Oracle MiniCluster S7-2 보안 설명서

부품 번호: E78269-02
2016년 10월

부품 번호: E78269-02

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 MiniCluster S7-2 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/minicluster-s7-2/docs에서 사용할 수 있습니다

피드백

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

보안 원칙 이해

이 설명서에서는 Oracle MiniCluster S7-2 시스템에 대한 보안 환경 계획, 구성 및 유지 관리에 대한 정보를 제공합니다.

이 절에서는 다음 항목을 다룹니다.

필요한 최소 보안 작업

엔지니어링된 시스템인 MiniCluster는 기본적으로 출하 시 높은 보안 시스템으로 구성되어 다음과 같은 보안 기능을 제공합니다.

- 모든 VM(가상 머신)에 대해 완전히 자동화된 보안 제어로 미리 구성되어 있습니다.
- 암호화가 기본적으로 사용으로 설정되어 보관 중 및 전송 중인 데이터의 보안을 보장합니다.
- VM은 호스트 기반 방화벽에 따라 강화 및 최소화된 OS로 자동 구성됩니다.
- 액세스 제어를 위해서는 최소 권한의 역할 기반 액세스가 필요합니다.
- 모든 VM에는 암호화된 ZFS 스토리지가 사용됩니다.
- PKCS#11을 사용하고 FIPS를 지원하는 중앙화된 키 관리 기능이 존재합니다.
- 시스템에는 중앙화된 감사 로그가 포함된 포괄적인 감사 정책이 포함됩니다.
- 시스템 및 모든 VM이 PCI-DSS, CIS 동등 또는 DISA-STIG 보안 프로파일로 구성됩니다.
  주 – 현재 DISA-STIG 프로파일은 검토 중입니다. 비프로덕션 환경에서 테스트용으로만 DISA-STIG 프로파일을 사용하십시오.
- 확인이 간편한 준수 대시보드에서 실행을 용이하게 해주는 준수 벤치마크를 지원합니다.

MiniCluster 설치 후 보안 관리자는 다음과 같은 두 작업을 즉시 수행해야 합니다.

- Oracle ILOM 루트 비밀번호를 변경합니다. 기본 Oracle ILOM root 비밀번호 변경 [25]을 참조하십시오.

이를 제외하고는 이 설명서의 보안 정보를 검토해서 MiniCluster 보안 기능을 이해하고 확인합니다.

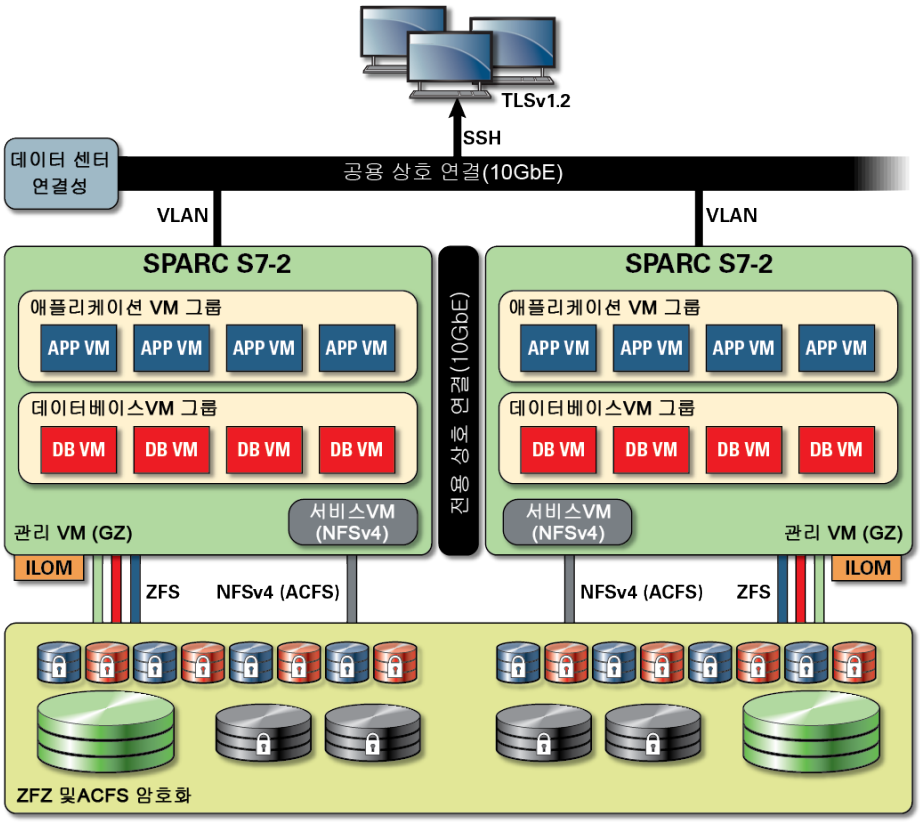
핵심 보안 원칙

MiniCluster는 애플리케이션 및 데이터베이스 통합을 위한 보안 클라우드 기반구조 플랫폼이며, 전용 컴퓨트 IaaS(Infrastructure as a Service) 기반 클라우드 서비스를 제공하기에 적합합니다. 범용 엔지니어링된 시스템으로 구성된 이 제품은 Oracle SPARC S7 프로세서의 강력한 성능, SPARC Solaris의 효율적인 가상화 기능, 전용 스토리지와 통합된 Oracle 데이터베이스의 최적화된 데이터베이스 성능이 결합되어 있습니다. 또한 10GbE 네트워크가 적용되어 클라이언트가 MiniCluster에서 실행되는 서비스에 액세스할 수 있습니다. 마지막으로 또 다른 10GbE 네트워크는 SPARC S7 서버의 가상 머신 환경과 호스트된 애플리케이션 사이의 모든 내부 통신을 지원하는 통로를 제공합니다.

SPARC S7 프로세서는 상시 하드웨어 보조 암호화 기능을 통해 MiniCluster에서 호스트되는 엔티티가 보관 중, 사용 중 및 전송 중인 데이터에 대한 고성능 데이터 보호 기능으로 자신의 정보를 보호할 수 있도록 지원합니다. 이 프로세서는 또한 Silicon Secured Memory 기능을 통해 메모리 데이터 손상 및 메모리 스크래핑과 관련된 공격을 감지 및 방지하여 애플리케이션 데이터의 무결성을 보장합니다.

기본적으로 MiniCluster는 250개 이상의 즉시 사용 가능한 보안 제어 기능으로 미리 구성되어 반드시 필요하지 않은 서비스, 포트 및 프로토콜을 사용 안함으로 설정하고, 노출된 서비스가 신뢰할 수 있는 연결만 수락하도록 구성함으로써 시스템의 공격 표면을 줄여줍니다.

이 시스템은 다양한 구성 및 배치 옵션을 지원합니다. 이 그림은 Oracle 데이터베이스 및 애플리케이션 작업 부하를 통합하는 일반적인 배치를 보여줍니다.



가상 머신 보안

MiniCluster 컴퓨트 노드 내에서의 보안은 여러 레벨에서 제공됩니다. 이러한 보안은 컴퓨트 노드의 보안 확인 부트, 격리된 가상 머신으로 실행되는 강화 및 최소화된 OS로부터 시작해서 권한 부여되지 않은 사용자 및 시스템이 작업 부하 및 데이터에 액세스하지 못하도록 방지하는 것까지 포함합니다. Oracle Solaris 영역 기술은 MiniCluster에서 가상 머신으로 사용되어 격리된 컴퓨트 환경을 호스트하고 동일한 운영체제에서 실행되는 서로 다른 애플리케이션을 효과적으로 샌드박싱하여 다른 가상 머신에서 발생하는 의도하지 않은 또는 악의적인 활동으로부터 보호합니다. 동일한 커널에서 실행됨에도 불구하고 각 Solaris 영역은 고유한 ID, 리소스, 이름 공간 및 프로세스 격리를 갖습니다. 기본적으로 Solaris 영역은 유형 1 하이퍼바이저에서 실행되는 기존의 가상 머신보다 더 적은 CPU 및 메모리 공간에서 강력한 격리 및 유연한 리소스 제어가 가능한 내장된 가상화 성능을 제공합니다. 각 가상 머신은 설치 프로세스 중 자동으로 적용되는 포괄적인 보안 제어 및 정책 세트를 정의하는 보안 프로파일로 구성됩니다. 또한 ZFS 풀 및 데이터 세트를 사용해서 가상 머신에 대해 보다 세부적인 단위로 스토리지를 분배 및 격리할 수 있으며, 고유한 보안 정책을 적용할 수 있습니다.

액세스 제어

애플리케이션 데이터, 작업 부하 및 이 모든 것들이 실행되는 기본 기반구조를 보호하기 위해 MiniCluster는 사용자 및 관리자 모두를 위해 포괄적이지만 유연한 액세스 제어 성능을 제공합니다. MiniCluster는 시스템 서비스에 액세스하는 사용자 및 애플리케이션에 대해 다양한 액세스 제어 방법을 얻기 위해 Oracle Solaris를 활용합니다. 기존 사용자 이름 및 비밀번호 쌍도 계속 널리 사용되지만, Oracle Solaris PAM(플러그인할 수 있는 인증 모듈) 구조를 사용해서 보다 강력한 인증 방법을 쉽게 통합할 수 있으며, LDAP, Kerberos 및 공개 키 인증을 사용할 수 있습니다. MiniCluster 컴퓨트 환경은 포괄적인 RBAC(역할 기반 액세스 제어) 기능을 기반으로 해서 조직이 필요에 따라 사용자 및 관리 액세스 권한을 유연하게 위임할 수 있게 해줍니다. 모두 강력한 수퍼 유저의 개념을 없앤 Oracle Solaris의 RBAC 기능을 통해 책임을 구분하고, 총체적으로 사용자 및 관리자에 대한 권한 지정을 위해 사용되는 관리 역할, 권한 부여, 미세 조정 권한 및 권한 프로파일의 개념을 지원합니다. RBAC는 Oracle Solaris SMF(서비스 관리 기능) 및 가상 머신을 포함한 다른 Oracle Solaris 서비스와 통합되어 모든 운영체제 레벨의 액세스 제어 요구를 지원하는 일관적인 구조를 제공합니다. MiniCluster는 액세스 제어 구조의 기초로 Oracle Solaris의 RBAC 기능을 활용해서 조직이 중앙화된 위치에서 운영체제 및 가상화 관리 액세스를 관리, 제어 및 감사할 수 있게 해줍니다. 모든 중요 작업은 다중 사용자 권한 부여 워크플로우로 지원되는 책임 구분 원칙을 사용해서 수행됩니다. 이 시스템에서는 두 명 이상의 사용자가 모든 보안 중요 작업을 승인해야 합니다. 총체적으로 이러한 기능을 통해 사용자의 ID 및 중요 비즈니스 작업의 처리에 대해 높은 수준의 확신을 제공할 수 있습니다.

MiniCluster 시스템의 모든 장치에는 구조적 방법(예: 네트워크 격리) 또는 패킷 필터링 및/또는 액세스 제어 목록을 사용해서 시스템에서 노출되는 서비스는 물론 물리 및 가상 장치 사이의 통신을 제한하여 서비스에 대한 네트워크 액세스를 제한하는 기능이 포함되어 있습니다. MiniCluster에는 SSH(보안 셸) 이외의 어떠한 네트워크 서비스도 인바운드 네트워크 트래픽을 수락하도록 사용으로 설정되지 않는 자체 보안 방식이 적용되어 있습니다. 사용으로 설정된 다른 네트워크 서비스는 의도적으로 Oracle Solaris 운영체제(가상 머신 또는 영역) 내부의 요청을 수신합니다. 이를 통해 모든 네트워크 서비스는 기본적으로 사용 안함으로 설정되거나, 로컬 시스템 통신만 수신하도록 설정됩니다. 조직은 자신의 요구사항에 맞게 이러한 구성을 자유롭게 사용자정의할 수 있습니다. MiniCluster는 Oracle Solaris IP 필터 기능을 사용해서 네트워크 및 전송 계층(stateful) 패킷 필터링으로 미리 구성되어 있습니다. IP 필터는 stateful 패킷 필터링, 네트워크 주소 변환 및 포트 주소 변환을 포함한 다양한 호스트 기반 네트워크 기능을 제공합니다.

데이터 보호

MiniCluster의 SPARC S7 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 애플리케이션 레벨 공격을 방지할 수 있는 Silicon Secured Memory 기술이 사용됩니다.

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 운영체제 레벨에서 암호화 하드웨어 가속화는 보안 셸, IPSec/IKE 및 암호화된 ZFS 데이터 세트에 대해 기본적으로 사용으로 설정되어 있습니다.

Oracle Database 및 Oracle Fusion Middleware는 MiniCluster에서 사용되는 Oracle Solaris 운영체제 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 애플리케이션 데이터 무결성을 보장합니다. MiniCluster는 IPsec(IP 보안) 사용을 지원하며, 공용 및 전용 네트워크를 통해 전송되는 VM 특정 및 VM 내부 통신의 기밀성 및 무결성 보호를 위해서는 IKE(인터넷 키 교환)가 권장됩니다.

MiniCluster에서 ZFS 데이터 세트 암호화는 중앙화된 Oracle Solaris PKCS#11 키 저장소를 활용해서 래핑 키를 안전하게 보호합니다. Oracle Solaris PKCS#11 키 저장소를 사용하면 모든 암호화 작업에 대해 SPARC 하드웨어 지원 암호화 가속화가 자동으로 사용됩니다. 이를 통해 Oracle은 ZFS 데이터 세트, Oracle Database TDE(투명한 데이터 암호화) 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. 데이터베이스 가상 머신은 Oracle Solaris PKCS#11 키 저장소를 활용해서 공유 전자 지갑 접근 방식을 사용하거나 ACFS 공유 스토리지에 디렉토리를 만들어서 가상 머신에 상주하는 데이터베이스 간에 전자 지갑이 공유되도록 할 수 있습니다. 각 컴퓨트 노드에서 중앙화된 공유 키 저장소를 사용하면 클러스터의 각 노드 간에 키가 동기화되기 때문에 시스템이 Oracle Grid 기반구조 기반의 클러스터화된 데이터베이스 구조에서 Oracle TDE의 키를 보다 효과적으로 관리, 유지 관리 및 순환할 수 있습니다. MiniCluster에는 또한 해당 ZFS 데이터 세트(파일 시스템/ZVOL) 레벨에서 암호화 정책 및 키 관리를 지원하는 가상 머신 및 연관된 ZFS 데이터 세트 보안 삭제 기능이 포함되어, 키 삭제를 통한 삭제 확인 기능을 제공합니다.

감사 및 준수

MiniCluster는 Oracle Solaris 감사 부속 시스템을 사용해서 감사 이벤트 정보를 수집, 저장 및 처리합니다. 각 가상 머신(비전역 영역)은 각 MiniCluster(전역 영역) 감사 저장소에 로컬로 저장되는 감사 레코드를 생성합니다. 이 접근 방법은 개별 가상 머신이 감사 정책, 구성 또는 기록된 데이터를 변경할 수 없도록 보장합니다. 이러한 작업의 책임은 클라우드 서비스 공급자에게 속하기 때문입니다.

Oracle Solaris 감사 기능은 가상 머신에서 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. 가상 머신을 사용하도록 구성된 경우, 각 가상 머신의 감사 레코드를 전역 영역에 저장하여 레코드가 손상되지 않도록 보호할 수 있습니다. 전역 영역은 또한 고유 Oracle Solaris 감사 기능을 사용해서 가상화 이벤트 및 MiniCluster 관리와 연관된 작업 및 이벤트를 기록합니다.

MiniCluster는 가상 머신에 상주하는 Oracle Solaris 런타임 환경의 준수를 평가 및 보고하는 도구를 제공합니다. 준수 유틸리티는 SCAP(Security Content Automation Protocol) 구현을 기반으로 합니다. MiniCluster에는 2개의 보안 준수 벤치마크 프로파일이 지원됩니다.

- **기본 보안 프로파일** – HIPAA, FISMA, SOX 등의 규제에 따라 설정된 보안 준수 요구사항을 보다 효과적으로 지원하도록 설정된 CIS 동등 프로파일(Center of Internet Security 벤치마크 기반)입니다.
- **PCI-DSS 프로파일** – Payment Card Industry Data Security Standard입니다.
- **DISA STIG 프로파일** – Defense Information System Agency - Security Technical Implementation Guidance 표준입니다. 이 프로파일은 기본 보안 프로파일을 기반으로 하며 추가 75 보안 제어, FIPS-140-2 암호화 및 S 암호 설정 지원을 소개합니다. 주 – 현재 이 프로파일은 검토 중입니다. 비프로덕션 환경에서 테스트용으로만 이 프로파일을 사용하십시오.

MiniCluster 관리자는 요청 시 준수 벤치마크를 실행하고 해당 환경의 준수 및 변형 상태를 확인할 수 있습니다. 이러한 프로파일링 도구는 산업 표준에 따라 강제되는 준수 요구사항에 보안 제어를 매핑합니다. 연관된 준수 보고서는 상당한 감사 시간 및 비용을 줄일 수 있습니다.

MiniCluster v.1.1.18부터 시스템에 다음 감사 기능이 포함됩니다.

- **감사자 역할** – MCMU 사용자에 대해 이 역할이 지정되면 사용자는 MCMU BUI에서 감사자의 검토 페이지에 액세스할 수 있습니다. 사용자는 다른 MiniCluster 관리 작업을 확인하거나 수행할 수 없습니다.
- **Auditor review(감사자 검토) 페이지** – 감사자 역할을 보유한 사용자에게만 표시되는 특수한 MCMU BUI 페이지입니다. 이 페이지에서는 감사 풀 상태에 액세스하고 영역별로 모든 사용자 작업에 대한 감사 레코드를 생성할 수 있습니다. 감사 보고서 생성 [36]을 참조하십시오.

보안 구성 이해

다음 항목에서는 MiniCluster 보안 제어에 대해 설명합니다.

내장 보안 프로파일

MiniCluster 초기화는 MCMU BUI 또는 CLI를 사용해서 수행됩니다. 설치 중 MCMU에서는 설치 프로그램이 다음 보안 프로파일 중 하나를 선택해야 합니다.

- **기본 보안 프로파일** – CIS(Center for Internet Security) 및 STIG(Security Technical Implementation Guidelines) 평가로 설정된 벤치마크와 동등하거나 이와 비슷한 요구사항을 충족합니다.
- **PCI-DSS 프로파일** – Payment Card Industry Security Standards Council에서 정의된 PCI DSS(Payment Card Industry Data Security Standard) 표준을 준수합니다.
- **DISA STIG 프로파일** – Defense Information System Agency - Security Technical Implementation Guidance 표준입니다. 이 프로파일은 기본 보안 프로파일을 기반으로 하며 추가 75 보안 제어, FIPS-140-2 암호화 및 eeprom 암호 설정 지원을 소개합니다. 주 – 현재 이 프로파일은 검토 중입니다. 비프로덕션 환경에서 테스트용으로만 이 프로파일을 사용하십시오.

선택한 정책을 기준으로 MCMU는 250개 이상의 보안 제어로 전역 영역 및 비전역 영역을 구성합니다.

초기화 후 가상 머신이 생성될 때 MCMU에서는 각 가상 머신에 대해 보안 프로파일 중 하나를 선택해야 합니다. 보안 요구사항에 따라 가상 머신에서 보안 프로파일을 혼합해서 사용할 수 있습니다.

▼ VM 보안 프로파일 확인(CLI)

영역 및 가상 머신에 대해 구성된 보안 프로파일을 확인 또는 식별하려면 다음 절차를 따릅니다.

주 - 이 절차를 수행하려면 `root` 역할이 있는 사용자 계정으로 시스템에 액세스해야 합니다.

주 - 전역 영역에 지정된 보안 프로파일을 식별하려면 MCMU BUI에서 System Setting(시스템 설정) -> User Input Summary(사용자 입력 요약)를 확인합니다. 보안 프로파일은 페이지 하단에 표시됩니다.

1. **전역 영역에 `mcinstall`로 로그인합니다.**

   시스템 액세스 방법에 대한 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

2. **`root` 역할을 맡습니다.**

   예:

   ```
   # su root
   ```

3. **로그 파일 이름에서 해당 VM을 찾습니다.**

   이 예에서는 각 VM에 대해 하나의 로그 파일이 존재합니다.

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **확인 로그 파일을 봅니다.**

   로그 파일의 마지막 라인을 봅니다. `(PCI-DSS)`가 표시된 경우 VM의 보안 프로파일은 PCI-DSS입니다. 프로파일이 나열되지 않은 경우 VM의 보안 프로파일은 CIS 동등입니다.

   - PCI-DSS 프로파일에서 VM의 마지막 22개 라인 예:

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured

     (PCI-DSS) Checking audit configuration (user audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (non-attributable audit flags):
     Passed/Configured

     (PCI-DSS) Checking audit configuration (audit_binfile plugin):
     Passed/Configured
     ```

```
(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- CIS 동등 프로파일에서 VM의 마지막 22개 라인 예:

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

데이터 보호

다음 항목에서는 MiniCluster 데이터 보호 기술에 대해 설명합니다.

ZFS 데이터 세트 암호화로 데이터 보호

MiniCluster에서 보관 중인 데이터 보호는 ZFS 데이터 세트 암호화를 사용해서 자동으로 구성됩니다. 암호화는 다음과 같이 구성됩니다.

- 모든 ZFS 데이터 세트는 루트 및 스왑 파일 시스템을 포함하는 가상 머신에서 암호화됩니다.
- 모든 ZFS 데이터 세트는 루트 및 스왑 파일 시스템을 제외하고 전역 영역에서 암호화됩니다.

암호화 키를 통해 암호화 구성을 확인할 수 있습니다. ZFS 데이터 세트 암호화 키 보기 (BUI) [19]를 참조하십시오.

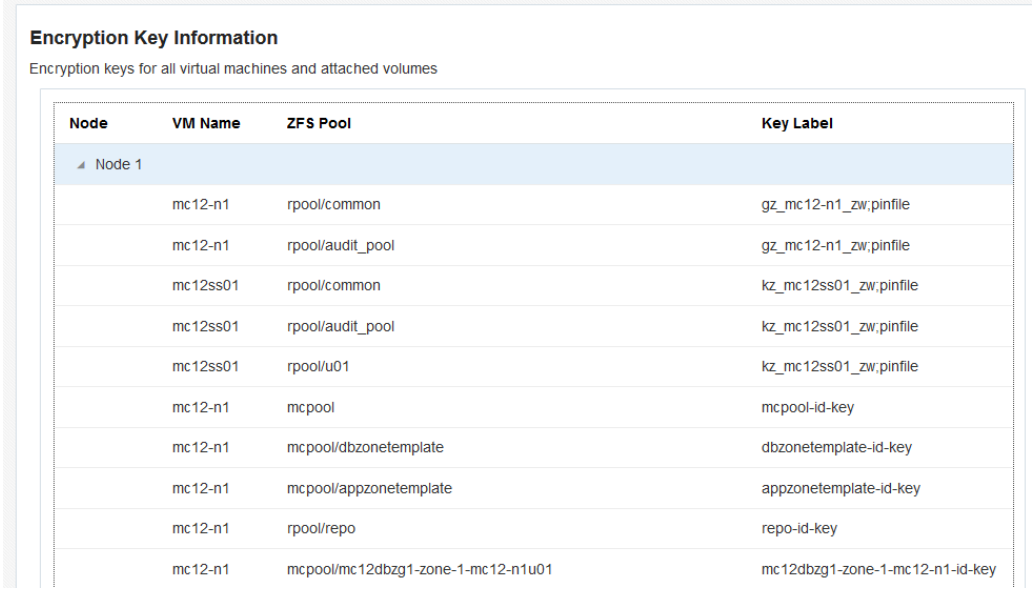
▼ ZFS 데이터 세트 암호화 키 보기(BUI)

이 절차를 수행하여 암호화 키 세부정보를 확인합니다.

1. **MCMU BUI에 액세스합니다.**

   MCMU BUI 액세스 방법에 대한 자세한 내용은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

2. **탐색 패널에서 System Settings(시스템 설정) -> Security(보안)를 선택합니다.**
   세부정보를 표시하려면 노드를 누릅니다.



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
◢ Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

보안 셸 서비스

사용자가 MiniCluster 컴퓨트 노드(전역 영역) 및 가상 머신 인스턴스(비전역 영역)에 안전하게 로그인하도록 하려면 MiniCluster에서 SSH 네트워크 프로토콜을 사용해야 합니다.

사용자가 SSH를 사용해서 처음 로그인하면 시스템이 해당 사용자에 대해 새로운 SSH 키 쌍을 자동으로 생성합니다.

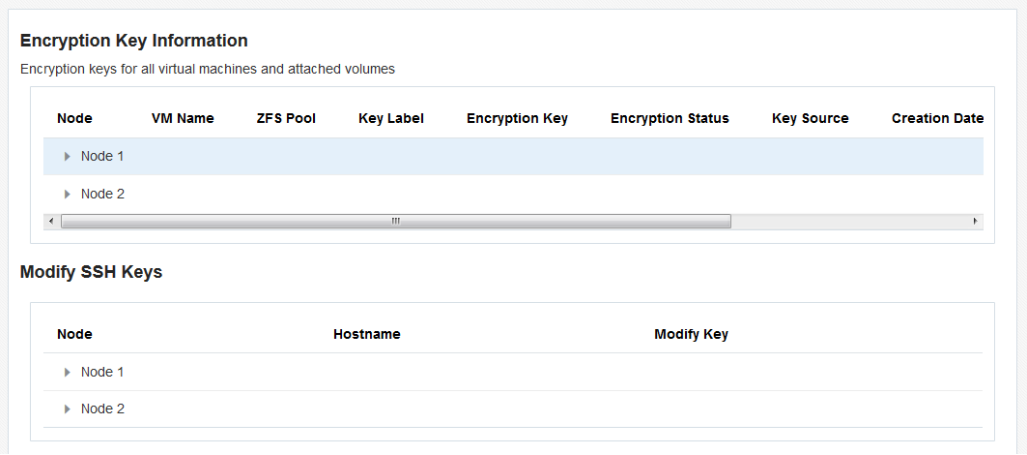
▼ SSH 키 변경(BUI)

이 절차에 따라 해당 구성 중 하나를 사용해서 영역 또는 VM에 대한 SSH 키를 변경합니다.

- 비밀번호 없이 SSH를 권한 부여하도록 새 키 삽입 - VM 사용자 이름, VM 머신 이름 및 RSA 공개 키를 입력해야 합니다.
- VM에 대한 새 키 자동 생성

주 - MCMU CLI를 사용해서 이 절차를 수행하려면 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

1. **MCMU BUI에 액세스합니다.**
2. **탐색 패널에서 System Settings(시스템 설정) -> Security(보안)를 선택합니다.**



3. **Modify SSH Keys(SSH 키 수정) 패널에서 표시를 확장하려면 노드를 누릅니다.**

4. **변경하려는 VM에 대해 Select(선택)를 누릅니다.**

5. **드롭다운 메뉴에서 옵션을 선택하고 Next(다음)를 누릅니다.**
   옵션은 다음과 같습니다.
   - 새 키를 입력하여 비밀번호 없는 SSH 사용 권한 부여
   - 머신에 대한 새 키 자동 생성
6. **Next(다음)를 누릅니다.**
7. **비밀번호 없이 SSH를 권한 부여하도록 선택한 경우, 다음 정보를 입력한 후 Next(다음)를 누릅니다.**
   - 머신의 사용자 이름
   - 머신의 호스트 이름
   - 머신의 RSA 공개 키
8. **Setup SSH(SSH 설정)를 누릅니다.**
   변경사항이 적용됩니다.

IPsec를 사용하여 통신 보안

영역 간 IP 기반 통신 및 네트워크를 통과하는 NFS 트래픽의 기밀성 및 무결성을 보호하기 위해서는 IPsec(IP 보안) 및 IKE(인터넷 키 교환)를 사용하는 것이 좋습니다. IPsec는 네트워크 레벨 피어 인증, 데이터 원점 인증, 데이터 기밀성, 데이터 무결성 및 재생 보호를 지원하기 때문에 권장됩니다. Oracle MiniCluster 플랫폼에 사용할 경우 IPsec 및 IKE는 하드웨어 보조 암호화 가속화를 자동으로 사용할 수 있기 때문에, 이 네트워크 채널을 통과하는 민감한 정보 보호를 위해 암호화를 사용할 때 발생하는 성능 영향을 최소화할 수 있습니다.

▼ IPsec 및 IKE 구성

IPsec를 구성하려면 먼저 통신 피어 사이에 사용되는 특정 호스트 이름 및/또는 IP 주소를 정의해야 합니다.

이 절차의 예에서 IP 주소 10.1.1.1 및 10.1.1.2는 단일 테넌트로 작동 중인 2개의 Solaris 비전역 영역을 지정하기 위해 사용됩니다. 이러한 두 주소 사이의 통신은 IPsec로 보호됩니다. 이 예는 IP 주소 10.1.1.1과 연관된 비전역 영역의 관점에서 가져온 예입니다.

지정된(가상 머신) 비전역 영역 쌍 사이에 IPsec 및 IKE를 구성하고 사용하려면 다음 단계를 따릅니다.

1. **IPsec 보안 정책을 정의합니다.**

통신 영역 쌍 사이에 적용되는 보안 정책을 정의합니다.

이 예에서는 10.1.1.1과 10.1.1.2 사이의 모든 네트워크 통신이 암호화됩니다.

```
{laddr 10.1.1.1 raddr 10.1.1.2}
ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
```

2. **`/etc/inet/ipsecinit.conf` 파일에 정책을 저장합니다.**

3. **IPsec 정책 구문이 올바른지 확인합니다.**

   예:

   ```
   # ipsecconf -c -f ipsecinit.conf
   ```

4. **IKE(인터넷 키 교환) 서비스를 구성합니다.**

   `/etc/inet/ike/config` 파일에서 호스트 및 알고리즘 설정에 따라 서비스를 구성합니다.

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5

   auth_alg sha256 encr_alg aes } }
   ```

5. **미리 공유한 키를 구성합니다.**

   IPsec를 사용으로 설정하려면 서로 인증할 수 있도록 두 피어 노드에 키 자료가 공유되어야 합니다.

   Oracle Solaris IKE 구현에는 미리 공유된 키 및 인증서를 포함한 여러 키 유형이 지원됩니다. 단순성을 위해 이 예에서는 /`etc/inet/secret/ike.preshared` 파일에 저장된 미리 공유된 키를 사용합니다. 하지만 더 엄격한 형식의 인증을 사용하길 원하는 조직의 경우 그렇게 할 수도 있습니다.

   /etc/inet/secret/ike.preshared 파일을 편집하고 미리 공유된 키 정보를 입력합니다. 예를 들면 다음과 같습니다.

   ```
   {
   localidtype IP
   localid 10.1.1.1
   remoteid type IP
   key "This is an ASCII phrAz, use strOng p@sswords"
   }
   ```

6. **두 피어 모두에서 IPsec 및 IKE 서비스를 사용으로 설정합니다.**

   암호화된 통신을 가능하게 하려면 먼저 두 통신 피어 모두에서 서비스를 사용으로 설정해야 합니다.

   예:

   ```
   # svcadm enable svc:/network/ipsec/policy:default
   # svcadm enable svc:/network/ipsec/ike:default
   ```

액세스 제어

다음 항목에서는 MiniCluster에서 사용 가능한 액세스 제어 기능을 다룹니다.

▼ 기본 Oracle ILOM `root` 비밀번호 변경

시스템은 두 노드 모두 Oracle ILOM 루트 계정에 기본 비밀번호가 지정된 상태로 제공됩니다. 이렇게 하면 예측 가능한 초기 액세스 계정을 사용해서 설치 프로세스를 수행할 수 있습니다. 최적의 보안을 보장하기 위해서는 설치 후 즉시 기본 비밀번호를 변경하십시오.

1. **노드 1에서 Oracle ILOM에 `root`로 로그인합니다.**

   `ssh` 명령을 사용해서 Oracle ILOM에 연결합니다.

   Oracle ILOM의 호스트 이름을 가져오려면 유틸리티 BUI에서 System Settings(시스템 설정) -> System Information(시스템 정보)을 선택합니다. 호스트 이름은 ILOM 열 아래에 나열됩니다.

   구문:

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

   기본 Oracle ILOM 루트 비밀번호: welcome1을 입력합니다.

2. **Oracle ILOM `root` 비밀번호를 변경합니다.**

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: ***********
```

3. **단계를 반복해서 노드 2에서 Oracle ILOM `root` 비밀번호를 변경합니다.**

4. **새 비밀번호를 사용해서 Oracle Engineered Systems Hardware Manager를 업데이트합니다.**

   Oracle MiniCluster S7-2 관리 설명서 의 “구성요소 비밀번호 업데이트”를 참조하십시오.

▼ EEPROM 비밀번호 구성

각 MiniCluster 노드에는 EEPROM(OpenBoot PROM이라고 하는 경우도 있음)이 있습니다. EEPROM은 시스템 부트를 원활하게 해주는 몇 가지 구성 매개변수와 드라이버를 포함하는 낮은 레벨의 펌웨어입니다. 기본적으로 EEPROM 비밀번호 기능은 사용 안함으로 설정되어 있습니다.

보안 환경에서 다음 절차에 따라 비밀번호 기능을 사용으로 설정하고 비밀번호를 설정할 수 있습니다. 그러면 비밀번호가 자동으로 사용으로 설정되며 두 노드에 적용됩니다.

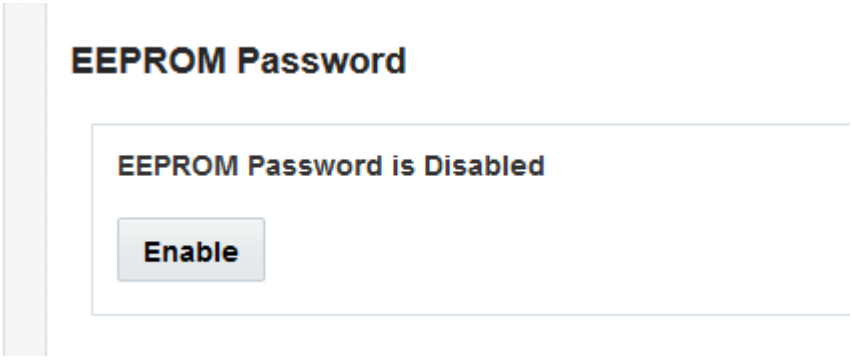
이 절차는 OpenBoot `ok` 프롬프트에서 비밀번호를 설정하거나 `eeprom` 명령을 사용하여 Oracle Solaris에서 비밀번호를 설정하는 이전 방법을 대체합니다.

주의 - 비밀번호를 기억해야 합니다. 비밀번호를 잊을 경우 지원 서비스에 연락하여 시스템을 다시 부트 가능한 상태로 설정해야 합니다.

주 - 이 절차에서는 MCMU BUI에서 비밀번호를 설정하는 방법에 대해 설명합니다. 또는 `mcmu security -e` 명령을 사용할 수도 있습니다.

1. **기본 관리자(예: `mcinstall`)로 MCMU에 로그인합니다.**

2. **탐색 패널에서 System Settings(시스템 설정) -> Security(보안)를 선택합니다.**



3. **다음 작업 중 하나를 수행합니다.**

   - 기능을 사용으로 설정한 후 비밀번호를 설정하려면 Enable(사용)을 누르고 비밀번호를 두 번 입력한 다음 Set Password(비밀번호 설정)를 누릅니다.
   - 기능을 사용 안함으로 설정하려면 Disable(사용 안함), Confirm(확인)을 차례로 누릅니다.
   - 기존 비밀번호를 변경하려면 Change Password(비밀번호 변경)를 누르고 새 비밀번호를 두 번 입력한 다음 Update(업데이트)를 누릅니다.

사용자 프로비전

MiniCluster 설치 중에는 설치 프로세스에 따라 `mcinstall`이라는 첫번째 MCMU 사용자를 만들고 등록해야 합니다. 전자메일 주소 및 전화 번호를 포함한 사용자의 통계 정보가 수집됩니다. `mcinstall` 사용자는 첫번째 기본 관리자 계정입니다. 첫번째 `mcinstall` 로그인 시, `mcinstall`이 보안 프로파일과 연관된 Oracle Solaris 비밀번호 정책에 따라 새 비밀번호를 만들어야 합니다.

`mcinstall` 사용자 등록 중에는 MCMU 관리책임자 역할을 수행할 사용자를 지정해야 합니다. 관리책임자는 이름 및 전자메일 주소로만 식별됩니다. 관리책임자는 MCMU 사용자가 아니며, 로그인 자격 증명을 갖지 않습니다.

관리책임자 및 mcinstall 사용자는 실제 사용자 이름 및 유효한 전자메일 주소와 연관되어 있습니다.

새 MCMU 사용자가 프로비전되면 각 사용자 계정에 기본 관리자 또는 보조 관리자의 역할이 지정됩니다(“역할 기반 액세스 제어 ” [29] 참조). 새 계정을 사용으로 설정하려면 `mcinstall` 사용자 및 관리책임자가 모두 전자메일을 수신하는 URL을 통해 새 사용자 계정을 승인해야 합니다(“MCMU 사용자 승인 프로세스” [28] 참조). 첫번째 로그인 후 사용자는 MCMU 비밀

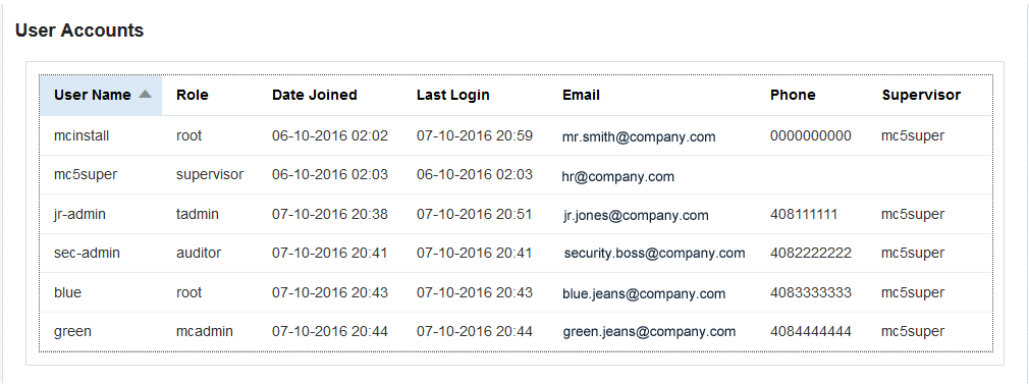
번호 정책에 맞는 비밀번호를 설정해야 합니다. “사용자 인증 및 비밀번호 정책” [30]을 참조하십시오.

MCMU 사용자 승인 프로세스

모든 MCMU 사용자 계정에는 MCMU 관리책임자 및 기본 관리자의 2명 승인이 필요합니다. 이 프로세스는 다음과 같이 작동합니다.

1. 예정 사용자(또는 이 사용자를 대신하는 MCMU 관리자)는 MCMU 등록 페이지에 액세스해서 다음과 같은 필수 세부정보를 제공합니다.
   - MCMU 사용자 이름
   - 전자메일 주소
   - 전체 이름
   - 전화 번호
   - MCMU 역할
2. MCMU는 MCMU 관리책임자 및 기본 관리자에게 승인 또는 거부를 요청하는 전자메일을 전송합니다. 전자메일에는 MCMU 승인/거부 기능에 대한 URL이 포함되며, 고유 키 식별자가 포함됩니다.
3. 관리책임자 및 기본 관리자가 모두 계정을 승인하면, 사용자 계정이 사용으로 설정되고, MCMU가 새 사용자에게 계정 활성화를 확인하는 전자메일을 전송합니다. 사용자에게는 MCMU BUI 또는 CLI를 통해 액세스할 수 있는 MCMU 계정이 수신됩니다. 사용자에게는 또한 Oracle Solaris 사용자 계정이 수신됩니다. 사용자가 회사 LDAP에 존재하고 MiniCluster가 LDAP 클라이언트로 구성된 경우, 사용자는 Oracle Solaris 계정에 대해서만 LDAP를 사용할 수 있습니다.

등록된 모든 사용자는 MCMU 저장소에 저장됩니다. MCMU 관리자는 MCMU System Settings(시스템 설정) -> User Accounts(사용자 계정)를 통해 사용자의 역할 및 관리책임자를 포함해서 사용자를 확인할 수 있습니다. 예:



이 섹션의 다음 항목에서는 이러한 작업을 수행하는 방법에 대해 설명합니다.

역할 기반 액세스 제어

MiniCluster에는 `root` 사용자가 없습니다. 대신 root는 역할이며, 기본 관리자로 등록된 MCMU 사용자에게 지정됩니다.

MCMU 사용자를 만들 때는 다음 역할 중 하나를 사용자에게 지정합니다.

- **기본 관리자(`root` 역할)** – `root` 역할은 모든 컴퓨트 노드, 네트워크, 데이터베이스 및 스토리지를 포함해서 MiniCluster 시스템의 기본 관리자가 갖고 있는 권한을 정의합니다. `root` 역할이 있는 사용자는 어떠한 제약 조건도 없이 모든 설치 및 모든 중요 관리 작업을 수행할 수 있습니다. 기본 관리자는 신규 기본 및 보조 관리자를 포함해서 사용자 추가 및 삭제를 승인하고 작업을 위임할 수 있습니다. 사용자는 자신의 고유 자격 증명으로 로그인해야 합니다. 수행되는 모든 작업은 역할 식별자가 아닌 사용자 식별자를 기준으로 기록 및 감사됩니다.
- **보조 관리자(`mcadmin` 역할)** – 이 역할은 MiniCluster 도메인 및 비전역 영역의 보조 관리자가 갖고 있는 권한을 정의합니다. 기본적으로 이 역할은 MCMU에 읽기 전용으로만 액세스할 수 있습니다. 수행되는 모든 작업은 역할 식별자가 아닌 사용자 식별자를 기준으로 기록 및 감사됩니다.
- **테넌트 관리자(`tadmin` 역할)** – 이 역할은 MiniCluster VM의 관리자가 갖고 있는 권한을 정의합니다. 이 역할은 애플리케이션 설치 및 배치를 지원하는 일상적인 관리 작업과 관련된 VM 관리자의 권한을 정의합니다. 모든 작업은 역할 식별자가 아닌 사용자 식별자를 기준으로 감사됩니다.
- **감사자(`auditor` 역할)** – 이 역할을 보유한 사용자만 MCMU BUI 감사 검토 페이지에 액세스하여 감사 풀 상태를 확인하고 사용자 작업에 대한 보고서를 생성할 수 있습니다. 이 역할을 보유한 사용자만 감사 검토 페이지에 액세스할 수 있습니다. 감사자는 감사 페이지를 제외한 MCMU에 액세스할 수 없으며 커널 영역 또는 VM에도 로그인할 수 없습니다.

사용자 계정

MiniCluster에는 이 표에 나열된 사용자 계정이 포함됩니다.

사용자	비밀번호	역할	설명
`mcinstall`	비밀번호는 설치 중에 구성됩니다. MCMU를 통해 재설정 및 변경할 수 있습니다.	`root`	설치 프로세스에서는 `mcinstall`을 MCMU 기본 관리자로 만들고 비밀번호를 만들어야 합니다. 이 계정은 MCMU용 기본 관리자로 사용됩니다. 이 사용자 계정은 다음과 같은 작업에 사용됩니다. ■ `installmc`를 실행해서 설치 시 시스템 초기화를 수행합니다. ■ MCMU BUI 및 `mcmu` CLI를 통해 VM을 비롯하여 시스템을 관리합니다.

사용자	비밀번호	역할	설명
			■ 수퍼 유저 권한을 얻기 위해 애플리케이션 VM 및 전역 영역과 커널 영역에서 `root` 역할(root에서 `su`)을 맡습니다.
MCMU 관리책임자 – 설치 시 결정된 계정 이름	해당 없음	해당 없음	MiniCluster 소프트웨어에서 관리책임자 사용자는 유일한 사용자 이름 및 전자메일 주소입니다. 로그인 자격 증명이 아닙니다. 이 계정을 사용하면 MCMU 사용자 승인 프로세스에서 두번째 레벨을 제공할 수 있습니다. 이 사용자에게는 새 MCMU 사용자가 생성될 때마다 전자메일이 수신됩니다. 사용자 계정을 사용으로 설정하기 위해서는 관리책임자 및 기본 관리자가 새 사용자를 승인해야 합니다. 이 계정을 사용하면 기본 관리자 이외의 사용자를 관리책임자로 지정하여 MCMU 사용자 승인 프로세스에서 두번째 계층을 제공할 수 있습니다.
(선택사항) 테넌트 관리자 – 사용자 등록 시 결정된 계정 이름	최초 로그인 시 결정됩니다.	`tadmin`	이 사용자는 VM에서만 모든 사후 설치 작업을 수행할 수 있습니다. 이 사용자는 전역 또는 커널 영역에 액세스할 수 없으며 MCMU BUI 또는 CLI를 실행할 수 없습니다.
(선택사항) 보조 관리자 – 사용자 등록 시 결정된 계정 이름	최초 로그인 시 결정됩니다.	`mcadmin`	MCMU 사용자가 만들어져 보조 관리자로 지정되면 비전역 영역에 대해 읽기 전용 액세스 권한을 가집니다.
`oracle`	비밀번호는 `mcinstall` 비밀번호와 동일합니다.	`root`	이 사용자 계정은 다음과 같은 작업에 사용됩니다. ■ 필요에 따라 데이터베이스, 데이터 및 다른 계정으로 데이터베이스 VM을 구성할 수 있는 데이터베이스 VM에 대한 초기 로그인 계정으로 사용됩니다. ■ 수퍼 유저 권한을 얻기 위해 데이터베이스 VM에서 루트 역할(루트에서 `su`)을 맡습니다.

최초 로그인 시 사용되는 기본 MCMU 비밀번호는 `welcome1`입니다. `welcome1`을 입력한 다음에는 사용자가 비밀번호 정책에 맞는 새 비밀번호를 만들어야 합니다. “사용자 인증 및 비밀번호 정책” [30]을 참조하십시오.

모든 MCMU 사용자가 수행하는 모든 작업은 해당 사용자의 식별자를 기준으로 기록됩니다. 감사 보고서에 대한 자세한 내용은 감사 및 준수 보고 [35]를 참조하십시오.

주 - MCMU 사용자 계정은 애플리케이션 및 데이터베이스 사용과 같은 일반적인 시스템 용도로 사용되지 않습니다. 이러한 사용자 계정은 Oracle Solaris, 애플리케이션, VM의 데이터베이스 및 사이트의 이름 서비스를 통해 관리됩니다.

사용자 인증 및 비밀번호 정책

MiniCluster에 프로비전된 모든 사용자에게는 보안 프로파일에 따라 적용되는 엄격한 암호 정책 및 암호 암호화에 따라 역할이 지정됩니다.

기본 보안 정책에는 다음과 같은 MCMU 비밀번호 요구사항이 적용됩니다.

- 최소 14자를 포함해야 합니다.

- 최소 1개의 숫자를 포함해야 합니다.
- 최소 1개의 대문자를 포함해야 합니다.
- 이전 비밀번호와 3자 이상 달라야 합니다.
- 이전 10개 비밀번호와 일치하지 않아야 합니다.

모든 사용자는 사용자의 고유 비밀번호만 사용해서 Oracle Solaris 계정에 로그인합니다.

▼ Oracle Solaris 사용자 역할 확인

1. **MiniCluster 전역 영역에 로그인하고 루트 역할을 맡습니다.**
   자세한 내용은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

2. **사용 가능한 역할 목록을 확인합니다.**

```
# logins -r
```

3. **인증에 필요한 사용자 역할 및 비밀번호를 확인합니다.**

```
# grep root /etc/user_attr
root::::audit_flags=lo\:no;type=role;roleauth=user
mcinstall::::auths=solaris.system.maintenance;roles=root
```

VM 보안 삭제

MCMU 기본 관리자만 VM 및 VM 그룹을 삭제할 수 있습니다. VM 구성요소가 삭제되면 해당 키가 자동으로 삭제되고 기본 관리자에게 전자메일이 전송됩니다.

이 기능을 확인하려면 VM 구성요소를 삭제하기 전에 MCMU BUI에 기본 관리자로 로그인하고, 암호화 키를 봅니다(System Settings(시스템 설정) -> Security(보안)). VM 구성요소를 삭제하고 키를 다시 봅니다. 삭제된 구성요소에 대한 VM 및 연관된 키 레이블이 더 이상 표시되지 않습니다.

▼ 호스트 기반 방화벽 규칙 확인

전역 영역, 커널 영역, 비전역 영역을 포함한 모든 컴퓨트 환경은 IPFilter 방화벽으로 자동으로 구성됩니다. 수동 작업은 필요하지 않습니다.

사용 중인 IPFilter를 확인하려면 다음 단계를 수행합니다.

1. **노드 1에서 전역 영역에 `mcinstall`로 로그인하고 `root` 역할을 맡습니다.**

Oracle ILOM 로그인 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. IPFilter 구성을 확인합니다.

`/etc/ipf/ipf.conf` 파일의 규칙이 다음 화면 출력과 일치하는지 확인합니다.

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. IPF 서비스가 온라인 상태인지 확인합니다.

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
```

```
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **방화벽 규칙을 변경하지 않아도 데이터베이스 및 애플리케이션에 액세스할 수 있는지 확인합니다.**

▼ 확인된 부트 환경 확인

Oracle Solaris 확인된 부트는 맬웨어 방지 및 무결성 기능으로, 악의적으로 또는 실수로 수정된 중요 부트 및 커널 구성요소가 도입되는 위험을 줄여줍니다. 이 기능은 펌웨어, 부트 시스템 및 커널의 공장 서명 암호화 서명을 확인합니다.

기본적으로 MiniCluster 전역 영역은 Oracle Solaris 확인된 부트를 사용해서 구성됩니다. 시스템이 확인된 부트로 구성되었는지 확인하려면 다음 단계를 수행합니다.

1. **노드 중 하나에서 Oracle ILOM에 로그인합니다.**

   Oracle ILOM 로그인 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

2. **Oracle ILOM에서 확인된 부트 구성을 확인합니다.**

   `boot_policy`가 `warning`으로 설정되었는지 확인합니다.

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **확인된 부트 정책 설정을 확인합니다.**

   `module_policy`가 `enforce`로 설정되었는지 확인합니다.

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **호스트 콘솔을 시작해서 전역 영역에 액세스합니다.**

   `mcinstall`로 로그인합니다.

```
-> start /HOST/console
```

```
Are you sure you want to start /HOST/console (y/n)? y

Serial console started.  To stop, type #.

Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **전역 영역에서 시스템이 확인된 부트 구성으로 부트되었는지 증거를 확인합니다.**

   `messages` 파일에서 `NOTICE: Verified boot enabled; policy=warning` 문자열을 찾습니다.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

▼ 공유 스토리지에 대한 액세스 제한

MiniCluster에는 SSD와 HDD가 혼합된 스토리지 배열이 포함되어 있습니다. VM에 공유 스토리지를 제공하도록 HDD를 구성할 수도 있습니다.

MiniCluster에는 공유 스토리지 격리 기능(전역 및 커널 영역에만 적용되는 공유 스토리지를 원활하게 격리시키는 토글 스위치)이 포함되어 있습니다. 이를 통해 보안 및 준수가 사용으로 설정된 VM 그룹 환경이 전역 및 커널 영역과 파일을 공유하지 않도록 격리시킬 수 있습니다. 그러면 VM 그룹이 더 이상 NFS 마운트에 연결되지 않으며 NFS 서비스가 사용 안함으로 설정됩니다.

높은 보안 환경에서는 데이터베이스 VM 및 애플리케이션 VM에 대해 공유 스토리지를 사용으로 설정하지 마십시오. 공유 스토리지가 사용으로 설정된 경우 파일 시스템이 VM에 읽기 전용으로 액세스할 수 있어야 합니다. 공유 스토리지를 사용 또는 사용 안함으로 설정하는 방법에 대한 지침은 *Oracle MiniCluster S7-2* 관리 설명서(`http://docs.oracle.com/cd/E69469_01`)를 참조하십시오.

`/sharedstore` 디렉토리는 공유 스토리지에 대한 마운트 지점입니다.

- **보안 요구에 따라 다음과 같은 권장 사항을 염두에 두고 공유 스토리지를 구성하십시오.**
  - 공유 스토리지를 데이터베이스 VM 및 애플리케이션 VM에 사용할 수 없는지 또는 읽기 전용인지 확인합니다.
  - 프로덕션 배치 시 공용 네트워크 또는 클라이언트 액세스 네트워크에 대한 직접 액세스를 통해 모든 커널 영역에 액세스할 수 없는지 확인합니다. 모든 직접 액세스와 공용 네트워크 또는 클라이언트 액세스를 통한 공유 스토리지 서비스 사용은 종료되어야 합니다. 가상 머신에서 NFS를 통해 `/sharedstore` 파일 시스템에 액세스해야 하는 경우 IPSEc/IKE 채널을 사용하는 것이 좋습니다.

감사 및 준수 보고

다음 항목에서는 MiniCluster에서 제공되는 감사 및 준수 보고 기능에 대해 설명합니다.

▼ 감사 정책 확인

감사 정책은 준수 프로파일(기본 CIS 동등 또는 PCI-DSS) 선택 시 전역 영역 및 비전역 영역을 설치하는 동안 구성됩니다.

감사 정책이 사용으로 설정되었는지 확인하려면 다음 단계를 수행합니다.

1. **전역 영역에 `mcinstall`로 로그인하고 `root` 역할을 맡습니다.**
   Oracle ILOM 로그인 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **감사 서비스가 온라인 상태인지 확인합니다.**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **감사 플러그인이 활성 상태인지 확인합니다.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **활성 감사 정책을 확인합니다.**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **모든 역할이 `cusa` 감사 정책에 대해 캡처되었는지 확인합니다.**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ 감사 로그 검토

1. **전역 영역에 `mcinstall`로 로그인하고 `root` 역할을 맡습니다.**
   Oracle ILOM 로그인 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **표시된 대로 `auditreduce` 명령을 사용합니다.**
   감사 로그 보기 구문은 다음과 같습니다.

```
auditreduce -z vm_name audit_file_name | praudit -s
```

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```

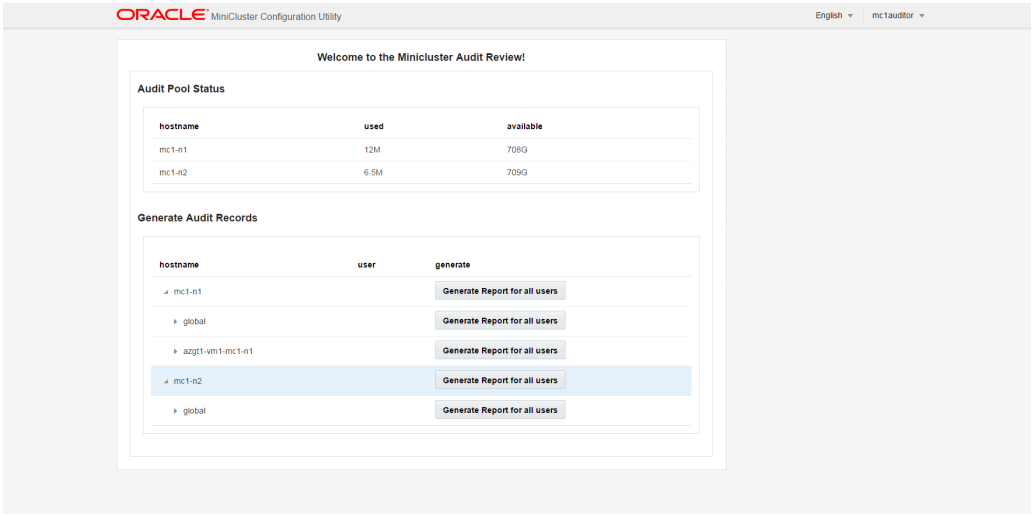
▼ 감사 보고서 생성

다음 절차에 따라 노드 또는 개별 VM과 전역 영역에 대한 감사 보고서를 생성할 수 있습니다.

1. **감사자 역할을 보유한 지정된 사용자로 MCMU에 로그인합니다.**
   MCMU 사용자 및 역할에 대한 자세한 내용은 *Oracle MiniCluster S7-2* 관리 설명서(http://docs.oracle.com/cd/E69469_01)를 참조하십시오.

2. **탐색 패널에서 System Settings(시스템 설정) -> Security(보안)를 선택합니다.**
   Audit Review(감사 검토) 페이지가 표시됩니다.

주 - 감사자 역할이 지정된 MCMU 사용자만 이 페이지를 표시할 수 있습니다.

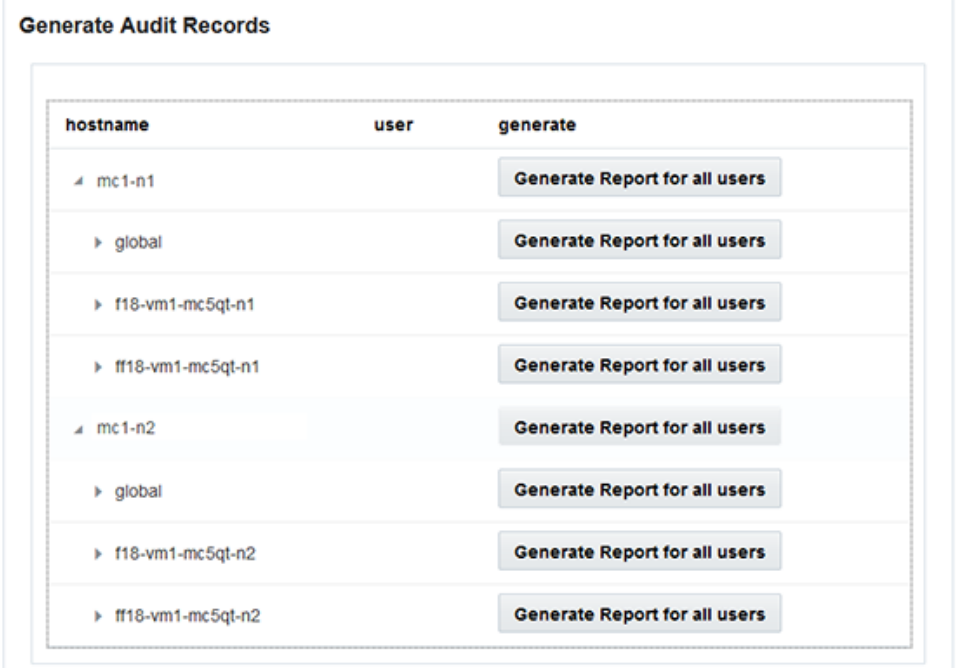


3. **Audit Pool Status(감사 풀 상태) 섹션을 확인합니다.**
   이 섹션에는 각 노드의 감사 풀에 대해 사용된 공간 및 사용 가능한 공간이 나열됩니다.

4. **전체 노드에 대한 보고서를 생성하려면 노드 중 하나에 대해 Generate(생성) 버튼을 누르고 6단계로 이동합니다.**
   또는 특정 VM이나 영역에 대한 보고서를 생성할 수도 있습니다. 5단계를 참조하십시오.

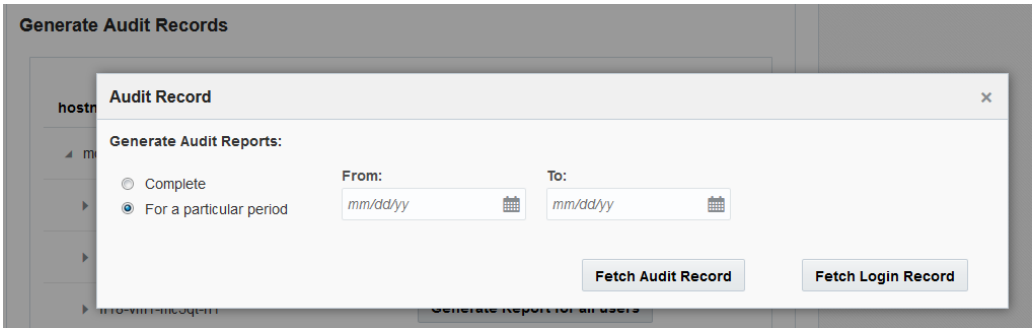
5. **특정 VM 또는 전역 영역에 대한 보고서를 생성하려면 다음 단계를 수행합니다.**

a. 노드 옆에 있는 삼각형을 눌러 뷰를 확장합니다.



b. VM 또는 전역 영역의 경우 **Generate Report for all users(**모든 사용자에 대해 보고서 생성**)**를 누릅니다.

6. **Audit Record(**감사 레코드**)** 대화 상자에서 감사 레코드 매개변수를 구성합니다.



옵션은 다음과 같습니다.

- **Complete(전체)** – 모든 감사 레코드를 포함하는 보고서를 생성하려는 경우 선택합니다.
- **For a particular period(특정 기간)** – 특정 기간을 지정하려는 경우 선택한 후 시작 및 종료 날짜를 입력합니다.

7. **인출 버튼 중 하나를 누릅니다.**

   옵션은 다음과 같습니다.

   - **Fetch Audit Record(감사 레코드 인출)** – 전체 감사 레코드를 생성합니다.
   - **Fetch Login Record(로그인 레코드 인출)** – 로그인, 로그아웃, 사용자 동작 등 사용자 작업을 생성합니다.

8. **Click Here(여기 누르기) 버튼을 누르고 XML 파일 다운로드를 선택합니다.**

   감사 분석 애플리케이션(예: Oracle Audit Vault)으로 XML 파일을 가져올 수 있습니다.

9. **Close(닫기)를 누릅니다.**

▼ (필요한 경우) FIPS-140 호환 작업을 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 암호화 사용은 필요에 따라 사용으로 설정할 수 있습니다.

FIPS 140 호환 작업에 맞게 구성된 경우에는 일부 Oracle ILOM 기능을 사용할 수 없습니다. 해당 기능 목록은 *Oracle ILOM* 보안 설명서의 "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" 제목 섹션에 설명되어 있습니다.

또한 “FIPS-140-2 레벨 1 준수” [40]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.**

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
```

FIPS-140-2 레벨 1 준수

MiniCluster에 호스트되는 암호화 애플리케이션은 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 애플리케이션에 제공합니다. 이러한 모듈로 호출되는 사용자 레벨 애플리케이션은 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 애플리케이션에 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 작업을 사용으로 설정(Oracle ILOM) [39]을 참조하십시오.

이 표에서는 MiniCluster에서 Oracle Solaris로 지원되는 FIPS 승인 알고리즘을 보여줍니다.

키 또는 CSP	인증서 번호	
	v1.0	v1.1
대칭 키		

키 또는 **CSP**	인증서 번호	
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)		
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 애플리케이션에 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 애플리케이션에 제공합니다. 이러한 모듈로 호출되는 사용자 레벨 애플리케이션은 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 애플리케이션에 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* 문서를 참조하십시오.

보안 준수 평가

다음 항목에서는 MiniCluster 보안 벤치마크 기능에 대해 설명합니다.

보안 준수 벤치마크

시스템이 설치되면 보안 프로파일(PCI-DSS, CIS 동등 및 DISA-STiG)이 선택되고 시스템이 해당 보안 프로파일을 충족하도록 자동으로 구성됩니다. 시스템이 보안 프로파일에 따라 계속 작동하도록 보장하기 위해 MCMU는 보안 벤치마크를 실행하고 벤치마크 보고서에 액세스할 수 있는 방법을 제공합니다. MCMU BUI 및 CLI를 사용해서 벤치마크를 관리할 수 있습니다.

보안 벤치마크를 실행하면 다음과 같은 이점이 있습니다.

- 데이터베이스의 현재 보안 상태 및 애플리케이션 VM을 평가할 수 있습니다.
- 보안 준수 테스트는 설치 중 구성된 보안 레벨을 기반으로 PCI-DSS, CIS 동등 표준(기본값) 및 DISA-STiG를 지원합니다.
- 보안 준수 테스트는 시스템이 부트될 때 자동으로 실행되며 요청 시 또는 일정이 잡힌 간격에 따라 실행할 수 있습니다.
- MCMU 기본 관리자에게만 제공되는 준수 점수 및 보고서는 MCMU BUI에서 쉽게 액세스할 수 있습니다.
- 준수 보고서는 치료 권장 사항을 제공합니다.

주 - 현재 DISA-STIG 프로파일은 검토 중입니다. 비프로덕션 환경에서 테스트용으로만 이 프로파일을 사용하십시오.

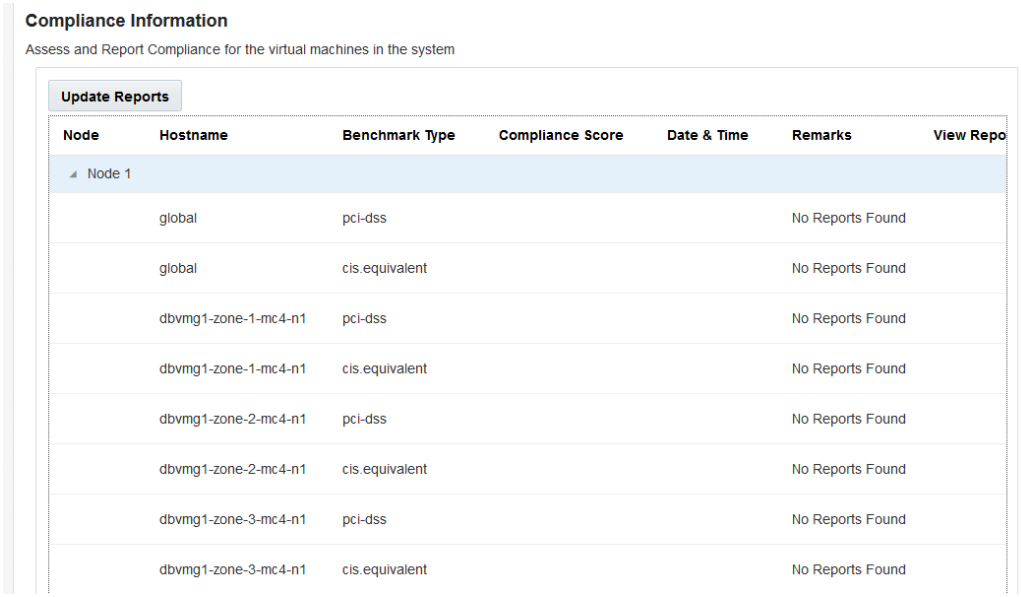
▼ 보안 준수 벤치마크 일정 잡기(BUI)

MCMU BUI를 사용해서 보안 벤치마크의 일정을 잡으려면 다음 절차를 따릅니다. 대신 MCMU CLI를 사용할 경우의 지침은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

1. **기본 관리자로 MCMU BUI에 로그인합니다.**
   자세한 내용은 *Oracle MiniCluster S7-2 Administration Guide*를 참조하십시오.

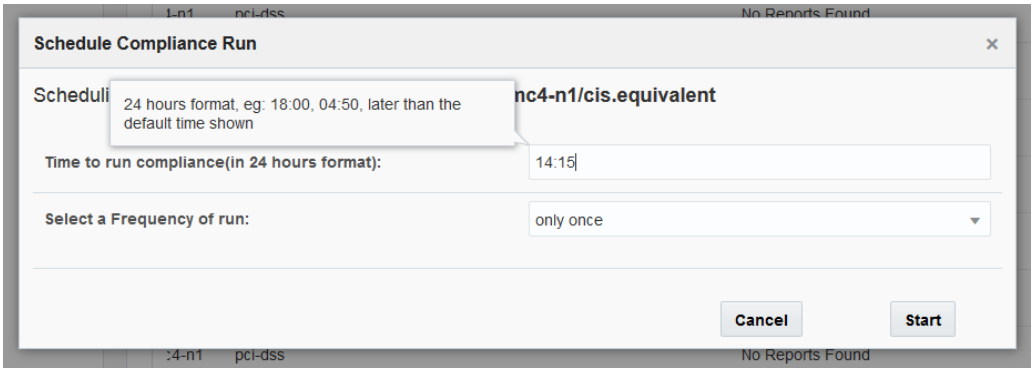
2. **홈 페이지에서 Compliance Information(준수 정보) 패널로 스크롤합니다.**

3. **세부정보를 확장하려면 노드를 누릅니다.**
   각 영역 및 VM은 보안 프로파일(CIS 동등 또는 PCI-DSS)로 구성되었습니다. 벤치마크의 일정을 잡을 때는 구성요소의 보안 프로파일에 해당하는 벤치마크를 선택합니다.



4. **오른쪽으로 스크롤하고 VM 중 하나에 대해 Schedule(일정) 버튼을 누릅니다.**

준수 일정 잡기 실행 페이지가 표시됩니다.



5. **시간 및 빈도를 지정한 후 Start(시작)를 누릅니다.**
보안 준수 테스트가 일정이 잡힌 시간에 실행된 후 보고서를 봅니다. 벤치마크 보고서 보기 (BUI) [45]를 참조하십시오.

▼ 벤치마크 보고서 보기(BUI)

허용 가능한 준수 결과는 다음과 같습니다.

	CIS 동등	PCI-DSS
전역 영역	약 88%	약 88%
VM	약 90%	약 93%

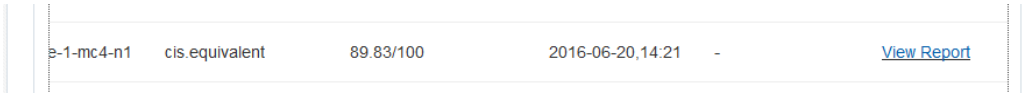
Oracle Solaris 문제로 인한 알려진 준수 테스트 오류는 다음과 같습니다.

- 패키지 무결성(코어 os, rad-python)
- GDM
- 경로 지정 데몬
- SSH 루프백 주소 - 완화로는 문제가 해결되지 않습니다.
- DNS가 인식되지 않는 이름 지정 서비스
- LDAP 클라이언트

MiniCluster 고객 요청 구성 문제로 인한 알려진 준수 테스트 오류는 다음과 같습니다.

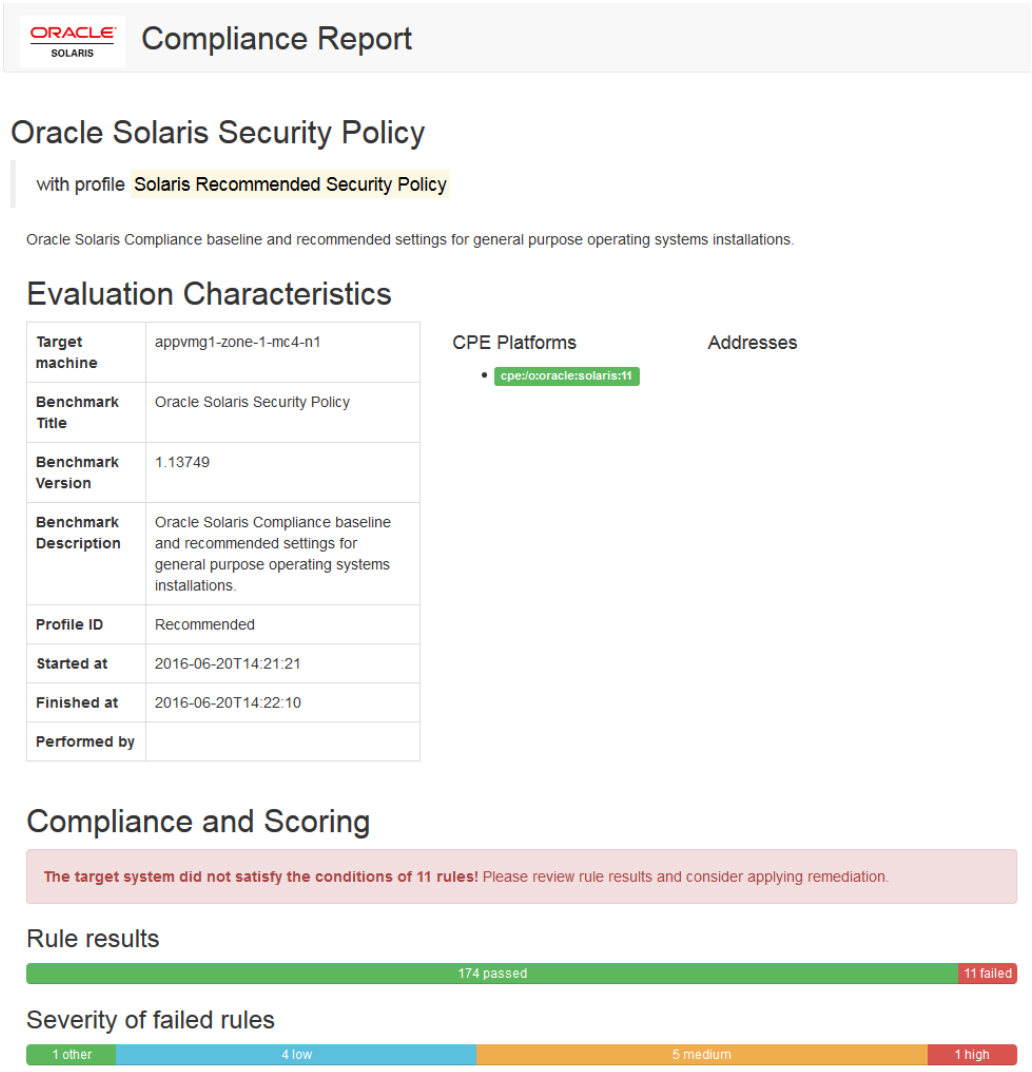
- NFS 클라이언트 서비스 - 제공해야 하는 서비스를 선택합니다.
- eeprom 비밀번호 설정 - 선택적 설정

1. **MCMU BUI에 로그인합니다.**
2. **홈 페이지에서 Compliance Information(준수 정보) 패널로 스크롤합니다.**
3. **Update Reports(보고서 업데이트)를 누릅니다.**
   업데이트 프로세스는 완료하는 데 1분 정도 걸릴 수 있습니다.
4. **노드 표시를 확장하고 준수 보고서를 식별합니다.**



5. **오른쪽으로 스크롤하여 View Report(보고서 보기)를 누릅니다.**
   벤치마크 보고서가 표시됩니다.

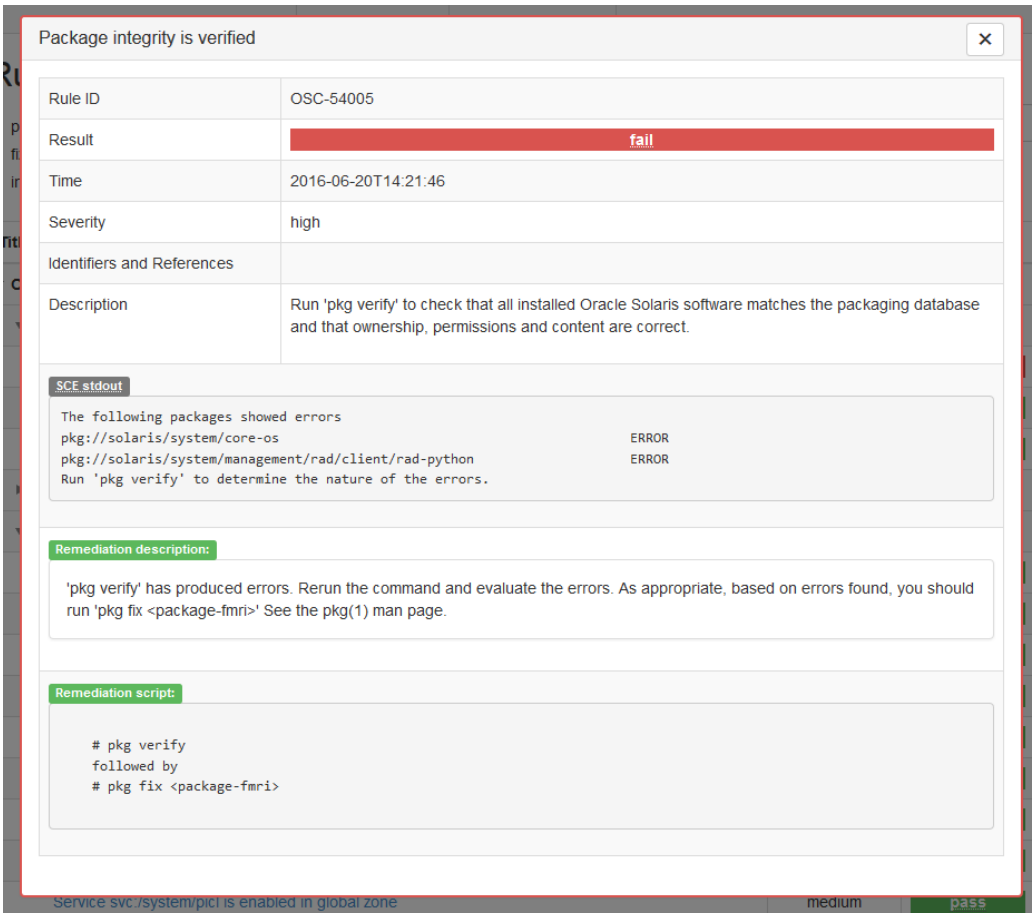
Rule Overview(규칙 개요) 아래에서 해당 결과를 기준으로 표시할 테스트 유형을 선택할 수 있습니다. 또한 검색 필드에 검색 문자열을 지정할 수도 있습니다.



6. **보고서를 기준으로, 보안 제어, 준수 점수, 비정상 및 치료 절차를 확인할 수 있습니다.**

7. **세부정보 및 권장 치료 정보를 보려면 테스트 이름을 누릅니다.**

주 - 보고서 하단에 있는 Show all Result Details(모든 결과 세부정보 표시)를 눌러서 모든 테스트의 모든 세부정보를 표시할 수 있습니다.



SPARC S7-2 서버 보안 제어 이해

다음 항목에서는 하드웨어 및 OpenBoot 환경에 대한 보안 제어를 설명합니다.

하드웨어 보안 이해

물리적 격리 및 액세스 제어를 기반으로 보안 구조를 구축해야 합니다. 물리적 서버가 안전한 환경에 설치되면 허용되지 않은 액세스로부터 보호됩니다. 마찬가지로 모든 일련 번호를 기록해 두면 도난, 재판매 또는 공급망 위험(위조 또는 손상된 구성요소의 조직 공급망 침투)을 방지할 수 있습니다.

다음 절에서는 MiniCluster에 대한 일반적인 하드웨어 보안 지침을 제공합니다.

액세스 제한

- 서버 및 관련 장비는 잠겨 있으며 액세스가 제한된 공간에 설치합니다.
- 장비가 잠금 문이 있는 랙에 설치된 경우 랙의 구성요소를 서비스해야 하기 전까지는 항상 랙 문을 잠급니다. 문을 잠그면 핫 플러그 또는 핫 스왑 장치에 대한 액세스도 제한됩니다.
- 예비 현장 교체 가능 장치(Field-Replaceable Unit, FRU) 또는 자가 교체 가능 장치(Customer-Replaceable Unit, CRU)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 액세스할 수 있도록 제한합니다.
- 랙 및 예비 장치 캐비닛에 대한 잠금 상태 및 무결성을 주기적으로 확인하여 변조 또는 사고로 인한 문 잠금 해제 상태 유지를 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 액세스는 네트워크 기반 공격에 노출되지 않으므로 구성요소에 액세스할 수 있는 보다 안전한 방법입니다.

- 원격 콘솔에 액세스할 수 있도록 외부 KVM에 콘솔을 연결합니다. KVM 장치는 두 단계 인증, 중앙화된 액세스 제어 및 감사를 지원하는 경우가 많습니다. KVM 보안 지침 및 모범 사례에 대한 자세한 내용은 KVM 장치와 함께 제공된 설명서를 참조하십시오.

일련 번호

- 모든 하드웨어의 일련 번호를 기록해 둡니다.
- 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 보관합니다. 인쇄된 문서만 소유권 증명이 될 수 있습니다.

무선 RFID(Radio Frequency Identification) 판독기는 자산 추적을 더욱 간소화할 수 있습니다. Oracle 백서 *How to Track Your Oracle Sun System Assets by Using RFID*는 다음 사이트에서 확인할 수 있습니다.

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

하드 드라이브

하드 드라이브는 중요한 정보를 저장하는 데 사용되는 경우가 많습니다. 이 정보가 무단으로 공개되지 않도록 보호하려면 하드 드라이브를 재사용하거나 구성 해제하거나 폐기하기 전에 정리해야 합니다.

- Oracle Solaris `format` (1M) 명령 등 디스크 완전 삭제 도구를 사용하여 디스크 드라이브에서 모든 데이터를 완전히 지웁니다.
- 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

OpenBoot에 대한 액세스 제한

다음 항목에서는 OpenBoot 프롬프트에서 액세스를 제한하는 방법에 대해 설명합니다.

OpenBoot 비밀번호를 구성하는 방법에 대한 지침은 EEPROM 비밀번호 구성 [26]을 참조하십시오.

OpenBoot 보안 변수 설정에 대한 자세한 내용은 다음 위치에 있는 OpenBoot 설명서를 참조하십시오.

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

▼ OpenBoot 프롬프트 표시

이 절차에서는 MiniCluster 컴퓨트 노드에서 OpenBoot 프롬프트를 표시하여 보안 제어를 구성하는 방법에 대해 설명합니다.

OpenBoot 프롬프트를 표시하려면 시스템을 종료해야 합니다. *Oracle MiniCluster S7-2 Administration* Guide에 설명된 대로 VM을 완전히 종료하기 위한 적절한 절차를 따릅니다.

1. **노드에서 Oracle ILOM에 로그인하고 다음 명령을 실행합니다.**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

호스트 콘솔에 `mcinstall` 사용자로 로그인하고 `root`에 대해 `su`를 실행합니다.

2. **모든 VM이 종료되면 루트 역할로 전역 영역을 정지합니다.**

```
# init 0
.
.
.
{0} ok
```

▼ 실패한 로그인 확인

1. **다음 예와 같이 `security-#badlogins` 매개변수를 사용하여 OpenBoot 환경에 대해 시도된 액세스 및 실패한 액세스가 있는지 확인합니다.**

```
{0} ok printenv security-#badlogins
```

이 명령으로 Ø보다 큰 값이 반환되면 OpenBoot 환경에 대해 실패한 액세스 시도가 기록된 것입니다.

2. **이 명령을 입력해서 매개변수를 재설정합니다.**

```
{0} ok setenv security-#badlogins 0
```

▼ 전원 켜기 배너 제공

직접적인 방지책이나 감지 제어 방법은 아니지만 다음과 같은 이유로 배너를 사용할 수 있습니다.

- 소유권을 전달합니다.
- 사용자에게 허용되는 서버 사용에 대한 주의를 줍니다.
- OpenBoot 매개변수에 대한 액세스 또는 수정이 허가된 사용자로 제한됨을 나타냅니다.

- **다음 명령을 통해 사용자정의 경고 메시지를 사용으로 설정합니다.**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

배너 메시지는 최대 68자일 수 있습니다. 인쇄 가능한 모든 문자가 허용됩니다.

색인