Intelligent Platform Management Interface) 서비스에서 다양한 모니터링 및 관리 기능에 대한 컴퓨터 인터페이스를 제공하기 위해 사용됩니다. 이 서비스는 Oracle Enterprise Manager Ops Center에서 하드웨어 인벤토리 데이터, FRU 설명, 하드웨어 센서 정보 및 하드웨어 구성 요소 상태 정보를 수집하는 데 사용되므로, 사용 안함으로 설정하지 않아야 합니다.
원격 KVMS	TCP	5120 5121 5123 5555 5556	총체적으로, 원격 KVMS 포트는 Oracle Integrated Lights Out Manager에서 사용할 수 있는 원격 키보드, 비디오, 마우스 및 저장소 기능을 제공하는 프로토콜 세트를 제공합니다.

서비스 이름	프로토콜	포트	설명
		7578	
		7579	
ServiceTag	TCP	6481	Oracle ServiceTag 서비스에서 사용됩니다. 서버를 식별하고 서비스 요청을 효율화하는 데 사용되는 Oracle 검색 프로토콜입니다. 이 서비스는 Oracle Enterprise Manager Ops Center와 같은 제품에서 Oracle ILOM 소프트웨어를 검색하고 다른 Oracle 자동 서비스 솔루션과 통합하기 위해 사용됩니다.
WS-Man over HTTPS	TCP	8888	통합 WS-Man 서비스가 HTTPS 프로토콜을 통해 Oracle ILOM을 관리하는 데 사용되는 표준 기반의 웹 서비스 인터페이스를 제공하기 위해 사용됩니다. 이 서비스를 사용 안함으로 설정하면 이 프로토콜을 사용해서 Oracle ILOM을 관리할 수 없습니다. 이 서비스는 Oracle ILOM version 3.2부터 더 이상 포함되지 않습니다.
WS-Man over HTTP	TCP	8889	이 포트는 통합 WS-Man 서비스가 HTTP 프로토콜을 통해 Oracle ILOM을 관리하는 데 사용되는 표준 기반의 웹 서비스 인터페이스를 제공하기 위해 사용됩니다. 이 서비스를 사용 안함으로 설정하면 이 프로토콜을 사용해서 Oracle ILOM을 관리할 수 없습니다. 이 서비스는 Oracle ILOM version 3.2부터 더 이상 포함되지 않습니다.
Single Sign-on	TCP	11626	이 포트는 사용자가 사용자 이름 및 암호를 입력해야 하는 횟수를 줄여주는 통합 Single Sign-On 기능에 사용됩니다. 이 서비스를 사용 안함으로 설정한 경우, 암호를 다시 입력하지 않으면 KVMS가 실행되지 않습니다.

Oracle ILOM 보안 구성 강화

다음 항목에서는 여러 구성 설정을 통해 Oracle ILOM에 대해 보안을 설정하는 방법을 설명합니다.

▼ 불필요한 서비스 사용 안함으로 설정(Oracle ILOM)

플랫폼의 운영 및 관리 요구 사항을 지원하는 데 필요하지 않은 모든 서비스를 사용 안함으로 설정합니다.

기본적으로 Oracle ILOM에는 필수가 아닌 서비스가 이미 사용 안함으로 설정된 네트워크 기본 보안 구성이 적용되어 있습니다. 하지만 사용자의 보안 정책 및 요구 사항에 따라 추가 서비스를 사용 안함으로 설정해야 할 수 있습니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **Oracle ILOM에서 지원되는 서비스 목록을 확인합니다.**

   ```
   -> show /SP/services
   ```

3. **제공된 서비스가 사용으로 설정되었는지 여부를 확인합니다.**

   *servicename*을 2단계에서 식별된 서비스 이름으로 바꿉니다.

   ```
   -> show /SP/services/servicename servicestate
   ```

   대부분의 서비스에서는 `servicestate` 매개변수를 인식하여 서비스의 사용 또는 사용 안함으로 설정 여부를 기록하지만, `servicetag`, `ssh`, `sso` 및 `wsman`과 같은 일부 서비스에서는 `state`라는 매개변수가 사용됩니다. 사용되는 실제 매개변수와 관계없이 다음 예에 표시된 것처럼 `servicestate` 또는 `state` 매개변수가 `enabled` 값을 반환하면 서비스 사용으로 설정된 것입니다.

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **필요하지 않은 서비스를 사용 안함으로 설정하려면 서비스 상태를 `disabled`로 설정합니다.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **이러한 서비스를 사용 안함으로 설정해야 하는지 확인합니다.**

   사용된 도구 및 방법에 따라 이러한 추가 서비스가 필요하지 않거나 사용되지 않는 경우, 사용 안함으로 설정할 수 있습니다.

   - **브라우저 관리 인터페이스(HTTP, HTTPS)에 대해 다음을 입력합니다.**

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **KVMS(키보드, 비디오, 마우스 서비스)에 대해서는 다음을 입력합니다.**

```
-> set /SP/services/kvms servicestate=disabled
```

- **웹 서비스 관리(HTTP/HTTPS를 통한 WS-Man)(Oracle ILOM 버전 3.1 이상)의 경우에는 다음을 입력합니다.**

```
-> set /SP/services/wsman state=disabled
```

- **SSO(Single-Sign On) 서비스의 경우에는 다음을 입력합니다.**

```
-> set /SP/services/sso state=disabled
```

▼ HTTPS에 대한 HTTP 재지정 구성(Oracle ILOM)

기본적으로 Oracle ILOM은 Oracle ILOM과 관리자 사이에 모든 브라우저 기반 통신이 암호화되도록 보장하기 위해 수신되는 HTTP 요청을 HTTPS 서비스로 재지정하도록 구성되어 있습니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.
2. **보안 재지정이 사용으로 설정되었는지 확인합니다.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **기본값이 변경된 경우 보안 재지정을 사용으로 설정할 수 있습니다.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **2단계를 반복하여 설정을 확인합니다.**

승인되지 않은 프로토콜 사용 안함으로 설정

다음 항목에 따라 승인되지 않은 프로토콜을 사용 안함으로 설정합니다.

- HTTPS에 대해 SSLv2 프로토콜 사용 안함으로 설정 [42]
- HTTPS에 대해 SSLv3 프로토콜 사용 안함으로 설정 [42]

▼ HTTPS에 대해 SSLv2 프로토콜 사용 안함으로 설정

기본적으로 SSLv2 프로토콜은 HTTPS 서비스에 대해 사용 안함으로 설정됩니다.

보안을 위해서는 SSLv2를 사용 안함으로 설정하는 것이 매우 중요합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.
2. **HTTP 서비스에 대해 SSLv2 프로토콜이 사용 안함으로 설정되었는지 확인합니다.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **서비스가 사용으로 설정된 경우 SSLv2 프로토콜을 사용 안함으로 설정합니다.**

```
-> set /SP/services/https sslv2=disabled
```

4. **2단계를 반복하여 설정을 확인합니다.**

▼ HTTPS에 대해 SSLv3 프로토콜 사용 안함으로 설정

기본적으로 SSLv3 프로토콜은 HTTPS 서비스에 대해 사용으로 설정됩니다.

보안을 위해 SSLv3 프로토콜을 사용 안함으로 설정합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.
2. **HTTP 서비스에 대해 SSLv3 프로토콜이 사용 안함으로 설정되었는지 확인합니다.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **SSLv3 프로토콜을 사용 안함으로 설정합니다.**

```
-> set /SP/services/https sslv3=disabled
```

4. **2단계를 반복하여 설정을 확인합니다.**

▼ HTTPS에 대해 승인되지 않은 TLS 프로토콜 사용 안함으로 설정

기본적으로 TLSv1.0, TLSv1.1 및 TLSv1.2 프로토콜은 HTTPS 서비스에 대해 사용으로 설정됩니다.

보안 정책과 호환되지 않는 하나 이상의 TLS 프로토콜 버전을 사용 안함으로 설정할 수 있습니다.

보안을 위해서는 TLS 프로토콜의 이전 버전이 필요하지 않은 한 TLSv1.2를 사용하십시오.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **HTTPS 서비스에 대해 사용으로 설정된 TLS 프로토콜 버전 목록을 확인합니다.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **TLSv1.0을 사용 안함으로 설정합니다.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **TLSv1.1을 사용 안함으로 설정합니다.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **2단계를 반복하여 설정을 확인합니다.**

▼ HTTPS에 대해 SSL 약한 암호화 및 중간 강도 암호화 사용 안함으로 설정

기본적으로 Oracle ILOM은 HTTPS 서비스에 대해 약한 암호화 및 중간 강도 암호화 사용을 사용 안함으로 설정합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**
   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **약한 암호화 및 중간 강도 암호화가 사용 안함으로 설정되었는지 확인합니다.**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **기본값이 변경된 경우 약한 암호화 및 중간 강도 암호화 사용을 사용 안함으로 설정할 수 있습니다.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **2단계를 반복하여 설정을 확인합니다.**

▼ 승인되지 않은 SNMP 프로토콜 사용 안함으로 설정 (Oracle ILOM)

기본적으로 Oracle ILOM 모니터 및 관리에 사용되는 SNMP 서비스에 대해 SNMPv3 프로토콜만 사용으로 설정됩니다. 필요한 경우가 아니면 이전 버전의 SNMP 프로토콜이 사용 안함으로 설정되어 있는지 확인합니다.

일부 Oracle 및 타사 제품은 새로운 SNMP 프로토콜 버전에서 지원이 제한적입니다. 해당 구성 요소와 연관된 제품 설명서를 참조하여 특정 SNMP 프로토콜 버전이 지원되는지 확인하십시오. Oracle ILOM이 해당 구성 요소에 필요한 모든 프로토콜 버전을 지원하도록 구성되었는지 확인합니다.

주 - SNMP 프로토콜 버전 3에서는 USM(User-based Security Model)에 대한 지원이 도입되었습니다. 이 기능은 기존 SNMP 커뮤니티 문자열을 특정 권한, 인증 및 개인 정보 보호 프로토콜 및 암호로 구성할 수 있는 실제 사용자 계정으로 바꿉니다. 기본적으로 Oracle ILOM은 USM 계정을 포함하지 않습니다. 사용자의 고유 배치, 관리 및 모니터링 요구 사항을 기준으로 SNMPv3 USM 계정을 구성합니다.

---

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **각 SNMP 프로토콜의 상태를 확인합니다.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **필요한 경우 SNMPv1 및 SNMPv2c를 사용 안함으로 설정합니다.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **2단계를 반복하여 설정을 확인합니다.**

▼ SNMP v1 및 v2c 커뮤니티 문자열 구성(Oracle ILOM)

이 작업은 SNMP v1 또는 SNMPv2c가 사용으로 설정되었고 사용하도록 구성된 경우에만 적용할 수 있습니다.

SNMP가 올바르게 작동하도록 하려면 클라이언트와 서버가 액세스 인증에 사용되는 커뮤니티 문자열에 동의해야 합니다. 따라서 SNMP 커뮤니티 문자열을 변경할 때는 SNMP 프로토콜을 사용하여 Oracle ILOM과 연결을 시도하는 모든 구성 요소와 Oracle ILOM에 모두 새로운 문자열이 구성되어 있는지 확인합니다.

SNMP는 장치의 건전성을 모니터하는 데 사용되는 경우가 많기 때문에 장치에 사용되는 기본 SNMP 커뮤니티 문자열을 고객 정의 값으로 바꾸는 것이 중요합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **새로운 SNMP 커뮤니티 문자열을 만듭니다.**

   이 예에서는 명령줄에서 다음 항목을 바꿉니다.

   - *string* – SNMP 커뮤니티 문자열 조합과 관련하여 미국 국방부 요구 사항과 호환되는 고객 정의 값으로 바꿉니다.
   - *access* – 읽기 전용 또는 읽기-쓰기 액세스 문자열인지 여부에 따라 `ro` 또는 `rw`로 바꿉니다.

```
-> create /SP/services/snmp/communities/string permission=access
```

   새 커뮤니티 문자열을 만든 다음에는 기본 커뮤니티 문자열을 제거해야 합니다.

3. **기본 SNMP 커뮤니티 문자열을 제거합니다.**

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

4. **SNMP 커뮤니티 문자열을 확인합니다.**

```
-> show /SP/services/snmp/communities
```

▼ 기본 자체 서명된 인증서 바꾸기(Oracle ILOM)

Oracle ILOM은 자체 서명된 인증서를 사용해서 SSL 및 TLS 프로토콜을 즉시 사용할 수 있게 해줍니다. 가능한 모든 경우에 자체 서명된 인증서를 사용자 환경에서 사용하도록 승인되었고 인정된 CA(인증 기관)에서 서명된 인증서로 바꾸십시오.

Oracle ILOM은 HTTPS, HTTP, SCP, FTP, TFTP를 포함한 디지털 인증서 및 개인 키를 액세스하는 데 사용할 수 있는 여러 방법을 지원하며, 정보를 웹 브라우저 인터페이스에 직접 붙여 넣습니다. 자세한 내용은 *Oracle ILOM* 구성 및 유지 관리 설명서를 참조하십시오("추가 Oracle ILOM 리소스" [49] 참조).

1. **Oracle ILOM에서 자체 서명된 기본 인증서를 사용 중인지 확인합니다.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **조직의 인증서를 설치합니다.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

▼ 관리 브라우저 인터페이스 비활성 시간 초과 구성

Oracle ILOM은 미리 정의된 시간(분) 동안 비활성 상태로 유지된 관리 세션을 연결 해제하고 로그아웃할 수 있는 기능을 지원합니다. 기본적으로 브라우저 인터페이스 세션은 15분 후 시간 초과됩니다.

HTTPS 및 HTTP 서비스와 연관된 세션 시간 초과 매개변수는 개별적으로 설정 및 관리됩니다. 각 서비스와 연관된 `sessiontimeout` 매개변수를 설정해야 합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **HTTPS 서비스와 연관된 비활성 시간 초과 매개변수를 확인합니다.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **비활성 시간 초과 매개변수를 설정합니다.**

*n*을 분 단위로 지정된 값으로 바꿉니다.

```
-> set /SP/services/https sessiontimeout=n
```

4. **HTTP 서비스와 연관된 비활성 시간 초과 매개변수를 확인합니다.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **비활성 시간 초과 매개변수를 설정합니다.**

   *n*을 분 단위로 지정된 값으로 바꿉니다.

```
-> set /SP/services/http sessiontimeout=n
```

6. **2단계 및 4단계를 반복하여 설정을 확인합니다.**

▼ 관리 인터페이스 시간 초과 구성(Oracle ILOM CLI)

Oracle ILOM은 미리 정의된 시간(분) 동안 비활성 상태로 유지된 관리 CLI 세션을 연결 해제하고 로그아웃할 수 있는 기능을 지원합니다.

기본적으로 SSH CLI는 지정된 시간 초과 값이 없으며, 따라서 이 서비스에 액세스하는 관리 사용자가 무제한 로그인된 상태로 유지됩니다.

보안을 위해서는 브라우저 사용자 인터페이스와 연관된 값과 일치하도록 이 매개변수를 설정합니다. 이 값은 15분 또는 다른 값일 수 있습니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **CLI와 연관된 비활성 시간 초과 매개변수를 확인합니다.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **비활성 시간 초과 매개변수를 설정합니다.**

   *n*을 분 단위로 지정된 값으로 바꿉니다.

```
-> set /SP/cli timeout=n
```

4. **2단계를 반복하여 설정을 확인합니다.**

▼ 로그인 경고 배너 구성(Oracle ILOM)

Oracle ILOM은 관리자가 장치에 연결되기 전 및 후에 고객 특정 메시지를 표시할 수 있는 기능을 지원합니다.

Oracle ILOM 연결 메시지는 인증 전에 표시되며, 로그인 메시지는 인증 후에 표시됩니다.

선택적으로 Oracle ILOM 기능에 대한 액세스 권한을 부여 받기 전에 로그인 메시지를 수락하도록 Oracle ILOM을 구성할 수 있습니다. 연결 및 로그인 메시지와 선택적인 수락 요구 사항은 브라우저 및 명령줄 액세스 인터페이스 모두에서 구현됩니다.

Oracle ILOM은 최대 1,000자까지 연결 및 로그인 메시지를 지원합니다.

1. **관리 네트워크에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM CLI에 로그인 [35]을 참조하십시오.

2. **연결 및 로그인 메시지가 구성되었는지 여부를 확인합니다.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **연결 또는 로그인 메시지를 설정합니다.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **로그인 메시지 수락이 사용으로 설정되었는지 여부를 확인합니다.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(선택사항) 로그인 메시지 수락을 강제 적용합니다.**

주의 - 로그인 메시지 수락을 요구하면 수락 요청에 응답할 수 없거나 응답하도록 구성되어 있지 않을 수 있기 때문에 SSH를 사용하는 자동 관리 프로세스의 올바른 작동이 방해될 수 있습니다. 따라서, 메시지 수락 요구 사항이 충족될 때까지 Oracle ILOM은 CLI 사용을 허용하지 않기 때문에 이러한 연결이 중단 또는 시간 초과될 수 있습니다.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **2단계 및 4단계를 반복하여 설정을 확인합니다.**

추가 Oracle ILOM 리소스

Oracle ILOM 관리 및 보안 절차에 대한 자세한 내용은 SuperCluster M7에서 실행되는 버전에 해당하는 Oracle ILOM 설명서 라이브러리를 참조하십시오.

- *Oracle ILOM* 보안 설명서 펌웨어 릴리스 *3.0, 3.1* 및 *3.2*:

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager 버전 3.2.*x*:

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager 버전 3.1.*x*:

  http://docs.oracle.com/cd/E24707_01
- Oracle Integrated Lights Out Manager 버전 3.0.*x*:

  http://docs.oracle.com/cd/E19860-01

연산 서버 보안

1개 또는 2개의 SPARC M7 서버(연산 서버)가 SuperCluster M7에 설치됩니다. 각 연산 서버는 하드웨어 분할 영역 2개(PDomain 2개)로 분리됩니다. 각 PDomian에는 섀시에서 사용할 수 있는 프로세서, 메모리 및 PCIe 확장 슬롯의 절반이 포함됩니다. 두 PDomain은 모두 동일한 섀시 내에서 개별 서버로 작동합니다. SPM(서비스 프로세서 모듈)의 중복 쌍이 각 분할 영역을 관리합니다.

각 PDomain은 보안을 설정해야 합니다.

이 절에서는 연산 서버에 대한 보안 제어 세트를 제공합니다.

▼ 연산 서버에 로그인 및 기본 암호 변경

Oracle ILOM을 통해 단일 PDomain에 액세스하려면 해당 PDomain을 제어하는 활성 SPM에 로그인해야 합니다. 다른 분할 영역이 정상적으로 작동하는 동안 하나의 분할 영역에 대해 전원 켜기, 재부트 또는 관리 작업을 수행할 수 있습니다.

다양한 방법으로 SuperCluster 연산 서버에 로그인할 수 있습니다. 이 작업에 설명된 방법에는 연산 서버의 SPM에서 Oracle ILOM CLI에 로그인이 포함됩니다. 이 방법을 통해 다음 상태의 서버에 액세스할 수 있습니다.

- 대기 전원 모드
- 시스템 전원이 켜져 있지만 호스트는 실행 중이 아님
- OS가 부트 중인 상태
- 완전히 전원이 켜져 있고 OS가 실행 중인 상태

1. **관리 네트워크에서 `ssh` 명령을 사용하여 로그인합니다.**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **프롬프트가 표시되면 암호를 입력합니다.**
   출하 시 기본 `root` 암호는 `welcome1`입니다.
   암호를 변경하라는 프롬프트가 표시되면 그렇게 합니다.
   이 시점에서는 연산 서버의 Oracle ILOM에서 수행되는 모든 보안 작업을 실행할 수 있습니다.

3. **연산 서버의 호스트 콘솔에 액세스하려면 호스트 콘솔을 시작합니다.**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

주 - 호스트가 실행 중이 아닌 경우 PDomain 프롬프트가 표시되지 않습니다.

주 - Oracle ILOM 프롬프트로 다시 전환하려면 제어 문자(기본 문자: `#.`)를 입력합니다.

4. **필요에 따라 수퍼 유저 역할로 전환합니다.**
   `su` 명령을 사용하여 `root` 역할로 구성된 사용자로 전환합니다.

기본 계정 및 암호(연산 서버)

계정	기본 암호	설명
`root`	`welcome1`	Oracle ILOM에서는 첫번째 로그인 성공 이후 즉시 기본 암호를 변경해야 합니다.
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ SuperCluster 소프트웨어 버전 확인

1. **연산 서버 중 하나에 로그인하고 호스트 콘솔에 액세스합니다.**

연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **다음 명령을 입력합니다.**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

출력에서 ssc에 연결된 번호가 소프트웨어 버전을 나타냅니다.
SuperCluster 소프트웨어 버전을 업데이트하려면 My Oracle Support(https://support.oracle.com)에서 제공되는 최신 SuperCluster 분기별 전체 스택 다운로드 패치를 설치합니다.

주 - SuperCluster의 경우 추가 제한 사항으로 인해 사용할 수 있는 소프트웨어 버전 및 해당 버전의 업데이트 방법이 제한될 수 있습니다. 이러한 경우에는 오라클 담당자에게 문의하십시오.

▼ 보안 셸 서비스 구성

이 작업을 수행하면 Oracle SuperCluster에 배치된 보안 셸 보안 구성이 향상됩니다.

/etc/ssh/sshd_config 파일은 보안 셸 서비스에 대한 매개변수를 구성하는 시스템 전체 구성 파일입니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **/etc/ssh/sshd_config 파일을 편집합니다.**

3. **SuperCluster 클라이언트 액세스 네트워크에서 시작되는 연결만 허용되도록 ListenAddress 매개변수를 구성합니다.**
ListenAddress IP 주소가 클라이언트 네트워크로 설정되었는지 확인합니다.
이렇게 하면 관리 또는 IB 네트워크를 통한 구성 요소 사이에 보안 셸 연결이 성공적으로 시작될 수 없게 됩니다.

4. **다른 sshd_config 매개변수를 검토하고 사이트 요구 사항에 따라 설정합니다.**
다음과 같은 설정은 보안 셸 서비스에 보안을 설정합니다.

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
```

```
ClientAliveCountMax 0
```

5. **sshd_config 파일을 저장합니다.**

6. **서비스를 다시 시작합니다.**
   변경사항을 적용하려면 서비스를 다시 시작해야 합니다.

```
# svcadm restart ssh
```

▼ root가 역할인지 확인

기본적으로 Oracle Solaris는 root가 사용자 계정이 아닌 역할이 되도록 구성되어 있습니다. 또한 SuperCluster 구성에서는 익명 root 사용자 로그인이 허용되지 않습니다. 대신, 모든 사용자는 루트 역할을 맡기 전에 일반 사용자로 로그인해야 합니다. 모든 SuperCluster 관리 작업은 root를 역할로 사용하여 수행해야 합니다.

1. **연산 서버 중 하나에 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **root 속성이 type=role로 설정되었는지 확인합니다.**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(선택사항) 모든 일반 사용자에게 root 역할을 지정합니다.**

```
# usermod -R root user_name
```

기본 노출된 네트워크 서비스(연산 서버)

이 표에서는 연산 서버에서 노출되는 기본 네트워크 서비스를 보여줍니다.

서비스 이름	프로토콜	포트	설명
SSH	TCP	22	CLI를 사용하여 연산 서버에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 보안 셸 서비스에서 사용됩니다.
HTTP (BUI)	TCP	80	브라우저 인터페이스를 사용하여 연산 서버에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTP 서비스에서 사용됩니다.
HTTPS (BUI)	TCP	443	브라우저 인터페이스를 사용하여 암호화된(SSL/TLS) 채널을 통해 연산 서버에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTPS 서비스에서 사용됩니다.
SNMP	UDP	161	연산 서버의 건전성을 모니터하고 수신된 트랩 알림을 모니터할 수 있는 관리 인터페이스를 제공하기 위해 통합된 SNMP 서비스에서 사용됩니다.

연산 서버 보안 구성 강화

다음 항목에서는 연산 서버를 보안 방식으로 구성하는 방법에 대해 설명합니다.

▼ `intrd` 서비스 사용으로 설정

인터럽트 밸런서(`intrd`) 서비스는 최적의 성능 보장을 위해 인터럽트와 CPU 사이의 지정을 모니터합니다. 자세한 내용은 `intrd(1M)` 매뉴얼 페이지를 참조하십시오.

이 서비스는 전역 영역에서만 실행됩니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **서비스를 시작합니다.**

```
# svcadm enable intrd
```

▼ 불필요한 서비스 사용 안함으로 설정(연산 서버)

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **시스템이 NFS 클라이언트 또는 서버가 아닌 경우 NFS 상태 모니터를 사용 안함으로 설정합니다.**
   이 서비스는 `lockd(1M)`와 상호 작용해서 NFS에 대한 잠금 서비스를 위한 충돌 및 복구 기능을 제공합니다.

```
# svcadm disable svc:/network/nfs/status
```

3. **NFS 또는 NFSv4를 모두 사용 중이 아닌 경우 NFS 잠금 관리자 서비스를 사용 안함으로 설정합니다.**
   NFS 잠금 관리자는 NFSv2 및 NFSv3에서 NFS 파일에 대한 레코드 잠금 작업을 지원합니다.

```
# svcadm disable svc:/network/nfs/nlockmgr
```

4. **시스템이 파일을 마운트 중이 아닌 경우 NFS 클라이언트 서비스를 사용 안함으로 설정하거나 해당 패키지를 설치 제거할 수 있습니다.**
   NFS 클라이언트 서비스는 시스템이 NFS 서버에서 파일을 마운트 중인 경우에만 필요합니다. 자세한 내용은 `mount_nfs(1M)` 매뉴얼 페이지를 참조하십시오.

```
# svcadm disable svc:/network/nfs/client
```

5. **NFS 파일 서버가 아닌 시스템에서 NFS 서버 서비스를 사용 안함으로 설정합니다.**
   NFS 서버 서비스는 NFS 버전 2, 3 및 4를 통해 클라이언트 파일 시스템 요청을 처리합니다. 이 시스템이 NFS 서버가 아니면 서비스를 사용 안함으로 설정합니다.

```
# svcadm disable svc:/network/nfs/server
```

6. **DNS SRV 레코드에 대한 FedFS 또는 LDAP 기반 참조를 사용 중이 아니면 서비스를 사용 안함으로 설정합니다.**
   FedFS(통합 파일 시스템) 클라이언트 서비스는 FedFS 정보를 저장하는 LDAP 서버에 대한 기본값 및 연결 정보를 관리합니다.

```
# svcadm disable svc:/network/nfs/fedfs-client
```

7. **`rquota` 서비스를 사용 안함으로 설정합니다.**

   `remote` 할당량 서버는 NFS를 통해 마운트되는 로컬 파일 시스템에 대한 할당량을 반환합니다. 그 결과는 `quota(1M)`에서 원격 파일 시스템에 대한 사용자 할당량을 표시하는 데 사용됩니다. `rquotad(1M)` 데몬은 일반적으로 `inetd(1M)`에 의해 호출됩니다. 이 데몬은 잠재적으로 악의적인 사용자에게 네트워크에 대한 정보를 제공합니다.

   ```
   # svcadm disable svc:/network/nfs/rquota
   ```

8. **`cbd` 서비스를 사용 안함으로 설정합니다.**

   `cbd` 서비스는 NFS 버전 4 프로토콜에 대한 통신 끝점을 관리합니다. `nfs4cbd(1M)` 데몬은 NFS 버전 4 클라이언트에서 실행되며 콜백에 대한 리스너 포트를 만듭니다.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **NFSv4를 사용 중이 아니면 `mapid` 서비스를 사용 안함으로 설정합니다.**

   NFS 사용자 및 그룹 ID 매핑 데몬 서비스는 NFS 버전 4 `owner` 및 `owner_group` 식별 속성과 NFS 버전 4 클라이언트 및 서버 모두에 사용되는 로컬 UID와 GID 번호에 대해 매핑됩니다.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **`ftp` 서비스를 사용 안함으로 설정합니다.**

    FTP 서비스는 암호화되지 않은 파일 전송 서비스를 제공하며 일반 텍스트 인증을 사용합니다. 암호화된 인증 및 파일 전송을 제공할 수 있도록 `ftp` 대신 보안 복사 프로그램인 `scp(1)` 프로그램을 사용하십시오.

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **원격 볼륨 관리자 서비스를 사용 안함으로 설정합니다.**

    이 이동식 볼륨 관리자는 이동식 매체 및 핫 플러그 가능 저장소를 자동으로 마운트 및 마운트 해제할 수 있는 HAL 인식 볼륨 관리자입니다. 사용자가 악의적인 프로그램을 가져오거나 시스템 외부로 중요한 데이터를 전송할 수 있습니다. 자세한 내용은 `rmvolmgr(1M)` 매뉴얼 페이지를 참조하십시오.

    이 서비스는 전역 영역에서만 실행됩니다.

    ```
    # svcadm disable svc:/system/filesystem/rmvolmgr
    ```

12. **`smserver` 서비스를 사용 안함으로 설정합니다.**

    `smserver` 서비스는 이동식 매체 장치에 액세스하는 데 사용됩니다.

    ```
    # svcadm disable rpc/smserver:default
    ```

13. **/etc/pam.d 디렉토리에서 r-protocol 서비스에 대한 인증 스택을 위한 모듈로 pam_deny.so.1을 지정합니다.**

    기본적으로 r-protocols, rlogin(1) 및 rsh(1)와 같은 레거시 서비스는 설치되지 않습니다. 하지만 이러한 서비스는 /etc/pam.d에 정의되어 있습니다. /etc/pam.d에서 서비스 정의를 제거하면 레거시 서비스가 사용으로 설정된 이벤트의 다른 서비스(예: SSH)가 사용됩니다.

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. **/etc/default/keyserv 파일을 편집해서 ENABLE_NOBODY_KEYS의 값을 NO로 변경합니다.**

    keyserv 서비스는 nobody 사용자 키를 사용할 수 없습니다. ENABLE_NOBODY_KEYS의 값은 기본적으로 YES입니다.

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. **ftpusers 파일에 사용자를 추가해서 ftp 액세스를 제한합니다.**

    FTP 파일 전송은 모든 사용자에게 제공되지 않아야 하며, 적격한 사용자가 자신의 이름 및 암호를 제공하도록 해야 합니다. 일반적으로 시스템 사용자는 FTP를 사용하도록 허용되지 않아야 합니다. 이 검사는 시스템 계정이 /etc/ftpd/ftpusers 파일에 포함되었는지 확인하여 이러한 계정이 FTP를 사용할 수 없도록 합니다.

    /etc/ftpd/ftpusers 파일은 사용자가 FTP 서비스를 사용하지 못하도록 금지하기 위해 사용됩니다. 최소한 root, bin, adm 등과 같은 모든 시스템 사용자를 포함해야 합니다.

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. **FTP 서버에서 생성되는 파일에 대해 강력한 기본 파일 생성 마스크를 설정합니다.**

    FTP 서버가 반드시 사용자의 시스템 파일 생성 마스크를 사용해야 하는 것은 아닙니다. FTP umask를 설정하면 FTP를 통해 전송되는 파일에 강력한 파일 생성 마스크가 사용되도록 할 수 있습니다.

```
# pfedit /etc/proftpd.conf
Umask          027
```

17. **네트워크 토폴로지 질의에 대한 응답을 사용 안함으로 설정합니다.**

에코 요청에 대한 응답을 사용 안함으로 설정하는 것이 중요합니다. ICMP 요청은 `ipadm` 명령을 사용해서 관리됩니다.

이러한 설정은 네트워크 토폴로지에 대한 정보 배포를 방지합니다.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

18. **ICMP 재지정 메시지를 사용 안함으로 설정합니다.**

    라우터는 ICMP 재지정 메시지를 사용하여 대상에 더 직접적인 경로를 호스트에 알립니다. 불법적인 ICMP 재지정 메시지는 중간 전달자의 공격을 초래할 수 있습니다.

    ```
    # ipadm set-prop -p _ignore_redirect=1 ipv4
    ```

19. **`mesg(1)`를 사용 안함으로 설정해서 원격 터미널에 대한 `talk(1)` 및 `write(1)` 액세스를 방지합니다.**

    ```
    # mesg -n
    ```

20. **(선택사항) 네트워크에서 수신 중인 불필요한 서비스를 검토하고 사용 안함으로 설정합니다.**

    기본적으로 `ssh(1)`는 네트워크 패킷을 전송 및 수신할 수 있는 유일한 네트워크 서비스입니다.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

▼ 엄격한 다중 홈 지정 사용으로 설정

방화벽 또는 VPN 노드와 같이 다른 도메인에 대한 게이트웨이인 시스템의 경우, 엄격한 다중 홈 지정을 사용으로 설정해야 합니다. `hostmodel` 등록 정보는 다중 홈 지정 시스템에 대한 IP 패킷의 전송 및 수신 동작을 제어합니다. 패킷이 다른 인스턴스에서 허용되지 않도록 `1`에 대해 엄격한 다중 홈 지정을 설정합니다. 기본값은 `0`입니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`1`에 대해 엄격한 다중 홈 지정을 설정합니다.**

   ```
   # ipadm set-prop -p _strict_dst_multihoming=1 ipv4
   ```

▼ ASLR 사용으로 설정

주 - 데이터베이스 도메인 또는 데이터베이스 영역에서 ASLR을 사용으로 설정하지 마십시오.

Oracle Solaris는 ASLR(주소 공간 레이아웃 모든 지정)을 사용으로 설정하기 위해 사용자 바이너리를 여러 개 태그 지정합니다. ASLR은 주소 공간의 키 부분에 대한 시작 주소를 임의 지정합니다. 이 보안 방어 방식은 소프트웨어 취약점을 악용하려는 ROP(Return Oriented Programming) 공격을 무효화할 수 있습니다. 영역은 해당 프로세스의 모든 지정된 레이아웃을 상속합니다. ASLR 사용이 모든 바이너리에 대해 최적이 아닐 수 있으므로 ASLR은 영역 또는 바이너리 레벨에서 구성할 수 있습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **ASLR을 사용으로 설정합니다.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

▼ TCP 연결 구성

포트별 IP 주소에 대해 최대 half-open TCP 연결을 4096으로 설정하면 SYN 플러드 서비스 거부 공격을 방어하는 데 도움이 됩니다. 대기열에 있는 수신 중인 연결 TCP의 최대 개수를 최소 1024로 설정하면 특정 DDoS(분산 서비스 거부) 공격을 방지하는 데 도움이 됩니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **최대 half-open 및 대기열에 있는 수신 중인 TCP 연결을 설정합니다.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

▼ PCI 준수를 위한 암호 기록 로그 및 암호 정책 설정

`/etc/default/passwd` 파일의 `HISTORY` 매개변수는 사용자가 `HISTORY` 값을 사용해서 비슷한 암호를 사용하지 못하도록 방지합니다.

`MINWEEKS`가 `3`으로 설정되어 있고 `HISTORY`가 `10`으로 설정된 경우 암호를 10개월 동안 재사용할 수 없습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`/etc/default/passwd` 파일을 편집하고 암호 매개변수를 설정합니다.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **`/etc/default/login` 파일을 편집해서 매개변수를 포함시킵니다.**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

▼ 사용자 홈 디렉토리에 적절한 권한이 있는지 확인

홈 디렉토리는 소유자가 쓰기 및 검색을 수행할 수 있어야 합니다. 일반적으로 다른 사용자는 해당 파일을 수정하거나 사용자의 홈 디렉토리에 파일을 추가할 수 있는 권한이 없습니다. 이렇게 할 수 있도록 사용자의 디렉토리에 대해 권한을 설정합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **사용자의 디렉토리에 대해 권한을 설정합니다.**

```
# chmod 750 /export/home/user_home_directory
```

▼ IP 필터 방화벽 사용으로 설정

IP 필터는 Stateful 패킷 필터링 및 NAT(Network Address Translation)를 제공하는 호스트 기반 방화벽입니다. 패킷 필터링은 네트워크 기반 공격에 대비한 기본적인 보호를 제공합니다. IP 필터는 Stateless 패킷 필터링도 포함하며, 주소 풀 생성 및 관리를 수행할 수 있습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **IP 필터 방화벽을 사용으로 설정합니다.**

```
# svcadm svc:/network/ipfilter:default
```

▼ 이름 서비스에 로컬 파일만 사용되는지 확인

OS는 호스트, `ipnodes`, 사용자(`passwd(4)`, `shadow(4)`, `user_attr(4)`) 및 `groups`에 대한 많은 정보의 데이터베이스를 사용합니다. 이러한 항목의 데이터는 여러 소스로부터 비롯됩니다. 예를 들어, 호스트 이름 및 호스트 주소는 `/etc/hosts`, NIS, LDAP, DNS 또는 멀티캐스트 DNS에서 찾을 수 있습니다. 제한된 환경의 시스템은 이러한 항목에 대해 로컬 파일 항목만 사용할 경우 보다 안전합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **로컬 파일만 사용하도록 이름 서비스를 구성합니다.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

▼ Sendmail 및 NTP 서비스 사용으로 설정

sendmail 서비스가 실행 중이어야 합니다. 그렇지 않으면 `root`에 대한 중요한 시스템 메일이 전달되지 않습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **sendmail을 사용으로 설정합니다.**

```
# svcadm enable smtp:sendmail
```

3. **필요한 경우 NTP 서비스를 설치합니다.**

   `ntp` 서비스는 보안 및 준수가 필요한 모든 시스템에 설치되어 있어야 합니다.

```
# pkg install service/network/ntp
```

4. **NTP 서비스를 클라이언트로 구성하고 서비스를 사용으로 설정합니다.**

   Network Time Protocol 데몬은 사용으로 설정되고 클라이언트로 올바르게 구성되어 있어야 합니다. `/etc/inet/ntp.conf` 파일은 서버 정의를 하나 이상 포함해야 합니다. 이 파일은 또한 클라이언트가 서버로 작동하는 것을 방지하기 위해 `restrict default ignore` 라인을 포함해야 합니다.

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

▼ GSS 사용 안함으로 설정(Kerberos를 사용하지 않는 경우)

일반 보안 서비스(`gss`)는 GSS-API(일반 보안 서비스 응용 프로그램 인터페이스) 보안 토큰의 생성 및 검증을 관리합니다. `gssd(1M)` 데몬은 커널 `rpc` 및 GSS-API 사이에서 작동합니다.

주 - Kerberos에서 이 서비스가 사용됩니다. Kerberos가 구성되지 않았고 사용 중이 아닌 경우 `rpc/gss` 서비스를 사용 안함으로 설정합니다.

---

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`rpc/gss`를 사용으로 설정합니다.**

```
# svcadm enable rpc/gss
```

3. **`/tmpfs`에 대한 크기 제한을 설정합니다.**

   `tmpfs` 파일 시스템의 크기는 기본적으로 제한되지 않습니다. 성능 영향을 방지하기 위해서는 각 `tmpfs` 마운트의 크기를 제한할 수 있습니다. 자세한 내용은 `mount_tmpfs(1M)` 및 `vfstab(4)` 매뉴얼 페이지를 참조하십시오.

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **연산 서버를 재부트합니다.**

```
# reboot
```

▼ 전체 쓰기 가능 파일에 대한 고정된 비트 설정

디렉토리의 고정된 비트는 전체 쓰기 가능 디렉토리의 파일이 파일 소유자 또는 `root` 역할을 제외하고 다른 사람에 의해 삭제 또는 이동되지 않도록 방지합니다. 이 기능은 `/tmp` 디렉토리와 같이 많은 사용자에게 일반적으로 사용되는 디렉토리에서 유용합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`/tmp` 및 다른 전체 쓰기 가능 파일에서 고정된 비트를 설정합니다.**

```
# chmod 1777 /tmp
```

▼ 코어 덤프 보호

코어 덤프는 중요한 데이터를 포함할 수 있습니다. 보호에는 파일 권한 및 코어 덤프 이벤트 로깅이 포함될 수 있습니다. `coreadm(1m)` 및 `chmod(1M)` 매뉴얼 페이지를 참조하십시오.

`coreadm` 명령을 사용해서 현재 구성을 보고 설정합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **현재 구성을 확인합니다.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **코어 파일을 구성하고 코어 덤프 디렉토리를 보호합니다.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
```

```
-d process -d proc-setid
```

4. **권한을 확인합니다.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **디렉토리에서 권한을 올바르게 설정합니다.**

```
# chmod 700 /var/share/cores
```

▼ 실행할 수 없는 스택 강제 적용

실행할 수 없는 스택 사용으로 설정은 특정 종류의 버퍼 오버플로우 스택을 방해하기 위한 매우 유용한 기법입니다. Oracle Solaris `nxstack`이 사용으로 설정된 경우 프로세스 스택 메모리 세그먼트는 실행할 수 없는 것으로 표시됩니다. 이 확장은 악의적인 코드 삽입 및 스택 실행을 사용하는 공격을 방어합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`nxstack`을 사용으로 설정합니다.**

```
# sxadm set model=all nxstack
```

3. **구성을 확인합니다.**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

▼ 암호화된 스왑 공간 사용으로 설정

ZFS 볼륨 또는 원시 장치에 관계없이 스왑 공간을 암호화합니다. 암호화는 시스템이 이러한 페이지를 디스크로 스왑해야 할 경우 사용자 암호와 같은 중요한 데이터가 보호되도록 보장합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`/etc/vfstab` 파일을 편집하고 `swap`을 `encrypted`로 설정합니다.**

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **PKCS #11 키 저장소를 만들고 초기화합니다.**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **대칭 키를 생성하고 PKCS #11 키 저장소에 저장합니다.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

▼ 감사 사용으로 설정

감사 로그가 명령 및 인수를 포함해서 모든 관리 작업을 캡처하는지 확인합니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **감사 기능을 구성합니다.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

▼ 전역 영역에서 데이터 링크(스푸핑) 보호 사용으로 설정

Oracle Solaris 데이터 링크 보호는 네트워크에 대한 악의적인 Guest VM에 의해 발생할 수 있는 손상을 방지합니다.

스누핑 증명 구성을 사용으로 설정하면 가상 환경의 네트워크 트래픽이 호스트 시스템에서 수신 또는 전송되는 더 넓은 트래픽에서 격리되도록 설정함으로써 네트워크 성능이 향상됩니다. 링크 보호는 네트워크에 대한 악의적인 Guest VM에 의해 발생할 수 있는 손상을 방지합니다. 이 기능은 다음의 기본적인 위협에 대한 보호를 제공합니다.

- IP 및 MAC 스푸핑

- BPDU(Bridge Protocol Data Unit) 공격과 같은 L2 프레임 스푸핑

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **링크 보호를 설정합니다.**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **구성을 확인합니다.**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **링크에서 허용되는 IP를 설정합니다.**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

▼ 비전역 영역에서 데이터 링크(스푸핑) 보호 사용으로 설정

Oracle Solaris 데이터 링크 보호는 SuperCluster 환경 내에 배치된 모든 Oracle Solaris 비전역 영역에 개별적으로 적용할 수도 있습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`zonecfg(1M)` 명령을 사용해서 특정 네트워크 인터페이스에서 데이터 링크 보호를 강제 적용합니다.**
   허용되는 IP 주소 목록이 정확하고 완전한지 확인합니다. 목록에는 Oracle Solaris IPMP, Oracle Real Application Clusters 등에서 사용되는 모든 가상 IP 주소를 포함해야 합니다. 또한 SuperCluster 비전역 영역 구성에 대한 변경사항은 비전역 영역이 다시 시작될 때까지 적용되지 않습니다.

```
# zonecfg -z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

▼ 암호화된 ZFS 데이터 세트 만들기

보관 중인 데이터 보호가 필요한 조직은 암호화된 ZFS 데이터 세트를 사용해서 영역 배치 응용 프로그램 및 정보를 추가로 보호하도록 선택할 수 있습니다. 관리자 개입 없이 각 비전역 영역이 시작될 수 있도록 보장하기 위해 암호화된 ZFS 데이터 세트는 개별 데이터베이스 또는 응용 프로그램 도메인 내에 로컬로 저장된 ZFS 암호화 키에 액세스하도록 구성됩니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**
연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **ZFS 암호화 키를 만듭니다.**
필요한 키를 만드는 간단한 방법은 다음과 비슷한 명령을 사용하는 것입니다.

```
# zfs create zfs_pool_name/zfskeystore
$ chown root:root /zfs_pool_name/zfskeystore
$ chmod 700 /zfs_pool_name/zfskeystore
$ pktool genkey keystore=file keytype=aes keylen=256 \
outkey=/zfs_pool_name/zfskeystore/zone_name.key
```

3. **암호화된 ZFS 데이터 세트를 만듭니다.**

```
# zfs create -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zone_name.key \
zfs_pool_name/zone_name
```

4. **u01 및 공통 데이터 세트를 암호화합니다.**
이러한 동일한 접근 방법을 사용해서 사이트별 요구 사항 및 정책에 따라 데이터 세트별로 동일한(SuperCluster 특정) 키 또는 고유한 키를 사용해서 u01 및 공통 데이터 세트를 암호화할 수 있습니다. 이 예에서 공통 데이터 세트는 3단계에서 생성된 것과 동일한 키를 사용해서 생성됩니다. 이러한 추가 데이터 세트를 만드는 동안에는 압축과 같은 추가 ZFS 구성 매개변수도 정의할 수 있습니다.

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ (선택사항) 키 저장소 액세스를 위한 문장암호 설정

이전 작업인 암호화된 ZFS 데이터 세트 만들기 [68]에서는 파일 시스템에 직접 저장해야 하는 로컬로 정의된(원시) 키 파일을 사용합니다. 또 다른 키 저장소 기법에서는 *Sun Software PKCS#11 Softtoken*이라는 문장암호로 보호되는 PKCS#11 키 저장소를 사용합니다. 이 방법을 사용하려면 다음 작업을 수행합니다.

ZFS에 키를 제공하려면 먼저 PKCS#11 키 저장소가 수동으로 잠금 해제되어 있어야 합니다. 결국, 암호화된 ZFS 데이터 세트를 마운트하기 위해(그리고 영역에서도 암호화된 ZFS 데이터

세트를 사용할 경우 비전역 영역을 시작하기 위해)서는 수동 관리 개입이 필요함을 의미합니다. 다른 키 저장소 전략에 대한 자세한 내용은 `zfs_encrypt(1M)` 매뉴얼 페이지를 참조하십시오.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **키 저장소에 액세스하기 위해 필요한 PIN(문장암호)을 설정합니다.**

   새로운 PKCS#11 키 저장소와 연관된 기본 PIN은 `changeme`입니다. 이 예의 첫번째 프롬프트에서 이 문장암호를 사용합니다.

```
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

3. **키를 다른 위치에 저장하기 위해 `${SOFTTOKEN}` 환경 변수를 정의합니다.**

   PKCS#11 Softtoken에서 사용되는 키 자료는 기본적으로 `/var/user/ ${USERNAME}/pkcs11_softtoken` 디렉토리에 저장됩니다. 키 자료를 다른 위치에 저장하기 위해서는 `${SOFTTOKEN}` 환경 변수를 정의할 수 있습니다. 이 기능을 사용하면 이 문장암호로 보호되는 키 자료에 대해 SuperCluster 특정 저장소를 사용으로 설정할 수 있습니다.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **키를 만듭니다.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **이전 단계에서 만든 키를 참조하는 암호화된 ZFS 데이터 세트를 만듭니다.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

▼ 변경할 수 없는 전역 영역 만들기

변경 불가 기능을 사용한 손상 방지를 통해 전역 영역 및 비전역 영역은 SuperCluster 연산 서버가 고유 서비스를 작동하는 탄력적이고 무결성이 뛰어난 작동 환경을 만들 수 있습니다. Oracle Solaris 전역 및 비전역 영역의 기본 보안 기능을 기반으로 작성되는 변경할 수 없는 영역은 (관리자의 개입 없이) (일부 또는 모든) OS 디렉토리 및 파일을 변경할 수 없도록 보장합

니다. 이렇게 읽기 전용 방식을 강제로 적용하면 허용되지 않은 변경을 방지하고, 보다 강력한 변경 관리 절차를 촉진시키고, 커널 및 사용자 기반 악성 프로그램의 삽입을 방해하는 데 도움이 됩니다.

주 - 변경할 수 없는 영역이 구성된 다음에는 신뢰할 수 있는 경로 로그인을 사용할 때 또는 `reboot -- -w`를 사용한 쓰기 가능한 모드로 시스템을 재부트할 때를 제외한 다른 방법으로는 업데이트가 불가능합니다.

변경할 수 없는 환경에서 응용 프로그램 소프트웨어가 항상 예상대로 실행되는지 확인해야 하지만, Oracle Solaris의 변경할 수 없는 비전역 영역 내에서 Oracle Database 인스턴스 및 Oracle RAC 클러스터가 올바르게 실행되는지 확인해야 합니다.

1. **Oracle Solaris 전역 영역(전용 도메인, 루트 도메인 또는 I/O 도메인)에 수퍼 유저로 로그인합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **`file-mac-profile` 등록 정보를 설정해서 Oracle Solaris 전역 영역 구성을 수정합니다.**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
zonecfg:global> commit
```

3. **변경사항이 적용되도록 Oracle Solaris 전역 영역을 재부트합니다. ILOM 콘솔을 통해 도메인에 로그인합니다.**

4. **변경할 수 없는 전역 영역의 신뢰할 수 있는 경로 콘솔을 시작합니다.**

   변경할 수 없는 전역 영역이 구성되었으므로, 다음 중단 시퀀스 중 하나를 사용해서 콘솔 로그인을 입력하는 것이 중요합니다.

   - **그래픽 콘솔** – F1-A
   - **직렬 콘솔** – <Break> 또는 대체 중단 시퀀스(CR~ Ctrl-b)

```
trusted path console login:
```

5. **I/O 도메인의 전역 영역에 로그인하고 `root` 역할로 전환해서 시스템에 대한 모든 특정 업데이트를 수행하고, 시스템을 재부트해서 다시 읽기 전용 모드로 전환합니다.**

```
# reboot
```

▼ 변경할 수 없는 비전역 영역 구성

Oracle Solaris 비전역 영역을 변경할 수 없도록 구성하려면 다음 작업을 수행합니다.

주 - Oracle Solaris 11 OS는 이 작업에 식별된 것 이외에 추가로 변경할 수 없는 영역 구성을 지원합니다(fixed-configuration). 이러한 옵션에 대한 자세한 내용은 `zonecfg(1M)` 매뉴얼 페이지를 참조하십시오. 하지만 fixed-configuration 옵션은 SuperCluster 기반구조의 일부로 테스트되었습니다.

주의 - 이 작업에 설명된 대로 Oracle Solaris 비전역 영역 변경 불가가 사용으로 설정된 다음에는 영역 사용자 계정 및 암호 추가, 수정 또는 삭제를 수행할 수 없습니다. 하지만 이 문제는 사용자, 역할, 그룹, 권한, 프로파일 등과 같은 영역 특정 정보를 포함하도록 LDAP 디렉토리를 배치하여 해결할 수 있습니다.

주의 - Oracle Solaris 변경할 수 없는 영역 기능은 기본적으로 Oracle Solaris 비전역 영역에서 구현되는 해당 ZFS 데이터 세트로 제한됩니다. 추가 파일 시스템, 풀 또는 데이터 세트는 읽기 전용 루프백 마운트 사용과 같은 다른 방법을 사용해서 이러한 파일 요소에 대한 액세스를 제어할 수 있더라도, 변경할 수 없는 영역 정책을 따르지 않습니다.

1. **연산 서버 중 하나에 수퍼 유저로 로그인하고 호스트 콘솔에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **Oracle Solaris 비전역 영역이 종료되었는지 확인합니다.**

   이 명령이 값을 반환할 경우, Oracle Solaris 비전역 영역이 실행 중이며, 사용자가 이를 종료해야 합니다.

   주 - `zoneadm(1M)` 명령을 사용해서 영역이 중단된 경우, 서비스 중단 및 데이터 손실 가능성을 방지하기 위해 조직에서 설정된 적절한 종료 절차를 따르십시오.

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **`file-mac-profile` 영역 구성 등록 정보를 설정해서 Oracle Solaris 비전역 영역 구성을 조정합니다.**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **필요한 경우 비전역 영역 변경할 수 없는 구성을 사용 안함으로 설정합니다.**

   ```
   # zonecfg -z zone_name set file-mac-profile=none
   ```

5. **변경사항이 적용되도록 Oracle Solaris 비전역 영역을 다시 시작합니다.**

   ```
   # zoneadm -z zone_name boot
   ```

▼ 보안 확인 부트 사용으로 설정(Oracle ILOM CLI)

Oracle ILOM CLI를 통한 보안 확인 부트를 사용으로 설정하려면 이 작업을 수행합니다. 또는 Oracle ILOM 웹 인터페이스를 사용할 수 있습니다. “보안 확인된 부트(Oracle ILOM 웹 인터페이스)” [73]를 참조하십시오.

확인된 부트는 디지털 서명을 사용한 실행 전의 객체 모듈 확인을 나타냅니다. Oracle Solaris는 의심스러운 커널 모듈이 로드되지 않도록 보호합니다. 확인된 부트는 실행 전 커널 모듈을 확인해서 Oracle Solaris의 보안 및 강도를 높여줍니다.

사용으로 설정된 경우, Oracle Solaris 확인된 부트는 모듈을 로드 및 실행하기 전에 커널 모듈에서 출하 시 서명을 확인합니다. 이 검사는 특정 모듈의 우연한 또는 악의적인 수정을 감지합니다. 수행되는 작업을 구성할 수 있으며, 사용으로 설정된 경우, 이러한 작업을 통해 경고 메시지를 출력하고, 모듈 로드 및 실행을 계속하거나, 작업이 실패하고 모듈이 로드 및 실행되지 않습니다.

1. **연산 서버에서 Oracle ILOM에 액세스합니다.**

   연산 서버에 로그인 및 기본 암호 변경 [51]을 참조하십시오.

2. **확인된 부트를 사용으로 설정합니다.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Oracle 제공 인증서를 액세스 및 표시합니다.**

   사전 설치된 확인된 부트 인증서 파일 `/etc/certs/ORCLS11SE`는 Oracle ILOM의 일부로 제공됩니다.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **인증서 로드를 시작합니다.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **`/etc/certs/ORCLS11SE` 파일 내용을 복사해서 Oracle ILOM 콘솔에 붙여넣습니다.**

   Ctrl-z를 입력해서 정보를 저장하고 처리합니다.

   종료하고 변경사항을 무시하려면 Ctrl-c를 입력합니다.

```
-----BEGIN CERTIFICATE-----
```

```
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. 인증서를 확인합니다.

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. OBP `use-nvram` 매개변수가 `false`로 설정되었는지 확인합니다.

확인된 부트를 사용할 때, OBP `use-nvram` 매개변수는 `false`로 설정되어 있어야 합니다. 이렇게 하면 확인된 부트 기능을 사용 안함으로 설정하기 위해 OBP가 수정되는 것을 방지할 수 있습니다. 기본값은 false입니다. Oracle Solaris에 로그인하고 다음을 입력합니다.

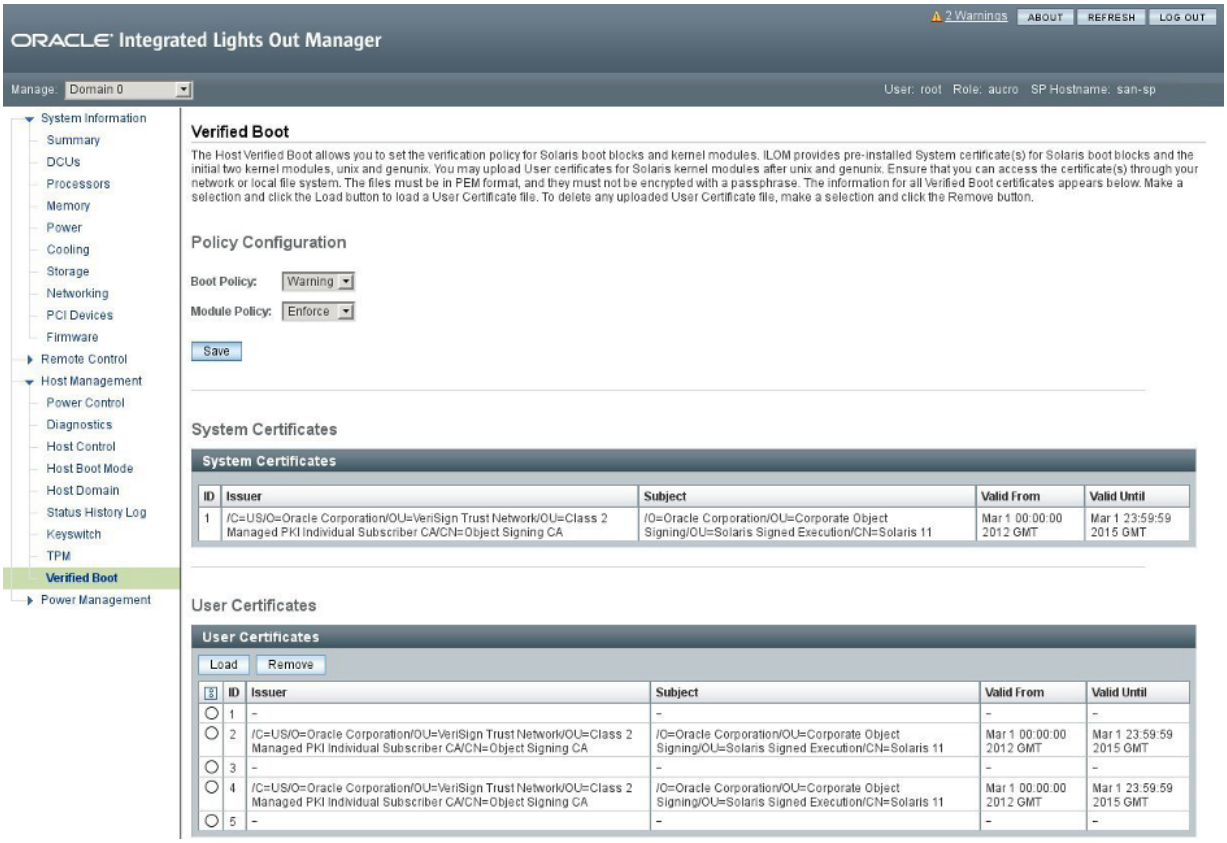
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

보안 확인된 부트(Oracle ILOM 웹 인터페이스)

Oracle ILOM 웹 인터페이스는 또한 확인된 부트 정책 변수의 설정 및 인증서 파일의 관리를 지원하며, CLI와 동일한 기능을 제공합니다. Host Management(호스트 관리) 탐색 메뉴 아래의 Verified Boot(확인된 부트) 링크로 이동합니다.

예를 들면 다음과 같습니다.



추가 연산 서버 리소스

Oracle Solaris OS 및 Oracle Solaris Cluster 보안 설명서를 보려면 OS 버전에 따라 설명서 라이브러리를 참조하십시오. 라이브러리는 http:/docs.oracle.com/en/operating-systems에서 제공됩니다.

Oracle VM Server for SPARC 보안 정보를 보려면 보안 설명서(http://docs.oracle.com/cd/E62357_01)를 참조하십시오.

연산 서버 하드웨어에 대한 보안 정보는 보안 설명서(http://docs.oracle.com/cd/E55211_01)를 참조하십시오.

ZFS Storage Appliance 보안

ZFS Storage Appliance는 비즈니스 인텔리전스, 데이터 웨어하우징, 가상화, 개발 및 테스트, 데이터 보호를 포함한 여러 가지 까다로운 작업 부하에서 저장소 통합을 지원하기 위한 SuperCluster 구성 요소 중 하나입니다.

ZFS Storage Appliance에는 2개의 중복된 ZFS 저장소 컨트롤러가 포함됩니다. 두 컨트롤러에 대해 모두 보안을 설정해야 합니다.

다음 절에서는 ZFS Storage Appliance 보안 지침 및 기능에 대해 설명합니다.

▼ ZFS Storage Appliance에 로그인

이 절에서 보안 작업을 수행하려면 관리 네트워크를 통해 ZFS Storage Appliance에 로그인합니다.

이 작업은 CLI를 사용해서 로그인하는 방법에 대해 설명합니다. Oracle ILOM 웹 인터페이스에 로그인하는 방법에 대한 지침은 *Oracle ZFS Storage Appliance* 관리 설명서를 참조하십시오(“추가 ZFS Storage Appliance 리소스” [84] 참조).

1. **관리 네트워크에서 SSH를 사용해서 ZFS Storage Appliance에 연결합니다.**

   어플라이언스를 관리할 다른 사용자를 구성하지 않은 경우 `root`로 로그인해야 합니다.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
```

```
hostname:>
```

2. **필요한 경우 CLI 도움말에 액세스합니다.**

   `help` 명령은 컨텍스트에 맞는 도움말을 제공합니다. 특정 항목에 대한 도움말은 `help`에 대한 인수로 해당 항목을 지정하여 사용할 수 있습니다. help 명령을 탭 완성하거나 `help topics`를 입력하면 사용 가능한 항목이 표시됩니다.

▼ ZFS Storage Appliance 소프트웨어 버전 확인

ZFS Storage Appliance에서 소프트웨어 버전을 확인하려면 이 절차를 수행합니다.

1. **ZFS Storage Appliance에 로그인합니다.**

   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **소프트웨어 버전을 표시합니다.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

이 예에서 ZFS Storage Appliance 소프트웨어 버전은 `2013.06.05.2.10`입니다.

ZFS Storage Appliance 소프트웨어 버전을 업데이트하려면 My Oracle Support(`https://support.oracle.com`)에서 제공되는 최신 SuperCluster 분기별 전체 스택 다운로드 패치를 설치합니다.

주 - SuperCluster의 경우 추가 제한 사항으로 인해 사용할 수 있는 ZFS Storage Appliance 소프트웨어 버전 및 해당 버전의 업데이트 방법이 제한될 수 있습니다. 이러한 경우에는 오라클 담당자에게 문의하십시오.

▼ ZFS Storage Appliance `root` 암호 변경

ZFS Storage Appliance 자체는 기본 `root` 암호로 사전 구성되어 있지 않습니다. ZFS Storage Appliance의 최초 구성은 포함된 Oracle ILOM에서 콘솔 세션을 통해 수행됩니다. 어플라이언스에 대한 `root` 암호는 이 최초 구성 세션 중에 설정됩니다.

어플라이언스의 콘솔에 처음 액세스하면 셸 인터페이스 구성 화면이 나타납니다. 화면의 정보를 확인하고 필요한 값을 입력합니다. ZFS Storage Appliance에 대한 `root` 암호는 이 프로세스 중에 설정됩니다.

주 - 어플라이언스에 대한 Oracle ILOM은 기본 `root` 계정과 암호 `welcome1`을 갖습니다. Oracle ILOM 보안 [35]을 참조하십시오.

`root` 계정이 준비된 다음에는 이 작업에 설명된 대로 언제라도 암호를 변경할 수 있습니다.

주 - Oracle Engineered Systems Hardware Manager가 관리하는 모든 SuperCluster 구성 요소(예: AFS 저장소 컨트롤러 OS)에 대해 암호가 변경된 경우 Oracle Engineered Systems Hardware Manager에서도 암호를 업데이트해야 합니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 관리 설명서를 참조하십시오.

---

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **`root` 암호를 변경합니다.**
   이 예에서는 미국 국방부 암호 복잡성 정책과 호환되는 암호로 *password*를 바꿉니다.

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

ZFS Storage Appliance의 초기 설치 및 구성에 대한 자세한 내용은 *Oracle ZFS Storage Appliance* 설치 설명서를 참조하십시오. "추가 ZFS Storage Appliance 리소스" [84]를 참조하십시오.

기본 노출된 네트워크 서비스(ZFS Storage Appliance)

이 표에서는 ZFS Storage Appliance에서 노출되는 기본 네트워크 서비스를 보여줍니다.

서비스	프로토콜	포트	설명
SSH	TCP	22	CLI를 사용해서 ZFS Storage Appliance에 대한 관리 액세스를 사용으로 설정하기 위해 보안 셸 서비스에서 사용됩니다.
PORTMAP	TCP/UDP	111	RPC(원격 프로시저 호출) 포트 매핑 데몬(`rpcbind` 또는 `portmap`)에서 사용됩니다. 이 서비스는 NFS 버전 3을 지원하기 위해 필요합니다.
NTP	UDP	123	로컬 시스템 시계를 하나 이상의 외부 시간 소스와 동기화하기 위해 통합된 NTP (Network Time Protocol)(클라이언트 전용) 서비스에서 사용됩니다.
HTTPS (BUI)	TCP	215	브라우저 인터페이스를 사용해서 암호화된(SSL/TLS) 채널을 통해 ZFS Storage Appliance에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTPS 서비스에서 사용됩니다.
원격 복제	TCP	216	통합 원격 데이터 복제 서비스에서 사용됩니다. 원격 데이터 복제는 암호화된(SSL/TLS) 채널을 통해 ZFS Storage Appliance 사이에 프로젝트 및 공유를 복제 및 동기화합니다.

서비스	프로토콜	포트	설명
NFS	TCP/UDP	2049 4045 다양	NFS(네트워크 파일 시스템) 서비스에서 사용됩니다. NFS는 네트워크 파일 공유 서비스를 제공합니다. 실제 포트 수는 사용되는 NFS 프로토콜 버전에 따라 달라집니다. NFS 버전 3은 RPC 포트 매핑 데몬(위 참조) 및 동적으로 할당된 포트를 사용해서 마운트, 상태, 할당량 및 관련 서비스를 제공합니다. 하지만 NFS 버전 4는 TCP/2049만 사용합니다. NFS 잠금 서비스는 TCP/4045를 사용합니다.
iSCSI/iSNS	TCP	3260	데이터 저장소 기능 연결을 위한 IP 기반 저장소 네트워킹 프로토콜을 제공하는 iSCSI 서비스에서 사용됩니다. ZFS Storage Appliance는 네트워크 연결 클라이언트와 iSCSI 장치(LUN)를 공유하도록 구성할 수 있습니다.
서비스 태그	TCP	6481	Oracle ServiceTag 서비스에서 사용됩니다. 서버를 식별하고 서비스 요청을 효율화하는 데 사용되는 Oracle 검색 프로토콜입니다. 이 서비스는 Oracle Enterprise Manager Ops Center와 같은 제품에서 ZFS Storage Appliance 소프트웨어를 검색하고 다른 Oracle 자동 서비스 솔루션과 통합하기 위해 사용됩니다.
NDMP	TCP	10000	ZFS Storage Appliance가 원격으로 조정되는 백업에 참여할 수 있게 해주는 NDMP (네트워크 데이터 관리 프로토콜) 서비스에서 사용됩니다.

ZFS Storage Appliance는 또한 `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV` 등을 포함해서 기본적으로 사용 안함으로 설정되는 다른 여러 서비스를 지원합니다. 설치 후 이러한 서비스를 사용으로 설정하면 추가 네트워크 포트가 노출될 수 있습니다.

ZFS Storage Appliance 보안 구성 강화

다음 항목에서는 ZFS Storage Appliance의 보안 구성을 강화하는 방법에 대해 설명합니다.

▼ Oracle ILOM 보안 구성 강화 구현

ZFS Storage Appliance에는 제품의 일부로 포함된 Oracle ILOM이 들어 있습니다. 다른 Oracle ILOM 구현에서와 같이 장치의 기본 보안 구성을 향상시키기 위해 구현할 수 있는 보안 관련 구성 변경사항이 있습니다.

- **Oracle ILOM 보안 [35]의 절차를 수행해서 ZFS Storage Appliance Oracle ILOM 인터페이스에 대해 보안을 설정합니다.**

▼ 불필요한 서비스 사용 안함으로 설정(ZFS Storage Appliance)

플랫폼의 운영 및 관리 요구 사항을 지원하는 데 필요하지 않은 모든 서비스를 사용 안함으로 설정합니다.

기본적으로 ZFS Storage Appliance에는 필수가 아닌 서비스가 사용 안함으로 설정된 네트워크 기본 보안 구성이 적용되어 있습니다. 하지만 사용자의 보안 정책 및 요구 사항에 따라 추가 서비스를 사용 또는 사용 안함으로 설정해야 할 수 있습니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **ZFS Storage Appliance에서 지원되는 서비스 목록을 표시합니다.**

   ```
   hostname:> configuration services
   ```

3. **제공된 서비스가 사용으로 설정되었는지 여부를 확인합니다.**
   *servicename*을 2단계에서 식별된 서비스 이름으로 바꿉니다.

   ```
   hostname:> configuration services servicename get <status>
   ```

   서비스 상태 매개변수가 `enabled` 값을 반환하면 서비스가 사용으로 설정된 것입니다. 예를 들면 다음과 같습니다.

   ```
   hostname:> configuration services iscsi get <status>
   <status> = online
   ```

4. **더 이상 필요하지 않은 서비스를 사용 안함으로 설정합니다.**
   서비스 상태를 사용 안함으로 설정합니다. 예를 들면 다음과 같습니다.

   ```
   hostname:> configuration services iscsi disable
   ```

▼ 동적 경로 지정 사용 안함으로 설정

ZFS Storage Appliance는 기본적으로 동적 경로 지정 프로토콜을 실행하도록 구성되어 있습니다.

동적 경로 지정 서비스를 사용 안함으로 설정하려면 먼저 통신해야 하는 모든 네트워크에 ZFS Storage Appliance가 직접 연결되었는지 확인하거나 정적 경로 지정 또는 기본 경로를 사용하도록 구성되었는지 확인하십시오. 이 단계는 동적 경로 지정이 사용 안함으로 설정된 후 연결이 손실되지 않도록 보장하기 위해 필요합니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **동적 경로 지정을 사용 안함으로 설정합니다.**

   ```
   hostname:> configuration services dynrouting disable
   ```

3. **동적 경로 지정이 사용으로 설정되었는지 확인하려면 다음을 입력합니다.**

   ```
   hostname:> configuration services dynrouting get <status>
   ```

▼ 보안 셸을 사용해서 원격 root 액세스 제한

기본적으로 ZFS Storage Appliance는 보안 셸(SSH) 서비스를 사용해서 root 계정에 대해 원격 관리 액세스를 허용하도록 구성되어 있습니다.

SSH를 사용해서 원격 루트 액세스를 사용 안함으로 설정하려면 다음 절차를 따르십시오.

이 구성을 변경한 다음에는 root 계정이 더 이상 SSH를 사용해서 시스템에 액세스할 수 없습니다. 하지만 root 계정은 HTTPS 관리 인터페이스를 사용해서 이 시스템에 액세스할 수 있습니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **원격 root 액세스를 사용 안함으로 설정합니다.**

   ```
   hostname:> configuration services ssh set permit_root_login=false
   ```

3. **root 계정이 더 이상 SSH를 사용해서 시스템에 액세스하도록 허용되지 않았는지 확인합니다.**

   ```
   hostname:> configuration services ssh get permit_root_login
   ```

4. **SSH 관리 액세스가 필요한 경우 1개 이상의 비root 계정을 만듭니다.**
   지침은 ZFS Storage Appliance에서 실행 중인 릴리스에 해당하는 *Oracle ZFS Storage Appliance* 관리 설명서를 참조하십시오. "추가 ZFS Storage Appliance 리소스" [84]를 참조하십시오.

▼ 관리 인터페이스 비활성 시간 초과 구성(HTTPS)

ZFS Storage Appliance는 미리 정의된 시간(분) 동안 비활성 상태로 유지된 관리 세션을 연결 해제하고 로그아웃할 수 있는 기능을 지원합니다. 기본적으로 브라우저 사용자 인터페이스(HTTPS) 세션은 15분 후에 시간 초과됩니다.

주 - 어떠한 상응하는 매개변수도 ZFS Storage Appliance의 SSH 명령줄 인터페이스에서 비활성 시간 초과를 강제 적용하지 않습니다.

비활성 시간 초과 매개변수를 사용자 정의 값으로 설정하려면 다음 절차를 따르십시오.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **브라우저 인터페이스와 연관된 현재 비활성 시간 초과 매개변수를 확인합니다.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **시간 초과 매개변수를 구성합니다.**

   `session_timeout` 값은 분 단위로 지정됩니다(이 예에서는 10분).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **2단계를 반복하여 시간 초과 매개변수를 확인합니다.**

▼ 승인되지 않은 SNMP 프로토콜 사용 안함으로 설정

기본적으로 SNMPv1 및 SNMPv2c는 ZFS Storage Appliance에서 사용으로 설정됩니다. ZFS Storage Appliance는 모든 지원되는 제품 버전에서 SNMPv1/v2c를 지원합니다. 2013.1.2 버전부터는 ZFS Storage Appliance에서 SNMPv3도 지원됩니다.

주 - SNMP 프로토콜 버전 3에서는 USM(User-based Security Model)에 대한 지원이 도입되었습니다. 이 기능은 기존 SNMP 커뮤니티 문자열을 특정 권한, 인증 및 개인 정보 보호 프로토콜 및 암호로 구성할 수 있는 실제 사용자 계정으로 바꿉니다. 기본적으로 ZFS Storage Appliance는 통합된(일기 전용) USM 계정에 대한 사용자 이름 또는 암호를 포함하지 않습니다. 보안을 위해서는 배치, 관리 및 모니터링 요구 사항에 따라 USM 자격 증명 및 프로토콜을 구성하십시오.

필요한 경우가 아니면 사용되지 않는 또는 이전 버전의 SNMP 프로토콜이 사용 안함으로 설정되어 있는지 확인합니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **장치에서 사용되는 SNMP 프로토콜 버전을 확인합니다.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **SNMPv3를 사용으로 설정합니다(가능한 경우).**
   SNMPv1/v2c 및 SNMPv3 사용은 서로 배타적이므로, SNMPv3을 사용으로 설정하면 SNMPv1/v2c가 사용 안함으로 설정됩니다.

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **SNMP 버전을 확인합니다.**

```
hostname:> configuration services snmp get version
version = v3
```

▼ SNMP 커뮤니티 문자열 구성

ZFS Storage Appliance가 SNMPv1 또는 v2를 사용하도록 구성된 경우에만 이 작업을 수행합니다.

SNMP는 장치의 건전성을 모니터하는 데 사용되는 경우가 많기 때문에 장치에 사용되는 기본 SNMP 커뮤니티 문자열을 고객 정의 값으로 변경하는 것이 중요합니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **SNMP 커뮤니티 문자열을 변경합니다.**
   이 예에서는 SNMP 커뮤니티 문자열 조합과 관련하여 미국 국방부 요구 사항과 호환되는 값으로 *string*을 바꿉니다.

```
hostname:> configuration services snmp set community=string
community = value
```

3. **SNMP 커뮤니티 문자열을 확인합니다.**

```
hostname:> configuration services snmp get community
```

▼ SNMP 권한 부여된 네트워크 구성

ZFS Storage Appliance가 SNMPv1 또는 v2를 사용하도록 구성된 경우에만 이 작업을 수행합니다.

시스템 구성 정보가 노출되는 것을 최소화하기 위해서는 승인된 네트워크 또는 호스트 소스의 SNMP 질의만 허용해야 합니다.

1. **ZFS Storage Appliance에 로그인합니다.**
   ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **SNMP 권한 부여된 네트워크 매개변수를 구성합니다.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **SNMP 권한 부여된 네트워크 매개변수의 값을 확인합니다.**
   이 예에서 네트워크 매개변수를 `127.0.0.1/8`로 설정하면 모든 네트워크 기반 SNMP 질의가 차단됩니다. 이 값은 필요에 따라 승인된 호스트 및 네트워크를 허용하도록 조정해야 합니다.

   `0.0.0.0/0` 값은 모든 네트워크 위치의 질의를 허용합니다.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

▼ 관리 네트워크 액세스 제한

이러한 보안 강화 절차 외에도 ZFS Storage Appliance에서 노출되는 관리 인터페이스는 전용의 격리된 관리 네트워크에 배치되어야 합니다. 이 단계는 허용되지 않은 또는 의도하지 않은 관리 네트워크 트래픽으로부터 ZFS Storage Appliance를 보호하는 데 도움이 됩니다. 관리 네트워크에 대한 액세스는 이 액세스 레벨이 필요한 관리자에게만 부여된 액세스 권한으로 엄격하게 제어해야 합니다.

또한 ZFS Storage Appliance는 특정 네트워크 인터페이스에서 관리 액세스를 사용 또는 사용 안함으로 설정하도록 구성할 수 있습니다. 이러한 변경은 다음 절차를 사용해서 구현할 수 있습니다.

1. **ZFS Storage Appliance에 로그인합니다.**

ZFS Storage Appliance에 로그인 [75]을 참조하십시오.

2. **관리 네트워크 인터페이스를 구성합니다.**

   이 예에서는 *interface* 값을 이 설정이 적용되는 실제 네트워크 인터페이스의 이름으로 바꿉니다.

   ```
   hostname:> configuration net interfaces select interface set admin=false
   ```

추가 ZFS Storage Appliance 리소스

ZFS Storage Appliance에 대한 추가 보안 지침은 ZFS Storage Appliance에서 실행되는 릴리스에 해당하는 보안 설명서를 참조하십시오. ZFS Storage Appliance 소프트웨어 버전 확인 [76]을 참조하십시오.

다음 설명서에서는 제품의 보안 기능, 성능 및 구성 옵션에 대한 추가 정보를 제공합니다.

- *Oracle ZFS Storage Appliance* 릴리스 보안 설명서(릴리스 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Oracle ZFS Storage Appliance* 릴리스 보안 설명서(릴리스 2013.1.3.0)

  http://docs.oracle.com/cd/E56021_01
- *Oracle ZFS Storage Appliance* 릴리스 보안 설명서(릴리스 2013.1.2.0)

  http://docs.oracle.com/cd/E51475_01

Exadata Storage Server 보안

Exadata Storage Server(저장소 서버)는 SuperCluster의 저장소 빌딩 블록입니다. 각 저장소 서버는 사전 설치된 상태로 제공되며 모든 필수 연산, 저장소 및 소프트웨어 구성 요소가 포함된 상태로 SuperCluster M7의 일부로 통합되어 있습니다.

주 - 사용자는 승인된 방법, 패치 또는 업데이트 적용을 통해서만 구성을 변경할 수 있습니다. 저장소 서버 소프트웨어는 다른 어떤 방법으로도 변경할 수 없습니다.

SuperCluster M7에는 최소 3개의 저장소 서버가 포함됩니다. 추가 저장소 서버는 기본 SuperCluster 랙 및 선택적인 확장 랙에 설치할 수 있습니다. 개별 저장소 서버에 대해 보안을 설정해야 합니다.

다음 항목에서는 저장소 서버 보안 방법에 대해 설명합니다.

▼ 저장소 서버 OS에 로그인

- **관리 네트워크에서 저장소 서버 중 하나에 `celladmin`으로 로그인합니다.**
  기본 암호에 대해서는 “기본 계정 및 암호” [85]를 참조하십시오.

```
# ssh celladmin@Storage_Server_IP_address
```

기본 계정 및 암호

다음 표에서는 저장소 서버 기본 계정 및 암호를 보여줍니다.

계정 이름	유형	기본 암호	설명
root	관리자	welcome1	일반 관리 작업을 수행하고 저장소 서버 소프트웨어를 업데이트하기 위해 저장소 서버 OS에 액세스하는 데 사용됩니다.
celladmin	셀 관리자	Welcome	저장소 서버 설정 및 구성을 수행하는 데 사용됩니다. 또한 플랫폼의 모든 저장소 서버는 이 계정을 사용해서 작동합니다.
cellmonitor	모니터	welcome	모니터링 목적으로만 사용됩니다. 이 계정은 제한된 셸을 사용해서 저장소 서버에 상주하는 객체 및 구성이 이 계정으로부터 수정될 수 없도록 보장합니다.

▼ 저장소 서버 암호 변경

기본 계정 및 암호 목록은 "기본 계정 및 암호" [85]를 참조하십시오.

주 - Oracle Engineered Systems Hardware Manager가 관리하는 모든 SuperCluster 구성 요소(예: Exadata Storage Server OS)에 대해 암호가 변경된 경우 Oracle Engineered Systems Hardware Manager에서도 암호를 업데이트해야 합니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 관리 설명서를 참조하십시오.

---

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **다음 방법 중 하나를 사용해서 기본 암호를 변경합니다.**

   - **로그인되어 있는 서버에서 계정에 대한 암호를 변경합니다.**

     ```
     # passwd account_name
     ```

   - **모든 저장소 서버에서 계정 암호를 변경합니다.**

     `cell_group`은 모든 저장소 서버의 호스트 이름(라인당 하나씩)이 나열된 간단한 텍스트 파일입니다.

     이 예에서는 다음 명령줄 항목을 바꿉니다.

     - *new_password* – 사이트 정책과 호환되는 새 암호로 바꿉니다.
     - *account_name* – Oracle Linux 계정의 이름으로 바꿉니다.

     ```
     # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
     ```

▼ Exadata Storage Server 소프트웨어 버전 확인

1. **저장소 서버 중 하나에 로그인합니다.**

저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **다음 명령을 입력합니다.**

   이 예에서 저장소 서버 소프트웨어 버전은 12.1.2.1.1.150316.2입니다.

```
# imageinfo -ver
12.1.2.1.1.150316.2
```

   소프트웨어 버전을 업데이트하려면 My Oracle Support(https://support.oracle.com)에서 제공되는 최신 SuperCluster 분기별 전체 스택 다운로드 패치를 설치합니다.

주 - SuperCluster의 경우 추가 제한 사항으로 인해 사용할 수 있는 소프트웨어 버전 및 해당 버전의 업데이트 방법이 제한될 수 있습니다. 이러한 경우에는 오라클 담당자에게 문의하십시오.

기본 노출된 네트워크 서비스(저장소 서버)

서비스 이름	프로토콜	포트	설명
SSH	TCP	22	CLI를 사용해서 시스템에 대한 관리 액세스를 제공하기 위해 저장소 서버 소프트웨어에 통합된 보안 셸 서비스에서 사용됩니다. 기본적으로 보안 셸 서버는 관리(NET 0) 및 IB(BONDIB0) 네트워크에서만 연결 요청에 응답하도록 구성됩니다.

저장소 서버는 또한 RDMA(Remote Direct Memory Access) 인터페이스를 통해 RDSv3(Reliable Datagram Sockets) 프로토콜을 사용해서 SuperCluster의 Oracle Database 도메인과 통신합니다. 이 지점 간 통신은 TCP/IP를 사용하지 않으며, SuperCluster 및 저장소 서버의 Oracle Database 도메인이 상주하는 내부 IB 네트워크 분할 영역으로 제한됩니다.

저장소 서버 보안 구성 강화

주 - 저장소 서버에는 제품 일부로 포함된 Oracle ILOM이 들어 있습니다. 다른 Oracle ILOM 구현에서와 같이 장치의 기본 보안 구성을 향상시키기 위해 구현할 수 있는 보안 관련 구성 변경사항이 있습니다. 자세한 내용은 Oracle ILOM 보안 [35]을 참조하십시오.

다음 항목에서는 저장소 서버의 보안을 강화하는 방법에 대해 설명합니다.

- "보안 구성 제한 사항" [88]

보안 구성 제한 사항

host_access_control 유틸리티는 저장소 서버에서 보안 구성 변경사항을 구현할 때 허용 및 지원되는 유일한 방법입니다. 오라클 고객지원센터 공지 1068804.1에 따라 이러한 장치의 구성은 수동으로 변경할 수 없습니다. 또한 이 도구를 사용하려면 먼저 오라클 SuperCluster 고객지원센터에서 해당 저장소 서버 보안 구성을 변경할 수 있는 명시적인 승인을 받아야 합니다. 이 승인을 요청하려면 오라클 고객지원센터에서 서비스 요청을 개설합니다.

Exadata 소프트웨어 버전 11.2.3.3.0에서 제공되는 host_access_control 명령은 액세스 및 보안 구성 설정의 제한된 세트를 구현하기 위해 사용됩니다.

- 원격 root 액세스 제한
- 특정 계정에 대한 네트워크 액세스 제한
- 암호 만료일 및 복잡성 정책 구현
- 로그인 경고 배너 구현
- 계정 잠금 및 세션 시간 초과 정책 정의

▼ host_access_control로 사용 가능한 보안 구성 표시

host_access_control 유틸리티에서 제공되는 항목을 보려면 다음 단계를 수행합니다.

1. **저장소 서버 OS에 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **(선택사항) 자세한 내용을 보려면 `host_access_control` 도움말을 표시합니다.**

```
# /opt/oracle.cellos/host_access_control --help
```

▼ 시스템 부트 로더 암호 구성

관리자가 부트 로더(GRUB) 편집기 또는 명령 인터페이스에 액세스하려고 시도할 때마다 시스템 부트 로더 암호를 요청하도록 저장소 서버를 구성할 수 있습니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**

   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **시스템 부트 로더 암호를 구성합니다.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **설정을 확인합니다.**

   명령이 이 예와 비슷한 값을 반환할 경우 부트 로더 암호가 설치된 것입니다.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

▼ Oracle ILOM 시스템 콘솔 액세스 사용 안함으로 설정

각 저장소 서버에는 원격 모니터링 및 관리를 사용으로 설정하기 위해 포함된 Oracle ILOM이 들어 있습니다. 또한 Oracle ILOM을 사용하면 저장소 서버 시스템 콘솔에 대한 원격 액세스를 제공할 수도 있습니다.

Oracle ILOM을 통해 저장소 서버에 대한 액세스를 사용 안함으로 설정하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**

   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **Oracle ILOM 시스템 콘솔 액세스를 사용 안함으로 설정합니다.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

▼ SSH를 사용해서 원격 root 액세스 제한

기본적으로 root 사용자는 각 저장소 서버에 원격으로 액세스하도록 허용됩니다.

1. **저장소 서버에 celladmin으로 로그인합니다.**
저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **SSH를 사용해서 원격 root 액세스를 사용 안함으로 설정합니다.**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

▼ 시스템 계정 잠금 구성

기본적으로 저장소 서버는 인증 시도가 5번 연속으로 실패한 후 시스템 계정을 잠그도록 구성되어 있습니다.

이 임계값을 변경하려면 다음 절차를 수행합니다.

1. **저장소 서버에 celladmin으로 로그인합니다.**
저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **임계값을 변경합니다.**
미국 국방부 보안 요구 사항을 준수하기 위해서는 값을 3으로 지정합니다. 필요한 경우 로컬 사이트 정책과 호환되는 값으로 바꿉니다.

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

▼ 암호 복잡성 규칙 구성

기본적으로 저장소 서버는 시스템 계정 암호의 복잡성을 관리하는 어떠한 중요한 제한 사항도 구현하지 않습니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **암호 복잡성 정책을 정의합니다.**
   구문:

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

*N0,N1,N2,N3,N4*를 콤마로 구분된 5개 값 세트로 바꿉니다. 이러한 5개 값은 총체적으로 실제 시스템 암호 복잡성 정책을 설정합니다. 이러한 값은 다음과 같습니다(`passwdqc.conf(5)` 매뉴얼 페이지에도 나열됨).

- *N0* – 한 가지 종류의 문자(숫자, 소문자, 대문자 및 특수 문자)로만 구성된 암호에 사용됩니다. 단순한 암호는 안전하지 않기 때문에 일반적으로 이 매개변수는 `disabled`로 설정됩니다.
- *N1* – 문장암호 요구 사항을 충족하지 않는 두 가지 문자 종류로 구성된 암호에 사용됩니다. 이 규칙을 적용하기 위해서는 암호가 N1 문자 수(길이) 이상이어야 합니다.
- *N2* – 문장암호로 구성된 암호에 사용됩니다. 이 규칙을 적용하기 위해서는 암호가 N2 문자 수(길이) 이상이어야 하고 문장암호 요구 사항을 충족해야 합니다.
- *N3* – 세 가지 이상의 문자 종류로 구성된 암호에 사용됩니다. 이 규칙을 적용하기 위해서는 암호가 N3 문자 수(길이) 이상이어야 합니다.
- *N4* – 네 가지 이상의 문자 종류로 구성된 암호에 사용됩니다. 이 규칙을 적용하기 위해서는 암호가 *N4* 문자 수(길이) 이상이어야 합니다.

미국 국방부 보안 요구 사항을 준수하기 위해서는 *N0,N1,N2,N3,N4* 매개변수를 `disabled,disabled,disabled,disabled,15`로 설정합니다. 이렇게 할 경우 4개 이상의 문자 종류(대문자, 소문자, 숫자 및 특수 문자)로 구성되고 길이가 최소 15자 이상인 암호만 허용됩니다.

주 - 암호 시작 부분의 대문자 및 암호 끝 부분의 숫자는 문자 종류 수를 계산할 때 포함되지 않습니다.

예를 들어, 미국 국방부 요구 사항을 충족하는 암호 복잡성을 설정하기 위해서는 다음을 입력합니다.

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **이 설정의 현재 상태를 확인합니다.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

▼ 암호 기록 정책 구성

기본적으로 저장소 서버는 사용자가 이전 10개 암호를 재사용하지 못하도록 방지하는 암호 기록 정책을 정의합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **암호 기록을 변경합니다.**
   미국 국방부 보안 및 PCI-DSS 요구 사항을 준수하기 위해서는 암호 기록 정책을 5로 설정합니다. 이렇게 하면 계정에 지정되었던 이전 5개 암호를 계정에 재사용할 수 없습니다. 필요한 경우 로컬 사이트 정책과 호환되는 값으로 바꿉니다.

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **설정을 확인하려면 2단계를 반복합니다.**

▼ 실패한 인증 잠금 지연 구성

기본적으로 저장소 서버는 인증 시도가 한 번 실패할 때마다 시스템 계정을 10분 동안 잠그는 정책을 구현합니다.

이 임계값을 변경하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **임계값을 변경합니다.**
   미국 국방부 보안 요구 사항을 준수하기 위해서는 값을 4(초)로 설정합니다. 필요한 경우 로컬 사이트 정책과 호환되는 값으로 바꿉니다.

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **설정을 확인하려면 2단계를 반복합니다.**

▼ 암호 만료일 제어 정책 구성

저장소 서버는 암호가 사용되는 최대 기간(일 수), 암호 변경 사이의 최소 기간(일 수) 및 사용자에게 암호 만료 경고가 표시되기 전의 기간(일 수)을 제어하는 매개변수를 포함해서 다양한 암호 만료일 제어 방법을 지원합니다.

미국 국방부 보안 및 PCI-DSS 요구 사항을 준수하기 위해서는 다음 표에 표시된 미국 국방부 값을 사용합니다.

정책	Oracle 기본값	DOD 값
최대 암호 사용 기간	90일	60일
최소 암호 사용 기간	1일	1일
최소 암호 길이	8자	15자
암호 만료 경고	7일	7일

이러한 매개변수를 변경하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **사이트 암호 정책에 따라 이러한 정책을 구성합니다.**

   - **최대 암호 사용 기간 매개변수를 변경하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

   - **최소 암호 사용 기간 매개변수를 변경하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

   - **최소 암호 길이 매개변수를 변경하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

- **암호 만료 경고 매개변수를 변경하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **설정을 확인하려면 2단계를 반복합니다.**

▼ 관리 인터페이스 비활성 시간 초과 구성(로그인 셸)

저장소 서버는 미리 정의된 시간(초) 이상 비활성 상태인 관리 세션을 종료할 수 있는 기능을 지원합니다.

시스템 계정 로그인 셸에 대한 관리 인터페이스 비활성 시간 초과를 정의하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **관리 인터페이스 비활성 시간 초과를 정의합니다.**
   미국 국방부 보안 및 PCI-DSS 요구 사항을 준수하기 위해서는 값을 `900`(초)으로 지정합니다. 필요한 경우 로컬 사이트 정책과 호환되는 값으로 바꿉니다.

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **설정을 확인하려면 2단계를 반복합니다.**

▼ 관리 인터페이스 비활성 시간 초과 구성(보안 셸)

저장소 서버는 미리 정의된 시간(초) 이상 비활성 상태인 관리 SSH 세션을 종료할 수 있는 기능을 지원합니다.

SSH 세션에 대한 관리 인터페이스 비활성 시간 초과를 정의하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

3. **SSH 세션에 대한 관리 인터페이스 비활성 시간 초과를 정의합니다.**
   미국 국방부 보안 요구 사항을 준수하기 위해서는 값을 `900`(초)으로 지정합니다. 필요한 경우 로컬 사이트 정책과 호환되는 값으로 바꿉니다.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **설정을 확인하려면 2단계를 반복합니다.**

▼ 로그인 경고 배너 구성(저장소 서버)

저장소 서버는 사용자가 시스템에 대해 성공적으로 인증되기 전에 고객 특정 메시지를 표시할 수 있는 기능을 지원합니다.

사전 인증 로그인 경고 배너를 정의하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **현재 설정을 확인합니다.**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **승인된 로그인 경고 배너 메시지를 포함하는 텍스트 파일을 만듭니다.**

4. **사전 인증 로그인 경고 배너를 정의합니다.**
   미국 국방부 보안 요구 사항을 준수하기 위해서는 *filename*을 승인된 로그인 경고 배너 메시지가 포함된 파일의 경로 및 이름으로 바꿉니다.

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **설정을 확인하려면 2단계를 반복합니다.**

원격 네트워크 액세스 제한

필터링 규칙 세트를 구현해서 저장소 서버에 대한 인바운드 원격 네트워크 액세스를 제한할 수 있습니다. 또한 사용자 정의 규칙 세트를 정의해서 네트워크 액세스를 미세하게 조정할 수도 있습니다.

원격 액세스를 제한하려면 다음 절차를 수행합니다.

저장소 서버 관리 네트워크 격리

저장소 서버는 격리된 전용 관리 네트워크에 배치됩니다. 이렇게 하면 허용되지 않은 또는 의도하지 않은 네트워크 트래픽으로부터 저장소 서버를 보호하는 데 도움이 됩니다. 관리 네트워크에 대한 액세스는 이 액세스 레벨이 필요한 관리자에게만 부여된 액세스 권한으로 엄격하게 제어해야 합니다.

▼ 원격 네트워크 액세스 제한

저장소 서버에서 원격 네트워크 액세스를 제한할 수 있는 방법은 몇 가지가 있습니다. 사용자 계정 및 시작점에 따라 액세스를 정의하는 하향식 필터링 규칙 세트를 구현해서 저장소 서버에 대한 인바운드 네트워크 액세스를 제한할 수 있습니다. 또한 미국 국방부 및 PCI-DSS 요구 사항에 따라 액세스를 허용 또는 거부하는 사용자 정의 규칙 세트를 정의할 수도 있습니다.

주의 - 시스템에 대한 액세스가 중단되지 않도록 비기본 정책을 구현할 때는 주의가 필요합니다. 새로운 개별 규칙을 추가할 때 변경사항은 즉시 적용됩니다.

규칙 세트를 구현하려면 다음 절차를 수행합니다.

1. **저장소 서버에 `celladmin`으로 로그인합니다.**
   저장소 서버 OS에 로그인 [85]을 참조하십시오.

2. **활성 규칙 세트를 조사합니다.**

```
# /opt/oracle.cellos/host_access_control access --status
```

3. **현재 규칙 세트를 파일로 내보내고 백업 복사본으로 저장합니다.**
   이 명령은 규칙 세트를 ASCII 텍스트 파일로 내보냅니다.

```
# /opt/oracle.cellos/host_access_control access-export --file filename
```

4. **규칙 세트를 만들기 위해 사용하려는 방법에 따라 이러한 명령 중 하나 이상을 수행해서 규칙 세트를 구성합니다.**

- **인바운드 네트워크 제한 사항을 제거하는 개방형 규칙 세트를 구현하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control access --open
```

- **SSH를 사용한 인바운드 액세스만 허용하는 폐쇄형 규칙 세트를 구현하려면 다음을 입력합니다.**

```
# /opt/oracle.cellos/host_access_control access --close
```

- **기존 규칙 세트를 수정하려면 다음을 입력합니다.**

  현재 규칙 세트를 ASCII 텍스트 파일로 내보냅니다.

```
# /opt/oracle.cellos/host_access_control access-export --file filename
```

  편집기를 사용해서 텍스트 파일을 편집해서 규칙 세트를 구성합니다.

  텍스트 파일로부터 규칙 세트를 가져와서 기존 규칙 세트를 대체합니다.

```
# /opt/oracle.cellos/host_access_control access-import --file filename
```

- **특정 규칙을 개별적으로 추가하려면 다음을 수행합니다.**

  이 방법에는 다음 매개변수를 기준으로 한 액세스 허용 및 거부가 포함됩니다.

  - **Username** – 유효한 값에는 `all` 키워드 또는 하나 이상의 유효한 로컬 계정 사용자 이름이 포함됩니다.
  - **Origin** – 유효한 값에는 `all` 키워드 또는 콘솔, 가상 콘솔, Oracle ILOM, IP 주소, 네트워크 주소, 호스트 이름 또는 DNS 도메인 등 시스템 액세스의 소스를 기술하는 개별 항목이 포함됩니다.

  이 예에서는 `trusted.example.org` 호스트 또는 `.trusted.domain.com` 도메인 내의 모든 호스트에서 연결이 시작될 경우 `celladmin` 사용자에게 저장소 서버에 대한 액세스 권한이 부여됩니다.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

추가 저장소 서버 리소스

Exadata Database Machine Security Guide(http://docs.oracle.com/cd/E50790_01/welcome.html)를 참조하십시오.

IB 및 이더넷 스위치 보안

SuperCluster에서 사용되는 Oracle Sun Data Center InfiniBand 스위치 36은 모든 내부 구성 요소 간에 성능 및 확장성이 뛰어나고 완전히 중복된 백플레인을 위한 네트워크 기초를 제공합니다.

IB 스위치는 연산 서버, 저장소 셀 및 ZFS Storage Appliance를 연결합니다. IB 스위치는 포함된 Oracle ILOM을 사용해서 고급 관리 및 모니터링 기능을 제공합니다. 특히 Oracle ILOM은 사용자, 하드웨어, 서비스, 프로토콜 및 기타 구성 매개변수를 모니터링 및 제어할 수 있게 해줍니다.

SuperCluster M7에는 최소 2개의 IB 스위치와 대규모 구성을 위해 필요에 따라 설치되는 추가 IB 스위치가 포함됩니다. 각 IB 스위치는 보안을 설정해야 합니다.

다음 항목에서는 SuperCluster M7에서 IB 스위치에 대해 보안을 설정하는 방법에 대해 설명합니다.

▼ IB 스위치에 로그인

이 작업에서는 스위치에서 대부분의 관리 작업이 수행되는 Oracle ILOM 인터페이스에 로그인하는 방법에 대해 설명합니다.

- **관리 네트워크에서 IB 스위치의 Oracle ILOM에 `ilom-admin`으로 로그인합니다.**
  기본 암호에 대해서는 “기본 계정 및 암호(IB 스위치)” [100]를 참조하십시오.

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ IB 스위치 펌웨어 버전 확인

최신 기능 및 보안 개선 사항을 활용하기 위해 IB 스위치가 지원되는 최신 펌웨어 버전으로 업데이트되어 있는지 확인합니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **펌웨어 버전을 표시합니다.**
   이 예에서 IB 스위치 펌웨어는 버전 `2.1.5-1`입니다.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

IB 스위치 펌웨어의 버전을 업데이트하려면 My Oracle Support(`https://support.oracle.com`)에서 제공되는 최신 SuperCluster 분기별 전체 스택 다운로드 패치를 설치합니다.

주 - SuperCluster M7의 경우 추가 제한 사항으로 인해 사용할 수 있는 IB 스위치 소프트웨어 버전이 제한될 수 있습니다. 제한 사항에는 또한 펌웨어 업데이트 방법도 지정되어 있습니다. 이러한 경우에는 오라클 담당자에게 문의하십시오.

기본 계정 및 암호(IB 스위치)

계정 이름	유형	기본 암호	설명
`root`	관리자	`welcome1`	IB 스위치 OS에 액세스하는 데 사용됩니다. 이 계정은 일반적으로 `ilom-admin`, `ilom-operator` 또는 고객 정의 계정을 대신해서 사용되지 않습니다.
`ilom-admin`	관리자	`ilom-admin`	포함된 Oracle ILOM 소프트웨어에서 관리 기능을 수행하고, 소프트웨어 업그레이드를 수행하고, 사용자 및 서비스를 구성하고, IB 스위치 진단 및 패브릭 관리 기능을 수행하는 데 사용됩니다.
`ilom-operator`	운영자	`ilom-operator`	Oracle ILOM 모니터링 및 IB 패브릭 진단 기능을 위해서만 사용됩니다.
`nm2user`	읽기 전용	`changeme`	이 계정은 IB 스위치의 명령줄 관리 인터페이스에 대한 읽기 전용 권한을 갖고 있습니다. 이 계정은 종종 스위치 하드웨어 및 소프트웨어 모니터링을 지원하기 위해 Oracle Enterprise Manager에서 사용됩니다.

▼ root 및 nm2user 암호 변경

IB 스위치는 두 위치에서 시스템 계정을 유지 관리합니다. root 및 nm2user 계정은 스위치의 기본 OS에서 구성 및 노출됩니다. 계정 추가, 제거 또는 변경은 이 계층에서 지원되지 않지만, 사용자가 기본 암호를 변경해야 합니다.

다른 계정 및 암호는 IB 스위치 암호 변경(Oracle ILOM) [101]을 참조하십시오.

IB 스위치는 암호 복잡성, 만료일, 기록 또는 기타 규칙을 정의 또는 강제 적용하는 기능을 갖고 있지 않습니다. 지정된 암호가 미국 국방부 암호 복잡성 요구 사항을 준수하는지 확인하고 미국 국방부 정책에 따라 암호가 업데이트되도록 보장하는 프로세스가 구현되었는지 확인해야 합니다.

새로운 계정 만들기, 기존 계정에 권한 지정 또는 계정 제거를 포함하여 IB 스위치 계정 관리에 대한 자세한 내용은 *Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide* 및 *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*을 참조하십시오. "추가 IB 스위치 리소스" [107]를 참조하십시오.

주 - Oracle Engineered Systems Hardware Manager가 관리하는 모든 SuperCluster 구성 요소(예: IB 스위치)에 대해 암호가 변경된 경우 Oracle Engineered Systems Hardware Manager에서도 암호를 업데이트해야 합니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 관리 설명서를 참조하십시오.

---

1. **IB 스위치에 root로 로그인합니다.**

```
# ssh root@IB_Switch_IP_address
```

기본 암호에 대해서는 "기본 계정 및 암호(IB 스위치)" [100]를 참조하십시오.

2. **root 암호를 변경합니다.**

```
$ passwd root
```

3. **nm2user 암호를 변경합니다.**

```
$ passwd nm2user
```

▼ IB 스위치 암호 변경(Oracle ILOM)

IB 스위치는 두 위치에서 시스템 계정을 유지 관리합니다. 이 절에서는 IB 스위치의 Oracle ILOM 인터페이스에서 암호를 변경하는 방법에 대해 설명합니다. 다른 계정 및 암호는 root 및 nm2user 암호 변경 [101]을 참조하십시오.

기본 IB 스위치 계정 및 고객 정의 계정은 IB 스위치에서 포함된 Oracle ILOM을 통해 관리됩니다.

계정을 보고 암호를 변경하려면 다음 절차를 수행합니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.
   기본 암호에 대해서는 "기본 계정 및 암호(IB 스위치)" [100]를 참조하십시오.

2. **IB 스위치에서 구성된 Oracle ILOM 계정을 확인합니다.**

```
-> show /SP/users
```

3. **`ilom-admin` 계정의 암호를 변경합니다.**

```
-> set /SP/users/ilom-admin password=password
```

IB 스위치 네트워크 격리

IB 스위치의 관리 인터페이스는 격리된 전용 관리 네트워크에 배치됩니다. 이렇게 하면 허용되지 않은 또는 의도하지 않은 네트워크 트래픽으로부터 IB 스위치를 보호할 수 있습니다.

이 관리 네트워크에 대한 액세스는 이 액세스 레벨이 필요한 관리자에게만 부여된 액세스 권한으로 엄격하게 제어해야 합니다.

기본 노출된 네트워크 스위치(IB 스위치)

서비스 이름	프로토콜	포트	설명
SSH	TCP	22	CLI를 사용해서 IB 스위치에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 보안 셸 서비스에서 사용됩니다.
HTTP(BUI)	TCP	80	브라우저 인터페이스를 사용해서 IB 스위치에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTP 서비스에서 사용됩니다. TCP/80은 일반적으로 일반 텍스트 액세스에 사용되지만, 기본적으로 IB 스위치는 수신되는 요청을 TCP/443에서 실행되는 서비스의 보안 버전으로 자동으로 재지정합니다.
NTP	UDP	123	로컬 시스템 시계를 하나 이상의 외부 시간 소스와 동기화하기 위해 사용되는 통합된 NTP(Network Time Protocol)(클라이언트 전용) 서비스에서 사용됩니다.

서비스 이름	프로토콜	포트	설명
SNMP	UDP	161	IB 스위치의 건전성을 모니터하고 수신된 트랩 알림을 모니터할 수 있는 관리 인터페이스를 제공하기 위해 통합된 SNMP 서비스에서 사용됩니다.
HTTPS(BUI)	TCP	443	브라우저 인터페이스를 사용해서 암호화된(SSL/TLS) 채널을 통해 IB 스위치에 대한 관리 액세스를 사용으로 설정하기 위해 통합된 HTTPS 서비스에서 사용됩니다.
IPMI	TCP	623	통합된 IPMI(Intelligence Platform Management Interface) 서비스에서 다양한 모니터링 및 관리 기능에 대한 컴퓨터 인터페이스를 제공하기 위해 사용됩니다. 이 서비스는 Oracle Enterprise Manager Ops Center에서 하드웨어 인벤토리 데이터, 현장 대체 가능 장치 설명, 하드웨어 센서 정보 및 하드웨어 구성 요소 상태 정보를 수집하는 데 사용되므로, 사용 안함으로 설정하지 마십시오.
ServiceTag	TCP	6481	Oracle ServiceTag 서비스에서 사용됩니다. 서버를 식별하고 서비스 요청을 효율화하는 데 사용되는 Oracle 검색 프로토콜입니다. 이 서비스는 Oracle Enterprise Manager Ops Center와 같은 제품에서 IB 스위치 소프트웨어를 검색하고 다른 Oracle 자동 서비스 솔루션과 통합하기 위해 사용됩니다.

IB 스위치 구성 강화

다음 항목에서는 여러 구성 설정을 통해 IB 스위치에 대해 보안을 설정하는 방법을 설명합니다.

▼ 불필요한 서비스 사용 안함으로 설정(IB 스위치)

플랫폼의 운영 및 관리 요구 사항을 지원하는 데 필요하지 않은 모든 서비스를 사용 안함으로 설정합니다. 기본적으로 IB 스위치에는 필수가 아닌 서비스가 이미 사용 안함으로 설정된 네트워크 기본 보안 구성이 적용되어 있습니다. 하지만 고객 보안 정책 및 요구 사항에 따라 추가 서비스를 사용 안함으로 설정해야 할 수 있습니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**

   IB 스위치에 로그인 [99]을 참조하십시오.

2. **IB 스위치에서 지원되는 서비스 목록을 확인합니다.**

```
-> show /SP/services
```

3. **제공된 서비스가 사용으로 설정되었는지 여부를 확인합니다.**

   *servicename*을 2단계의 서비스 이름으로 바꿉니다.

   ```
   -> show /SP/services/servicename servicestate
   ```

   대부분의 서비스에서는 `servicestate` 매개변수를 인식하여 서비스의 사용 또는 사용 안함으로 설정 여부를 기록하지만, `servicetag`, `ssh`, `sso` 및 `wsman`과 같은 일부 서비스에서는 `state`라는 매개변수가 사용됩니다. 사용되는 실제 매개변수와 관계없이 다음 예에 표시된 것처럼 서비스 상태 매개변수가 `enabled` 값을 반환하면 서비스가 사용으로 설정된 것입니다.

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **더 이상 필요하지 않은 서비스를 사용 안함으로 설정하려면 서비스 상태를 `disabled`로 설정합니다.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **이러한 서비스를 사용 안함으로 설정해야 하는지 확인합니다.**

   사용된 도구 및 방법에 따라 HTTP 및 HTTPS 브라우저 서비스는 필요하지 않거나 사용되지 않는 경우, 사용 안함으로 설정할 수 있습니다. 유형:

   ```
   -> set /SP/services/http servicestate=disabled
   -> set /SP/services/http secureredirect=disabled
   -> set /SP/services/https servicestate=disabled
   ```

   - 브라우저 관리 인터페이스(HTTP, HTTPS):
     - -> **set /SP/services/http servicestate=disabled**
     - -> **set /SP/services/http secureredirect=disabled**
     - -> **set /SP/services/https servicestate=disabled**

▼ HTTPS에 대한 HTTP 재지정 구성(IB 스위치)

기본적으로 IB 스위치는 스위치와 관리자 사이에 모든 브라우저 기반 통신이 암호화되도록 보장하기 위해 수신되는 HTTP 요청을 HTTPS 서비스로 재지정하도록 구성되어 있습니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **보안 재지정이 사용으로 설정되었는지 확인합니다.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **기본값이 변경된 경우 보안 재지정을 사용으로 설정할 수 있습니다.**

```
-> set /SP/services/http secureredirect=enabled
```

▼ 승인되지 않은 SNMP 프로토콜 사용 안함으로 설정(IB 스위치)

기본적으로 SNMPv1, SNMPv2c 및 SNMPv3은 IB 스위치 모니터 및 관리에 사용되는 SNMP 서비스에 대해 모두 사용으로 설정되어 있습니다. 필요한 경우가 아니면 이전 버전의 SNMP 프로토콜이 사용 안함으로 설정되어 있는지 확인합니다.

주 - SNMP 프로토콜 버전 3에서는 USM(User-based Security Model)에 대한 지원이 도입되었습니다. 이 기능은 기존 SNMP 커뮤니티 문자열을 특정 권한, 인증 및 개인 정보 보호 프로토콜 및 암호로 구성할 수 있는 실제 사용자 계정으로 바꿉니다. 기본적으로 IB 스위치는 USM 계정을 포함하지 않습니다. 사용자의 고유 배치, 관리 및 모니터링 요구 사항을 기준으로 SNMPv3 USM 계정을 구성합니다.

---

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **각 SNMP 프로토콜의 상태를 확인합니다.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **필요한 경우 SNMPv1 및 SNMPv2c를 사용 안함으로 설정합니다.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

▼ SNMP 커뮤니티 문자열 구성(IB 스위치)

이 작업은 SNMP v1 또는 SNMPv2c가 사용으로 설정되었고 사용하도록 구성된 경우에만 적용할 수 있습니다.

SNMP는 장치의 건전성을 모니터하는 데 사용되는 경우가 많기 때문에 장치에 사용되는 기본 SNMP 커뮤니티 문자열을 고객 정의 값으로 바꾸는 것이 중요합니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **새로운 SNMP 커뮤니티 문자열을 만듭니다.**
   이 예에서는 명령줄에서 다음 항목을 바꿉니다.

   - *string* – SNMP 커뮤니티 문자열 조합과 관련하여 미국 국방부 요구 사항과 호환되는 고객 정의 값으로 바꿉니다.
   - *access* – 읽기 전용 또는 읽기-쓰기 액세스 문자열인지 여부에 따라 `ro` 또는 `rw`로 바꿉니다.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   새 커뮤니티 문자열을 만든 다음에는 기본 커뮤니티 문자열을 제거해야 합니다.

3. **기본 SNMP 커뮤니티 문자열을 제거합니다.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **SNMP 커뮤니티 문자열을 확인합니다.**

   ```
   -> show /SP/services/snmp/communities
   ```

▼ 기본 자체 서명된 인증서 바꾸기(IB 스위치)

IB 스위치는 자체 서명된 인증서를 사용해서 HTTPS 프로토콜을 즉시 사용할 수 있게 해줍니다. 가장 좋은 방법은 자체 서명된 인증서를 사용자 환경에서 사용하도록 승인되었고 인정된 CA(인증 기관)에서 서명된 인증서로 바꾸는 것입니다.

IB 스위치는 HTTPS, HTTP, SCP, FTP, TFTP를 포함한 SSL/TLS 인증서 및 개인 키를 액세스하는 데 사용할 수 있는 여러 방법을 지원하며, 정보를 웹 브라우저 인터페이스에 직접 붙여 넣습니다. 자세한 내용은 *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36 document*를 참조하십시오. “추가 IB 스위치 리소스” [107]를 참조하십시오.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **IB 스위치에서 자체 서명된 기본 인증서를 사용 중인지 확인합니다.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **조직의 인증서를 설치합니다.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

▼ 관리 CLI 세션 시간 초과 구성(IB 스위치)

IB 스위치는 미리 정의된 시간(분) 동안 비활성 상태로 유지된 관리 CLI 세션을 연결 해제하고 로그아웃할 수 있는 기능을 지원합니다.

기본적으로 CLI는 15분 후 시간 초과됩니다.

1. **IB 스위치에 `ilom-admin`으로 로그인합니다.**
   IB 스위치에 로그인 [99]을 참조하십시오.

2. **CLI와 연관된 비활성 시간 초과 매개변수를 확인합니다.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **비활성 시간 초과 매개변수를 설정합니다.**
   *n*을 분 단위로 지정된 값으로 바꿉니다.

```
-> set /SP/cli timeout=n
```

추가 IB 스위치 리소스

IB 스위치 관리 및 보안 절차에 대한 자세한 내용은 Sun Datacenter InfiniBand Switch 36 설명서 라이브러리(http://docs.oracle.com/cd/E36265_01)를 참조하십시오.

▼ 이더넷 스위치 암호 변경

주 - Oracle Engineered Systems Hardware Manager가 관리하는 모든 SuperCluster 구성 요소(예: 이더넷 스위치)에 대해 암호가 변경된 경우 Oracle Engineered Systems Hardware Manager에서도 암호를 업데이트해야 합니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 관리 설명서를 참조하십시오.

1. **이더넷 스위치 콘솔에서 랩탑 또는 비슷한 장치로 직렬 케이블을 연결합니다.**

   기본 직렬 포트 속도는 9600보, 8비트, 패리티 없음, 1 중지 비트 및 핸드셰이크 없음입니다.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **스위치를 사용으로 설정 모드로 설정합니다.**

```
sscsw-adm0> enable
```

3. **암호를 설정합니다.**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **구성을 저장합니다.**

```
sscsw-adm0# copy running-config startup-config
```

5. **세션을 종료합니다.**

```
sscsw-adm0# exit
```

6. **이더넷 스위치에서 랩탑을 연결 해제합니다.**

“준수 감사” [109]

Oracle Solaris compliance 유틸리티를 사용하면 알려진 벤치마크에 대해 시스템 준수 상태를 평가하고 보고할 수 있습니다.

Oracle Solaris `compliance` 명령은 특정 요구 사항에 대한 준수를 확인하는 코드, 파일 또는 명령 출력에 벤치마크 요구 사항을 매핑합니다. Oracle SuperCluster에는 현재 2개의 보안 준수 벤치마크 프로파일이 지원됩니다.

- **Recommented** – Center of Internet Security 벤치마크 기반의 프로파일입니다.
- **PCI-DSS** – PCI DSS(지불 카드 업계 데이터 보안 표준) 준수 요구 사항을 확인하는 프로파일입니다.

이러한 프로파일링 도구는 보안 컨트롤을 준수 요구 사항에 매핑하며, 결과 준수 보고서를 통해 감사 시간을 상당히 줄일 수 있습니다. 또한 준수 기능은 각 보안 검사의 근거와 실패한 검사의 수정 단계가 포함된 설명서를 제공합니다. 설명서를 교육용으로 사용하거나 향후 테스트 지침으로 사용할 수 있습니다. 기본적으로 설치할 때 각 보안 프로파일의 설명서가 생성됩니다. SuperCluster Solaris 관리자는 벤치마크를 추가 또는 변경할 수 있으며 새 설명서를 만들 수 있습니다.

다음 항목에서는 준수 보고서 실행 방법 및 FIPS-140 준수에 대해 설명합니다.

▼ 준수 평가 생성

이 작업을 실행하려면 패키지를 시스템에 추가할 수 있도록 소프트웨어 설치 권한 프로파일이 지정되어 있어야 합니다. 대부분의 준수 명령을 수행하려면 관리 권한이 지정되어 있어야 합니다.

1. **준수 패키지를 설치합니다.**

```
# pkg install compliance
```

이 메시지는 패키지가 설치되어 있음을 나타냅니다.

```
No updates necessary for this image.
```

자세한 내용은 `pkg(1)` 매뉴얼 페이지를 참조하십시오.

주 - 준수 테스트를 실행할 모든 영역에 패키지를 설치합니다.

---

2. 사용 가능한 벤치마크, 프로파일 및 모든 이전 평가를 나열합니다.

이 예에는 2개의 벤치마크가 있습니다.

- **`pci-dss`** — `Solaris_PCI-DSS`라는 프로파일이 포함됩니다.
- **`solaris`** — `Baseliine` 및 `Recommended`라는 2개의 프로파일이 포함됩니다.

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. 준수 평가를 생성합니다.

다음 구문을 사용하여 `compliance` 명령을 실행합니다.

`compliance assess -b` 벤치마크 `-p` 프로파일

`-b`	특정 벤치마크를 지정합니다. 지정되지 않은 경우 값이 기본적으로 `solaris`로 설정됩니다.
`-p`	프로파일을 지정합니다. 프로파일 이름은 대소문자를 구분합니다. 지정되지 않은 경우, 값이 기본적으로 첫번째 프로파일로 설정됩니다.

예:

- `Recommended` 프로파일을 사용합니다.

  ```
  # compliance assess -b solaris -p Recommended
  ```

  이 명령은 `/var/share/compliance/assessments`에서 로그 파일, XML 파일 및 HTML 파일에 평가가 포함된 디렉토리를 만듭니다.
- PCI-DSS 프로파일 사용:

  ```
  # compliance assess -b pci-dss
  ```

주 - `pci-dss` 벤치마크에는 프로파일이 하나만 포함되므로 명령줄에서 프로파일 옵션(`-p`)이 필요하지 않습니다.

---

4. 준수 파일이 생성되었는지 확인합니다.

```
# cd /var/share/compliance/assessments/filename_timestamp
```

```
# ls
recommended.html
recommended.txt
recommended.xml
```

주 - 동일한 compliance 명령을 다시 실행해도 파일이 바뀌지 않습니다. 평가 디렉토리를 다시 사용하려면 먼저 파일을 제거해야 합니다.

5. **(선택사항) 사용자 정의 보고서를 만듭니다.**

   사용자 정의 보고서는 반복해서 실행할 수 있습니다. 하지만 평가는 원래 디렉토리에서 한 번만 실행할 수 있습니다.

   이 예에서는 보고서에 표시할 결과 유형을 선택하기 위해 -s 옵션이 사용되었습니다.

   기본적으로 notselected 또는 notapplicable을 제외한 모든 결과 유형이 보고서에 표시됩니다. 결과 유형은 기본값 외에 추가로 표시하도록 콤마로 구분된 목록에 지정됩니다. 앞에 -를 표시하여 개별 결과 유형을 숨길 수 있으며, =를 사용하여 목록을 시작하면 포함할 결과 유형을 정확하게 지정합니다. 결과 유형은 pass, fixed, notchecked, notapplicable, notselected, informational, unknown, error 또는 fail입니다.

   ```
   # compliance report -s -pass,fail,notselected
   /var/share/compliance/assessments/filename_timestamp/report_A.html
   ```

   이 명령은 선택되지 않은 실패한 항목을 HTML 형식으로 포함하는 보고서를 만듭니다. 가장 최근 평가에 대해 보고서가 실행됩니다.

6. **전체 보고서를 봅니다.**

   텍스트 편집기에서 로그 파일을 보거나, 브라우저에서 HTML 파일을 보거나, XML 뷰어에서 XML 파일을 볼 수 있습니다. 예를 들어, 이전 단계의 사용자 정의 HTML 보고서를 보려면 다음 브라우저 항목을 입력합니다.

   ```
   file:///var/share/compliance/assessments/filename_timestamp/report_A.html
   ```

7. **보안 정책을 통과하는 데 필요한 오류를 수정합니다.**

   수정을 완료하기 위해 시스템을 재부트해야 할 경우 시스템을 재부트한 다음 평가를 다시 실행합니다.

8. **오류가 없을 때까지 평가를 반복합니다.**

▼ (선택사항) cron 작업을 사용하여 준수 보고서 실행

- **수퍼 유저 권한으로 crontab -e 명령을 사용하여 적합한 항목을 crontab 파일에 추가합니다.**

  이 목록은 crontab 항목 예를 제공합니다.

  - 오전 2:30에 일간 준수 평가를 실행합니다.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

- 일요일 오전 1:15에 주간 준수 평가를 실행합니다.

```
15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
```

- 매월 1일 오전 4:00에 월간 평가를 실행합니다.

```
0 4 1 * * /usr/bin/compliance assess -b pci-dss
```

- 매월 첫번째 월요일 오전 3:45에 평가를 실행합니다.

```
45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
```

FIPS-140-2 레벨 1 준수

SuperCluster에 호스트되는 암호화 응용 프로그램은 FIPS 140-2 레벨 1 준수에 대해 검증된 Oracle Solaris의 암호화 프레임워크 기능을 사용합니다. Oracle Solaris 암호화 프레임워크는 Oracle Solaris를 위한 중앙 암호화 저장소이며, 사용자 공간 및 커널 레벨 프로세스를 지원하는 두 가지 FIPS 140 확인 모듈을 제공합니다. 이러한 라이브러리 모듈은 암호화, 해독, 해싱, 서명 생성 및 확인, 인증서 생성 및 확인, 메시지 인증 기능을 응용 프로그램에 제공합니다. 이러한 모듈로 호출되는 사용자 레벨 응용 프로그램은 FIPS 140 모드에서 실행됩니다.

Oracle Solaris 암호화 프레임워크 외에 Oracle Solaris에 포함된 OpenSSL 객체 모듈은 FIPS 140-2 레벨 1 준수에 대해 검증되었으며, 보안 셸 및 TLS 프로토콜 기반의 응용 프로그램에 대한 암호화를 지원합니다. 클라우드 서비스 공급자는 FIPS 140 호환 모드에서 테넌트 호스트를 사용으로 설정하도록 선택할 수 있습니다. FIPS 140 호환 모드로 실행할 때 FIPS 140-2 공급자인 Oracle Solaris 및 OpenSSL은 FIPS 140 검증 암호화 알고리즘 사용을 강화합니다.

또한 (필요한 경우) FIPS-140 호환 작업 사용으로 설정(Oracle ILOM) [36]을 참조하십시오.

이 표에서는 SuperCluster M7에서 Oracle Solaris로 지원되는 FIPS 승인 알고리즘을 보여줍니다.

키 또는 **CSP**	인증서 번호	
	v1.0	**v1.1**
대칭 키		
AES: 128, 192, 256비트 키 크기에 대한 ECB, CBC, CFB-128, CCM, GMAC, GCM 및 CTR 모드	#2311	#2574
AES: 256 및 512비트 키 크기에 대한 XTS 모드	#2311	#2574
TripleDES: 키 입력 옵션 1에 대한 CBC 및 ECB 모드	#1458	#1560
비대칭 키		
RSA PKCS#1.5 서명 생성/확인: 1024, 2048비트(SHA-1, SHA-256, SHA-384, SHA-512 사용)	#1194	#1321
ECDSA 서명 생성/확인: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
SHS(보안 해싱 표준)		

키 또는 **CSP**	인증서 번호	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
(키 입력) 해시 기반 메시지 인증		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
난수 생성기		
swrand FIPS 186-2 난수 생성기	#1154	#1222
n2rng FIPS 186-2 난수 생성기	#1152	#1226

Oracle Solaris는 FIPS 140-2 레벨 1에 대해 검증된 두 가지 암호화 알고리즘 공급자를 제공합니다.

- Oracle Solaris의 암호화 프레임워크 기능은 Oracle Solaris 시스템의 중앙 암호화 저장소이며 두 가지 FIPS 140 모듈을 제공합니다. userland 모듈은 사용자 공간에서 실행되는 응용 프로그램에 암호화를 제공하고, kernel 모듈은 커널 레벨 프로세스에 암호화를 제공합니다. 이러한 라이브러리 모듈은 암호화, 해독, 해싱, 서명 생성 및 확인, 인증서 생성 및 확인, 메시지 인증 기능을 응용 프로그램에 제공합니다. 이러한 모듈로 호출되는 사용자 레벨 응용 프로그램은 FIPS 140 모드로 실행됩니다(예: `passwd` 명령 및 IKEv2). 커널 레벨 소비자(예: Kerberos 및 IPsec)는 전용 API를 사용하여 커널 암호화 프레임워크를 호출합니다.
- OpenSSL 객체 모듈은 SSH 및 웹 응용 프로그램에 암호화를 제공합니다. OpenSSL은 SSL(Secure Sockets Layer) 및 TLS(Transport Layer Security) 프로토콜용 오픈 소스 툴킷으로, 암호화 라이브러리를 제공합니다. Oracle Solaris에서 SSH 및 Apache 웹 서버는 OpenSSL FIPS 140 모듈의 소비자입니다. Oracle Solaris는 모든 소비자에 대해 제공되는 Oracle Solaris 11.2의 경우 OpenSSL의 FIPS 140 버전이 제공되지만, Oracle Solaris 11.1의 버전은 Solaris SSH에 대해서만 제공됩니다. FIPS 140-2 공급자 모듈은 CPU를 많이 사용하므로 기본적으로 사용으로 설정되지 않습니다. 관리자는 FIPS 140 모드에서 공급자를 사용으로 설정하고 소비자를 구성해야 합니다.

Oracle Solaris에서 FIPS-140 공급자를 사용으로 설정에 대한 자세한 내용은 Oracle Solaris 11 운영체제 보안 제목(http://docs.oracle.com/cd/E36784_01) 아래에 제공되는 *Using a FIPS 140 Enabled System in Oracle Solaris 11.2*라는 문서를 참조하십시오.

SuperCluster M7 시리즈 시스템 보안 유지

다음 항목에서는 시스템 수명 전반에 걸친 보안 유지 관리를 위해 사용할 수 있는 SuperCluster M7 시리즈 기능에 대해 설명합니다.

SuperCluster 보안 관리

SuperCluster M7에는 Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager 및 Oracle Identity Management Suite를 포함해서 다양한 제품의 기능이 사용됩니다. 다음 절에서는 다음과 같은 세부정보를 제공합니다.

보안 관리를 위한 Oracle ILOM

Oracle ILOM은 여러 SuperCluster M7 구성 요소에 포함된 서비스 프로세서입니다. Oracle ILOM을 사용해서 다음과 같은 아웃오브밴드 관리 활동을 수행할 수 있습니다.

- SuperCluster 구성 요소의 보안 정전 관리를 수행하기 위한 보안 액세스를 제공합니다. 액세스에는 SSL로 보호되는 웹 기반 액세스, 보안 셸과 IPMI v2.0 및 SNMPv3 프로토콜을 사용하는 명령줄 액세스가 포함됩니다.

- RBAC 모델을 사용하여 임무 요구 사항을 구분합니다. 사용자가 수행할 수 있는 기능을 제한하는 특정 역할로 개별 사용자를 지정합니다.
- 모든 로그인 및 구성 변경사항에 대한 감사 레코드를 제공합니다. 각 감사 로그 항목은 작업을 수행하는 사용자를 시간 기록과 함께 나열합니다. 이 기능을 사용하면 허용되지 않은 활동 또는 변경사항을 감지하고 이러한 작업과 연관된 특정 사용자를 확인할 수 있습니다.

자세한 내용은 Oracle Integrated Lights Out Manager 설명서(http://docs.oracle.com/en/hardware/?tab=4)를 참조하십시오.

Oracle Identity Management Suite

Oracle Identity Management 제품군은 조직 내에서 사용자 ID 및 계정에 대한 종단간 수명 주기를 관리할 수 있습니다. 이 제품군에는 Single Sign-On, 웹 기반 액세스 제어, 웹 서비스 보안, ID 관리, 강력한 인증 및 ID 및 액세스 관리에 대한 지원이 포함됩니다.

Oracle Identity Management는 Oracle SuperCluster에서 실행되는 응용 프로그램 및 서비스뿐만 아니라 이를 관리하는 기본 기반구조 및 서비스에 대해서도 ID 및 액세스 관리를 위한 단일 지점을 제공할 수 있습니다.

자세한 내용은 다음 위치의 Oracle Identity Management 설명서를 참조하십시오.

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager는 보관 중인 정보를 보호하는 암호화 키의 관리 및 모니터링을 간소화하는 포괄적인 KMS(키 관리 시스템)입니다.

Oracle Key Manager는 수천 개의 장치 및 수백만 개의 키를 관리할 수 있는 확장성 및 가용성이 뛰어난 기반구조로 엔터프라이즈급 환경을 지원합니다. 이 기능은 강화된 운영 환경에서 작동하며, 키 관리 및 모니터링 작업을 위해 강력한 액세스 제어 및 역할을 강화하고, FIPS 140-2 등급 하드웨어 보안 모듈인 Oracle Sun Crypto Accelerator 6000 PCIe 카드에서 키 보안 저장소를 선택적으로 지원합니다.

SuperCluster의 컨텍스트 내에서 Oracle Key Manager는 테이프 드라이브를 암호화하는 Oracle StorageTek, 투명한 데이터 암호화를 사용하여 암호화된 Oracle Database, Oracle Solaris 11 OS에서 제공되는 암호화된 ZFS 파일 시스템에서 사용되는 암호화 키 액세스에 대해 권한 부여, 보안 및 관리를 수행할 수 있습니다.

자세한 내용은 다음 위치의 Oracle Key Manager 설명서를 참조하십시오.

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager는 Oracle 서비스 담당자가 사용하기 위한 BUI 기반의 랙 레벨 하드웨어 관리 도구입니다. 자세한 내용은 *Oracle SuperCluster M7* 시리즈 소유자 안내서*:* 관리를 참조하십시오.

Oracle Engineered Systems Hardware Manager에는 두 가지 인증 정보 세트가 포함됩니다.

- **SuperCluster M7 구성 요소 암호**

  Oracle Engineered Systems Hardware Manager는 모든 SuperCluster M7 하드웨어의 모든 출하 시 기본 계정에 대한 암호 보안 저장소를 유지합니다. 이 소프트웨어는 이러한 암호를 사용하여 SuperCluster M7 구성 요소를 관리합니다.

  이러한 암호가 변경되면 Oracle Engineered Systems Hardware Manager 응용 프로그램을 새 암호로 업데이트해야 합니다.
- **로컬 인증**

  Oracle Engineered Systems Hardware Manager에는 두 가지 로컬 사용자 계정이 포함됩니다. 한 가지 계정은 고객이 해당 환경에 대해 Oracle Engineered Systems Hardware Manager를 조정하고 서비스 계정을 관리하기 위해 사용합니다. 다른 계정은 Oracle 서비스 담당자가 SuperCluster M7 하드웨어 구성, 지원 및 서비스를 위해 사용합니다.

Oracle Engineered Systems Hardware Manager는 다음과 같은 로컬 관리 리소스를 제공합니다.

- **암호 정책** – 기업 정책에 따라 응용 프로그램 암호를 구성함으로써 기업 표준에 따라 암호를 사용하도록 보장할 수 있습니다.

  주 - 암호 정책 설정은 해당 기업의 보안 관리자에게 문의하십시오.

- **인증서** – Oracle Engineered Systems Hardware Manager는 인증서를 사용하여 연산 서버와 Oracle Engineered Systems Hardware Manager 서버 및 BUI 사이의 통신에 보안을 설정합니다. 이러한 인증서는 설치 중에 자동으로 생성되며, 각 SuperCluster 인스턴스에 대해 고유하지만, 고객이 제공한 인증서 및 키로 바꿀 수 있습니다.
- **포트** – Oracle Engineered Systems Hardware Manager에서 사용되는 네트워킹 포트는 기업 정책과 충돌할 경우 구성 가능합니다. 사용되는 포트는 8001부터 8004(포함)까지입니다.

구성 지침은 *Oracle SuperCluster M7* 시리즈 소유자 안내서*:* 관리를 참조하십시오.

Oracle Enterprise Manager

Oracle Enterprise Manager 제품군은 응용 프로그램, 미들웨어, 데이터베이스 및 물리/가상 기반구조의 수명 주기 관리에 집중된 포괄적인 통합 클라우드 관리 솔루션입니다(Oracle Enterprise Manager Ops Center 사용). Oracle Enterprise Manager는 다음과 같은 관리 기술을 제공합니다.

- 응용 프로그램, 미들웨어 및 데이터베이스에 대한 세부 모니터링, 이벤트 알림, 패치 적용, 변경 관리, 연속 구성, 준수 관리 및 보고를 지원합니다.
- 데이터베이스 그룹에 대한 액세스 제어 및 감사 정책은 물론 보안 구성 설정을 중앙에서 유지 관리할 수 있게 해줍니다. 이러한 기능에 대한 액세스는 권한이 부여된 사용자로 제한하여, 관리 액세스를 통해 의무, 최소 권한 및 책임 구분을 위한 준수 위임을 지원할 수 있습니다.
- 다양한 방법, 세부 조정된 액세스 제어 및 포괄적인 감사를 통해 강력한 인증을 지원하여 SuperCluster 환경을 보안 방식으로 관리할 수 있도록 보장합니다.

자세한 내용은 Oracle Enterprise Manager 설명서(http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html)를 참조하십시오.

Oracle Enterprise Manager Ops Center(선택사항)

Oracle Enterprise Manager Ops Center는 Oracle SuperCluster의 일부 보안 특성을 관리하기 위해 사용할 수 있는 선택적인 기술입니다.

Oracle Enterprise Manager 제품군에 포함되는 Oracle Enterprise Manager Ops Center는 서버, OS, 펌웨어, 가상 시스템, 영역, 저장소 및 네트워크 패브릭에 대한 단일 관리 인터페이스를 제공하는 통합 하드웨어 관리 솔루션입니다.

Oracle Enterprise Manager Ops Center를 사용하면 물리 및 가상 시스템 모음에 관리 액세스를 지정하고, 관리자 활동을 모니터하고, 결함을 감지하고, 경보를 구성 및 관리할 수 있습니다. Oracle Enterprise Manager Ops Center에서는 알려진 구성 기준 요소, 패치 레벨 및 보안 취약점에 따라 시스템을 비교할 수 있게 해주는 다양한 보고서가 지원됩니다.

자세한 내용은 Oracle Enterprise Manager Ops Center 설명서(http://docs.oracle.com/cd/E27363_01/index.htm)를 참조하십시오.

주 - 이전 버전의 Oracle Enterprise Manager Ops Center에서는 Ops Center 소프트웨어가 SuperCluster 시스템으로부터 설치 및 실행되었습니다. Oracle Enterprise Manager Ops Center 12c 릴리스 2(12.2.0.0.0) 릴리스부터는 SuperCluster 시스템 외부의 시스템에 Ops Center 소프트웨어를 설치 및 실행해야 합니다.

보안 모니터링

준수 보고 또는 사고 대응에 관계없이 모니터링 및 감사는 IT 환경에 대해 향상된 가시성을 얻기 위해 반드시 사용해야 하는 핵심 기능입니다. 모니터링 및 감사는 해당 환경의 위험 또는 치명적인 특성에 따라 적용 강도가 결정되는 경우가 많습니다.

SuperCluster M7 시리즈 시스템은 서버, 네트워크, 데이터베이스 및 저장소 계층에서 포괄적인 모니터링 및 감사 기능을 제공함으로써 감사 및 준수 요구 사항을 지원하면서 정보에 대한 가용성을 보장합니다.

다음 절에서는 작업 부하 및 데이터베이스 모니터링 및 감사에 대해 설명합니다.

- "작업 부하 모니터링" [119]
- "데이터베이스 작업 모니터링 및 감사" [119]
- "네트워크 모니터링" [120]

작업 부하 모니터링

Oracle Solaris OS에는 관리 작업, 명령줄 호출 및 개별 커널 레벨의 시스템 호출까지 모니터할 수 있는 포괄적인 감사 기능이 포함되어 있습니다. 이 기능은 세부적인 구성이 가능하며, 전역, 영역별 및 사용자별 감사 정책까지 제공합니다.

시스템이 Oracle Solaris 영역을 사용하도록 구성된 경우, 각 영역에 대한 감사 레코드를 전역 영역에 저장하여 훼손되지 않도록 보호할 수 있습니다.

Oracle Solaris 감사는 시스템 로그(`syslog`) 기능을 사용해서 원격 수집 지점으로 감사 레코드를 전송할 수 있는 기능을 제공합니다. Oracle Solaris 감사 레코드는 많은 상업용 침입 감지 및 방지 서비스에서 분석 및 보고를 위한 추가 입력 정보로 사용될 수 있습니다.

Oracle VM Server for SPARC는 고유 Oracle Solaris 감사 기능을 사용해서 가상화 이벤트 및 도메인 관리와 연관된 작업 및 이벤트를 기록합니다.

자세한 내용은 다음 위치의 Oracle Solaris 보안 지침에서 Oracle Solaris 보안 모니터링 및 유지 관리 절을 참조하십시오.

`http://docs.oracle.com/cd/E26502_01`

데이터베이스 작업 모니터링 및 감사

Oracle Database의 세부 감사 지원을 통해 감사 레코드 생성 시간을 선택적으로 결정하는 정책을 설정할 수 있습니다. 이 기능은 다른 데이터베이스 작업에 집중할 수 있게 해주고 감사 작업과 연관된 오버헤드를 줄여줍니다.

Oracle Audit Vault and Database Firewall은 데이터베이스 감사 설정 관리를 중앙화하고 보안 저장소로의 감사 데이터 통합을 자동화합니다. 이 소프트웨어에는 권한이 부여된 사용자 작업 및 데이터베이스 구조 변경사항을 포함하여 다양한 범위의 작업들을 모니터하기 위한 내장 보고 기능이 포함되어 있습니다. Oracle Audit Vault and Database Firewall에서 생성되는 보고서는 다양한 응용 프로그램 및 관리 데이터베이스 작업에 대한 가시성을 제공하고 작업 책임을 지원할 수 있는 자세한 정보를 제공합니다.

Oracle Audit Vault and Database Firewall은 허용되지 않은 액세스 시도 또는 시스템 권한 남용을 나타낼 수 있는 활동을 사전에 감지 및 경보할 수 있게 해줍니다. 이러한 경보에는 권한이 부여된 사용자 계정 생성 또는 중요한 정보가 포함된 테이블 수정 등 시스템 및 사용자 정의 이벤트 및 조건이 모두 포함될 수 있습니다.

Oracle Audit Vault and Database Firewall Remote Monitor는 실시간 데이터베이스 보안 모니터링을 제공할 수 있습니다. 이 기능은 데이터베이스 접속을 질의해서 응용 프로그램 우회, 승인되지 않은 작업, SQL 삽입 및 기타 위협과 같은 악의적인 트래픽을 감지합니다. 이 소프트웨어는 정확한 SQL 문법 기반 방식을 사용하여 의심스러운 데이터베이스 활동을 신속하게 식별할 수 있게 해줍니다.

자세한 내용은 Oracle Audit Vault and Database Firewall 설명서(http://docs.oracle.com/cd/E37100_01/index.htm)를 참조하십시오.

네트워크 모니터링

보안 지침에 따라 네트워크가 구성된 다음에는 정기적인 검토 및 유지 관리가 필요합니다.

시스템에 대한 로컬 및 원격 액세스 보안을 유지하려면 다음 지침을 따르십시오.

- 로그를 검토하여 발생 가능한 사고를 확인하고 조직의 보안 정책에 따라 이를 아카이브합니다.
- 호스트 및 Oracle ILOM 설정이 그대로 유지되고 있는지 클라이언트 액세스 네트워크를 정기적으로 검토합니다.

자세한 내용은 다음 위치에서 Oracle Solaris OS에 대한 보안 지침을 참조하십시오.

- Oracle Solaris 11 OS – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 OS – http://www.oracle.com/goto/Solaris10/docs

소프트웨어 및 펌웨어 업데이트

SuperCluster M7 시리즈 시스템 업데이트는 QFSDP로 제공됩니다. QFSDP를 설치하면 동시에 모든 구성 요소가 업데이트됩니다. 이 방식은 Oracle에서 완전히 테스트된 소프트웨어 버전 조합에서 모든 구성 요소가 계속 실행되도록 보장합니다.

My Oracle Support에서 최신 QFSDP를 얻을 수 있습니다. http://support.oracle.com

지원되는 소프트웨어 및 펌웨어에 대한 자세한 내용은 *Oracle SuperCluster M7* 시리즈 제품 안내서를 참조하십시오. 제품 안내서에 액세스하기 위한 지침은 MOS 참고 자료 1605591.1을 참조하십시오.

주 - 반응적 유지 관리를 위해서는 오라클 고객지원센터의 조언에 따라 격리된 상태의 개별 구성 요소에 대해서만 업그레이드, 업데이트 또는 패치 적용을 수행하십시오.

색인