Oracle® Server X5-2 보안 설명서

부품 번호: **E58181-01**
2014년 10월

부품 번호: E58181-01

목차

기본 보안

이 문서에서는 Oracle 서버, 서버 네트워크 인터페이스 및 연결된 네트워크 스위치를 보호하는 데 유용한 일반적인 보안 지침을 제공합니다.

사용 중인 시스템 및 특정 환경과 관련된 추가 보안 요구 사항은 IT 보안 관리자에게 문의하십시오.

모든 하드웨어와 소프트웨어를 사용할 때 준수해야 할 기본 보안 원칙이 있습니다. 이 절에서는 네 가지 기본 보안 원칙을 다룹니다.

액세스

액세스란 하드웨어에 대한 물리적 액세스나 소프트웨어에 대한 물리적 또는 가상 액세스를 의미합니다.

- 침입으로부터 하드웨어와 데이터를 보호하려면 물리적 제어 및 소프트웨어 제어를 사용합니다.
- 시스템을 새로 설치할 때 기본 암호를 모두 변경합니다. 대부분의 장비 유형은 널리 알려지고 허용되지 않은 하드웨어 또는 소프트웨어 액세스를 허가할 수 있는 기본 암호(예: `changeme`)를 사용합니다.
- 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
- 서버 및 관련 장비는 잠겨 있으며 접근이 제한된 공간에 설치합니다.
- 잠금 문이 있는 랙에 장비가 설치된 경우 랙의 구성 요소를 수리해야 하는 경우를 제외하고는 문을 잠가 둡니다.
- USB 포트 및 콘솔에 대한 접근을 제한합니다. 시스템 컨트롤러, PDU(전원 분배 장치) 및 네트워크 스위치 등의 장치는 USB 연결을 제공할 수 있는데 이를 통해 시스템에 직접 액세스할 수 있습니다. 물리적 접근은 네트워크 기반 공격에 노출되지 않으므로 구성 요소에 접근할 수 있는 보다 안전한 방법입니다.
- 네트워크를 통해 시스템을 다시 시작할 수 있는 기능을 제한합니다.

- 특히 핫 플러그 또는 핫 스왑 장치는 쉽게 분리될 수 있으므로 접근을 제한합니다.
- 스페어 FRU(현장 교체 가능 장치) 및 CRU(자가 교체 가능 장치)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.

인증

인증은 일반적으로 기밀 정보(예: 사용자 이름 및 암호)를 통해 사용자가 식별되는 방식입니다. 인증을 통해 하드웨어 또는 소프트웨어 사용자가 실제로 등록된 사용자인지 확인됩니다.

- 사용자가 실제로 등록된 사용자인지 확인할 수 있도록 사용 중인 플랫폼 운영 체제에서 암호 시스템 등의 인증 기능을 설정합니다.
- 담당자가 컴퓨터실에 출입할 때는 사원 명찰을 사용하도록 합니다.
- 사용자 계정에 대해서는 필요한 경우 액세스 제어 목록을 사용하고, 확장된 세션에 대한 시간 초과를 설정하고, 사용자에 대한 권한 레벨을 설정합니다.

권한 부여

권한 부여를 통해 관리자는 사용자가 수행하거나 사용할 수 있는 작업 또는 권한을 제어할 수 있습니다. 담당자는 지정된 작업만 수행하고 지정된 권한만 사용할 수 있습니다. 권한 부여란 하드웨어 및 소프트웨어를 사용할 담당자를 제한하는 것을 의미합니다.

- 담당자가 사용 교육 및 자격을 받은 하드웨어와 소프트웨어만 사용할 수 있도록 합니다.
- 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어합니다.

계정 및 감사

계정 및 감사란 시스템에서의 사용자 작업 레코드를 유지 관리하는 것을 의미합니다. Oracle 서버의 소프트웨어 및 하드웨어 기능을 통해 관리자는 로그인 작업을 모니터하고 하드웨어 인벤토리를 유지 관리할 수 있습니다.

- 시스템 로그를 사용하여 사용자 로그인을 모니터링합니다. 시스템 관리자 및 서비스 계정에는 잘못 사용할 경우 시스템 손상 또는 데이터 손실을 일으킬 수 있는 명령에 대한 액세스 권한이 있으므로 해당 계정을 모니터링합니다. 액세스 및 명령은 시스템 로그를 통해 주의해서 모니터링해야 합니다.
- 모든 하드웨어의 일련 번호를 기록해 둡니다. 구성 요소 일련 번호를 사용하여 시스템 자산을 추적할 수 있습니다. Oracle 부품 번호는 카드, 모듈 및 마더보드에 전자적으로 기록되어 인벤토리 용도로 사용할 수 있습니다.
- 구성 요소를 감지 및 추적하려면 컴퓨터 하드웨어의 모든 중요한 품목(예: FRU 및 CRU)에 보안 표시를 해두십시오. 특수 자외선 펜 또는 돌출된 레이블을 사용합니다.

- 특히 시스템 비상 시 하드웨어 활성화 키 및 라이센스를 시스템 관리자가 쉽게 액세스할 수 있는 보안 위치에 유지합니다. 인쇄된 문서만 소유권 증명이 될 수 있습니다.

안전하게 서버 구성 및 관리 도구 사용

소프트웨어 및 펌웨어 도구를 사용하여 서버를 구성하고 관리할 때는 이 절의 보안 지침을 따릅니다.

사용 중인 시스템 및 특정 환경과 관련된 추가 보안 요구 사항은 IT 보안 관리자에게 문의하십시오.

Oracle System Assistant 보안

Oracle System Assistant는 서버 하드웨어를 구성 및 업데이트하고 지원되는 운영 체제를 설치할 수 있도록 지원하기 위해 사전 설치되는 도구입니다. Oracle System Assistant 사용 방법에 대한 자세한 내용은 다음 웹 사이트의 *Oracle X5* 시리즈 서버 관리 설명서를 참조하십시오.

`http://www.oracle.com/goto/x86AdminDiag/docs`

다음 내용에서는 Oracle System Assistant와 관련된 보안 문제에 대해 설명합니다.

- **Oracle System Assistant에는 부트 가능한 루트 환경이 있음**

  Oracle System Assistant는 사전 설치된 내부 USB 플래시 드라이브에서 실행되는 응용 프로그램입니다. Oracle System Assistant는 부트 가능한 Linux 루트 환경에 구축됩니다. Oracle System Assistant는 기본 루트 셸에 액세스할 수 있는 기능도 제공합니다. 시스템에 대해 물리적 액세스 권한을 가지거나 시스템에 대해 Oracle ILOM을 통한 원격 KVMS(키보드, 비디오, 마우스 및 저장소) 액세스 권한을 가진 사용자는 Oracle System Assistant 및 루트 셸에 액세스할 수 있습니다.

  루트 환경에서는 시스템 구성 및 정책을 변경하고 다른 디스크의 데이터에 액세스할 수 있습니다. 보안을 향상시키려면 서버에 대한 물리적 액세스를 보호하고 Oracle ILOM 사용자에 대한 관리자 및 콘솔 권한을 제한적으로 지정하십시오.

  Oracle System Assistant 셸에서는 적합한 권한을 가진 사용자가 시스템 관리 용도로 Oracle Hardware Management Pack CLI 도구를 사용할 수 있습니다. 셸에서는 네트워크 서비스가 제공되지 않습니다. 보안 레벨을 가장 높게 유지하기 위해 네트워크 서비스는 기본적으로 사용 안함으로 설정되어 있으므로 사용으로 설정하지 않아야 합니다.

- **Oracle System Assistant는 운영 체제에서 액세스할 수 있는 USB 저장 장치를 마운트함**

  부트 가능한 환경 외에 Oracle System Assistant는 설치 후 호스트 운영 체제에서 액세스할 수 있는 USB 저장 장치(플래시 드라이브)로도 마운트됩니다. 이 기능은 유지 관리와 재구성을 위해 도구 및 드라이버에 액세스할 때 유용합니다. Oracle System Assistant USB 저장 장치는 읽기/쓰기가 가능하므로 바이러스에 의해 악용될 수 있습니다.

  보안을 향상시키려면 일반적인 바이러스 검사, 무결성 검사 등 디스크 보호에 사용하는 것과 동일한 방법을 Oracle System Assistant 저장 장치에 적용하십시오.

- **Oracle System Assistant를 사용 안함으로 설정할 수 있음**

  Oracle System Assistant는 서버 설정, 펌웨어 업데이트 및 구성, 호스트 운영 체제 설치에 유용한 도구입니다. 하지만 앞서 설명된 보안 문제가 발생하지 않도록 하려는 경우 또는 도구가 필요하지 않은 경우 Oracle System Assistant를 사용 안함으로 설정할 수 있습니다. Oracle System Assistant를 사용 안함으로 설정한 후에는 호스트 운영 체제에서 더 이상 USB 저장 장치에 액세스할 수 없으며 사용자는 Oracle System Assistant로 부트할 수 없습니다.

  도구 자체에서 또는 BIOS에서 Oracle System Assistant를 사용 안함으로 설정할 수 있습니다. 사용 안함으로 설정한 후에는 BIOS Setup Utility를 통해서만 Oracle System Assistant를 다시 사용으로 설정할 수 있습니다. 권한이 부여된 사용자만 Oracle System Assistant를 다시 사용으로 설정할 수 있도록 BIOS Setup Utility를 암호로 보호하는 것이 좋습니다.

- **Oracle System Assistant 설명서 참조**

  Oracle System Assistant 기능에 대한 자세한 내용은 다음 웹 사이트의 *Oracle X5* 시리즈 서버 관리 설명서를 참조하십시오.

  http://www.oracle.com/goto/x86AdminDiag/docs

Oracle ILOM 보안

Oracle x86 기반 서버 및 Oracle SPARC 기반 서버에 내장된 Oracle ILOM(Integrated Lights Out Manager) 관리 펌웨어를 사용하여 시스템 구성 요소를 보안, 관리 및 모니터링할 수 있습니다. 시스템 관리자에게 부여된 권한 부여 레벨에 따라 이러한 기능에 서버 전원 끄기, 사용자 계정 만들기, 원격 저장 장치 마운트 등의 기능이 포함될 수 있습니다.

- **보안되는 신뢰할 수 있는 내부 네트워크 사용**

  Oracle ILOM에 대한 물리적 관리 연결을 로컬 직렬 포트, 전용 네트워크 관리 포트 또는 표준 데이터 네트워크 포트를 통해 설정할지 여부에 관계없이, 서버에 있는 이 물리적 포트는 항상 신뢰할 수 있는 내부 네트워크나 전용 보안 관리 또는 개인 네트워크에 연결되어야 합니다.

  Oracle ILOM SP(서비스 프로세서)를 인터넷 등의 공용 네트워크에 연결하지 마십시오. Oracle ILOM SP 관리 트래픽을 별도의 관리 네트워크에 유지하고 시스템 관리자에게만 액세스 권한을 부여해야 합니다.

- **기본 관리자 계정 사용 제한**

기본 관리자 계정(root)은 Oracle ILOM에 처음 로그인할 때만 사용합니다. 이 기본 관리자 계정은 초기 서버 설치를 지원할 목적으로만 제공됩니다. 따라서 가장 안전한 환경을 보장하려면 시스템 초기 설정의 일부로 이 기본 관리자 암호(changeme)를 변경해야 합니다. 기본 관리자 계정에 대한 액세스가 허용되면 사용자는 Oracle ILOM의 모든 기능에 제한 없는 액세스가 가능합니다. 또한 새 Oracle ILOM 사용자 각각에 대해 고유한 암호를 사용하는 새 사용자 계정을 설정하고 권한 부여 레벨(사용자 역할)을 지정하십시오.

- **터미널 서버에 직렬 포트를 연결할 때 위험을 신중하게 고려해야 함**

  터미널 장치가 악의적인 침입으로부터 네트워크를 보호하는 데 필요한 적합한 레벨의 사용자 인증 또는 권한 부여를 항상 제공하는 것은 아닙니다. 원치 않는 네트워크 침입으로부터 시스템을 보호하려면 서버의 액세스 제어가 충분하지 않은 경우 터미널 서버 등의 네트워크 재지정 장치 유형을 통해 Oracle ILOM에 대한 직렬 연결(직렬 포트)을 설정하지 마십시오.

  또한 특정 Oracle ILOM 기능(예: 암호 재설정 및 Preboot 메뉴)은 물리적 직렬 포트를 통해서만 제공됩니다. 인증되지 않은 터미널 서버를 사용하여 네트워크에 직렬 포트를 연결하면 물리적 액세스가 불필요하므로 해당 기능과 연관된 보안 수준이 낮아집니다.

- **Preboot 메뉴에 액세스하려면 서버에 대한 물리적 액세스가 필요함**

  Oracle ILOM Preboot 메뉴는 Oracle ILOM을 기본값으로 재설정하고 Oracle ILOM이 응답하지 않는 경우 펌웨어에 알릴 수 있도록 하는 강력한 유틸리티입니다. Oracle ILOM이 재설정된 경우 사용자는 서버에서 버튼을 누르거나(기본값) 암호를 입력해야 합니다. Oracle ILOM Physical Presence 등록 정보가 이 동작을 제어합니다(check_physical_presence= true). Preboot 메뉴에 액세스할 때 보안을 최대화하려면 Preboot 메뉴에 액세스할 때 항상 서버에 대한 물리적 액세스를 수행해야 하도록 기본 설정(true)을 변경하지 마십시오.

- **Oracle ILOM 설명서 참조**

  암호 설정, 사용자 관리 및 보안 관련 기능 적용에 대해 자세히 알아보려면 Oracle ILOM 설명서를 참조하십시오. Oracle ILOM과 관련된 보안 지침은 Oracle ILOM 설명서 라이브러리에 포함된 *Oracle ILOM* 보안 설명서를 참조하십시오. Oracle ILOM 설명서는 다음 웹 사이트에서 확인할 수 있습니다.

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

Oracle Hardware Management Pack 보안

Oracle Hardware Management Pack은 서버, 기타 여러 Oracle x86 기반 서버 및 일부 Oracle SPARC 기반 서버에 사용할 수 있습니다. Oracle Hardware Management Pack은 두 가지 구성 요소로 SNMP 모니터링 에이전트와 서버 관리용 운영 체제 간 CLI(명령줄 인터페이스) 도구 제품군을 제공합니다.

- **Hardware Management Agent SNMP 플러그인 사용**

  SNMP는 시스템을 모니터하거나 관리하는 데 사용되는 표준 프로토콜입니다. Hardware Management Agent SNMP 플러그인과 함께 SNMP를 사용하면 데이터 센터에서 Oracle 서버를 모니터할 수 있으며 2개의 관리 지점인 호스트와 Oracle ILOM에 연결하지

않아도 된다는 장점이 있습니다. 이 기능을 통해 단일 IP 주소(호스트의 IP 주소)를 사용하여 여러 서버를 모니터할 수 있습니다.

SNMP 플러그인은 Oracle 서버의 호스트 운영 체제에서 실행됩니다. SNMP 플러그인 모듈은 호스트 운영 체제에서 고유 SNMP 에이전트를 확장하여 추가 Oracle MIB 기능을 제공합니다. Oracle Hardware Management Pack 자체에는 SNMP 에이전트가 포함되어 있지 않습니다. Linux의 경우 net-snmp 에이전트에 모듈이 추가됩니다. Oracle Solaris의 경우 Oracle Solaris Management Agent에 모듈이 추가됩니다. Microsoft Windows의 경우 플러그인이 고유 SNMP 서비스를 확장합니다. Oracle Hardware Management Pack의 경우 SNMP와 관련된 보안 설정은 플러그인이 아닌 고유 SNMP 에이전트나 서비스의 설정에 따라 결정됩니다.

SNMPv1 및 SNMPv2c는 암호화를 제공하지 않으며 커뮤니티 문자열을 인증 형식으로 사용합니다. SNMPv3은 암호화를 사용하여 보안 채널과 개별 사용자 이름 및 암호를 제공하므로 보다 안전합니다. 따라서 이 버전을 사용하는 것이 좋습니다.

- **Oracle Hardware Management Pack 설명서 참조**

  이러한 기능에 대한 자세한 내용은 Oracle Hardware Management Pack 설명서를 참조하십시오. Oracle Hardware Management Pack과 관련된 보안 지침은 Oracle Hardware Management Pack 설명서 라이브러리에 포함된 *Oracle Hardware Management Pack (HMP) Security Guide*를 참조하십시오. Oracle Hardware Management Pack 설명서는 다음 웹 사이트에서 확인할 수 있습니다.

  `http://www.oracle.com/goto/OHMP/docs`

보안 환경 계획

시스템이 도착하기 전에 보안 지침을 준비해야 합니다. 시스템이 도착한 후에는 조직의 최신 보안 요구 사항이 반영되도록 보안 지침을 주기적으로 검토 및 조정해야 합니다.

서버 및 관련 장비 설치/구성을 수행하기 전, 그리고 수행하는 동안 이러한 절의 정보를 참조하십시오.

사용 중인 시스템 및 특정 환경과 관련된 추가 보안 요구 사항은 IT 보안 관리자에게 문의하십시오.

암호 보호

잘못 선택된 암호로 인해 회사 리소스에 대한 허용되지 않은 액세스가 발생할 수 있으므로 암호는 보안의 중요한 요소입니다. 암호 관리를 위한 최적의 방법을 구현하면 사용자가 자신의 암호를 만들고 보호하는 데 필요한 일련의 지침을 준수할 수 있게 됩니다. 암호 정책의 일반적인 구성 요소를 정의해야 합니다.

- 암호 길이 및 강도
- 암호 기간
- 공통 암호 원칙

강력하고 복잡한 암호를 만들려면 다음과 같은 표준 원칙을 적용하십시오.

- 사용자 이름, 직원 이름 또는 가족 이름이 포함된 암호를 만들지 마십시오.
- 쉽게 추측할 수 있는 암호를 선택하지 마십시오.
- 연속된 숫자 문자열(예: 12345)이 포함된 암호를 만들지 마십시오.
- 단순 인터넷 검색으로 쉽게 검색 가능한 단어 또는 문자열이 포함된 암호를 만들지 마십시오.
- 사용자가 동일한 암호를 여러 시스템에서 재사용하지 않도록 합니다.

- 사용자가 이전 암호를 재사용하지 않도록 합니다.

암호를 정기적으로 변경합니다. 그러면 악의적인 작업을 막을 수 있고 암호가 현재 암호 정책을 준수하게 됩니다.

운영 체제 보안 지침

다음 사항에 대한 자세한 내용은 Oracle OS(운영 체제) 문서를 참조하십시오.

- 시스템을 구성할 때 보안 기능을 사용하는 방법
- 응용 프로그램 및 사용자를 시스템에 추가할 때 안전하게 작동하는 방법
- 네트워크 기반 응용 프로그램을 보호하는 방법

지원되는 Oracle 운영 체제에 대한 보안 설명서 문서는 운영 체제 설명서 라이브러리에 포함되어 있습니다. Oracle 운영 체제에 대한 보안 설명서 문서를 확인하려면 다음 웹 사이트의 Oracle 운영 체제 설명서 라이브러리로 이동하십시오.

운영 체제	링크
Oracle Solaris OS	http://www.oracle.com/technetwork/documentation/Solaris-11-192991.html
Oracle Linux OS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

다른 공급업체에서 제공하는 운영 체제(예: Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows, VMware ESXi)에 대한 자세한 내용은 해당 공급업체의 설명서를 참조하십시오.

네트워크 스위치 및 포트

네트워크 스위치는 다른 레벨의 포트 보안 기능을 제공합니다. 다음 작업을 수행하는 방법에 대해 알아보려면 스위치 설명서를 참조하십시오.

- 로컬 및 원격으로 스위치에 액세스하기 위해 인증, 권한 부여 및 계정 기능을 사용합니다.
- 기본적으로 여러 사용자 계정 및 암호를 가질 수 있는 네트워크 스위치에서 모든 암호를 변경합니다.
- 스위치를 아웃오브밴드(데이터 트래픽에서 분리)로 관리합니다. 아웃오브밴드 관리가 가능하지 않으면 인밴드 관리를 위해 별도의 VLAN(가상 LAN) 번호를 지정합니다.
- IDS(침입 방지 시스템) 액세스를 위해 네트워크 스위치의 포트 미러링 기능을 사용합니다.
- 스위치 구성 파일을 오프라인으로 유지 관리하고 권한이 부여된 관리자로만 액세스를 제한합니다. 구성 파일에는 각 설정에 대한 세부 설명이 포함되어 있어야 합니다.

- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 오토 트렁킹을 사용 안함으로 설정합니다.
- 스위치에서 사용 가능한 경우 다음 포트 보안 기능을 사용합니다.
  - **MAC 잠금**: 하나 이상의 연결된 장치의 MAC(Media Access Control) 주소를 스위치의 물리적 포트와 연관시키는 것과 관련됩니다. 특정 MAC 주소로 스위치 포트를 잠그면 수퍼 유저가 허위 액세스 포인트가 있는 네트워크로의 백도어를 만들 수 없습니다.
  - **MAC 잠금**: 지정된 MAC 주소가 스위치에 연결되지 않도록 합니다.
  - **MAC 학습**: 네트워크 스위치에서 현재 연결을 기반으로 보안을 설정할 수 있도록 각 스위치 포트의 직접 연결에 대한 정보를 사용합니다.

VLAN 보안

VLAN(가상 LAN)을 설정한 경우 VLAN은 네트워크의 대역폭을 공유하므로 추가 보안 조치가 필요합니다.

- VLAN을 사용하는 경우 시스템의 중요한 클러스터를 나머지 네트워크에서 분리합니다. 그러면 사용자가 해당 클라이언트 및 서버의 정보에 대한 액세스 권한을 얻을 가능성이 줄어듭니다.
- 고유한 VLAN 번호를 트렁크 포트에 지정합니다.
- 트렁크를 통해 전송할 수 있는 VLAN을 엄격하게 요구되는 VLAN으로만 제한합니다.
- 가능한 경우 VTP(VLAN Trunking Protocol)를 사용 안함으로 설정합니다. 그렇지 않은 경우 VTP에 대해 관리 도메인, 암호 및 제거를 설정합니다. 그런 다음 VTP를 투명 모드로 설정합니다.
- 가능한 경우 정적 VLAN 구성을 사용합니다.
- 사용되지 않은 스위치 포트를 사용 안함으로 설정하여 사용되지 않은 VLAN 번호를 지정합니다.

Infiniband 보안

Infiniband 호스트 보안을 유지합니다. Infiniband 패브릭은 최소한의 보안 Infiniband 호스트만큼만 안전합니다.

분할 영역은 Infiniband 패브릭을 보호하지 않습니다. 분할 영역은 호스트의 가상 시스템 간에 Infiniband 트래픽 격리만 제공합니다.

보안 환경 유지 관리

초기 설치 및 설정 후 계속해서 Oracle 하드웨어 및 소프트웨어 보안 기능을 사용하여 하드웨어 및 소프트웨어 자산을 제어할 수 있습니다.

이 절의 정보를 사용하여 보안 환경을 유지 관리합니다.

사용 중인 시스템 및 특정 환경과 관련된 추가 보안 요구 사항은 IT 보안 관리자에게 문의하십시오.

전원 제어

소프트웨어를 사용하여 일부 Oracle 시스템의 전원을 켜고 끌 수 있습니다. 일부 시스템 캐비닛의 PDU(전원 분배 장치)도 원격으로 사용 및 사용 안함으로 설정할 수 있습니다. 이러한 명령에 대한 권한 부여는 일반적으로 시스템 구성 중에 설정되며 시스템 관리자 및 서비스 담당자로 제한됩니다.

자세한 내용은 시스템 또는 캐비닛 설명서를 참조하십시오.

자산 추적

일련 번호를 사용하여 인벤토리를 추적할 수 있습니다. Oracle은 옵션 카드 및 시스템 주보드의 펌웨어에 일련 번호를 포함합니다. LAN(근거리 통신망) 연결을 통해 이러한 일련 번호를 확인할 수 있습니다.

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

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

소프트웨어 및 펌웨어 업데이트

새로운 소프트웨어 릴리스 및 패치를 통해 향상된 보안 기능이 소개되었습니다. 효율적인 사전 예방적 패치 관리는 시스템 보안의 중요한 부분입니다. 최상의 보안을 위해서는 최신 소프트웨어 릴리스 및 필요한 모든 보안 패치로 시스템을 업데이트하십시오.

- 소프트웨어 업데이트 및 보안 패치를 정기적으로 확인합니다.
- 항상 소프트웨어 또는 펌웨어의 최신 릴리스 버전을 설치합니다.
- 소프트웨어에 필요한 보안 패치를 설치합니다.
- 네트워크 스위치 등의 장치에는 펌웨어가 포함되어 있어 패치 및 펌웨어 업데이트가 필요할 수 있습니다.

다음 My Oracle Support 웹 사이트에서 소프트웨어 업데이트 및 보안 패치를 찾을 수 있습니다.

http://support.oracle.com

네트워크 보안

보안 원칙에 따라 네트워크를 구성한 후에는 정기적인 검토 및 유지 관리가 필요합니다.

시스템에 대한 로컬 및 원격 액세스를 보안하려면 다음 지침을 따릅니다.

- Telnet 대신 SSH를 사용하여 원격 구성을 특정 IP 주소로 제한합니다. Telnet은 사용자 이름 및 암호를 일반 텍스트로 전달하여 잠재적으로 LAN(근거리 통신망) 세그먼트에 있는 모든 사용자가 로그인 자격 증명을 볼 수 있습니다. SSH에 대해 강력한 암호를 설정합니다.
- SNMP(Simple Network Management Protocol)의 버전 3을 사용하여 보안 전송을 제공합니다. 이전 버전의 SNMP는 보안되지 않아 암호화되지 않은 텍스트로 인증 데이터를 전송합니다. SNMPv3은 암호화를 사용하여 보안 채널을 제공하며 개별 사용자 이름과 암호를 사용합니다.
- SNMPv1 또는 SNMPv2가 필요한 경우 기본 SNMP 커뮤니티 문자열을 강력한 커뮤니티 문자열로 변경합니다. 일부 제품에는 기본 SNMP 커뮤니티 문자열로 PUBLIC이 설정되어 있습니다. 공격자는 커뮤니티를 쿼리하여 거의 완전한 네트워크 맵을 작성하고 MIB(Management Information Base) 값을 수정할 수 있습니다.
- 시스템 컨트롤러에 브라우저 인터페이스가 사용되는 경우 시스템 컨트롤러를 사용한 후 항상 로그아웃합니다.
- TCP(Transmission Control Protocol) 또는 HTTP(Hypertext Transfer Protocol)와 같이 불필요한 네트워크 서비스는 사용 안함으로 설정합니다. 필요한 네트워크 서비스를 사용으로 설정하고 이러한 서비스를 안전하게 구성합니다.

- 로그인 시 표시되도록 허용되지 않은 액세스가 금지됨을 알리는 배너 메시지를 만듭니다. 사용자에게 중요한 정책 또는 규칙을 알릴 수 있습니다. 배너는 사용자에게 특정 시스템에 대한 특수한 액세스 제한을 경고하거나 사용자에게 암호 정책 및 올바른 사용을 상기시키는 데 사용할 수 있습니다.
- 필요한 경우 액세스 제어 목록을 사용하여 제한 사항을 적용합니다.
- 확장된 세션에 대해 시간 초과를 설정하고 권한 레벨을 설정합니다.
- 로컬 및 원격으로 스위치에 액세스하기 위한 인증, 권한 부여 및 계정 기능을 사용합니다.
- 이러한 서비스는 채널 보호를 위한 인증서 및 기타 형식의 강력한 암호화로 보호되므로 매우 안전한 환경에서 사용합니다.
  - Active Directory
  - LDAP/SSL(Lightweight Directory Access Protocol/Secure Socket Layer)
- 의심되는 악의적인 사용자가 없는 개인 보안 네트워크에서 이 서비스를 사용합니다.
  - RADIUS(Remote Authentication Dial In User Service)
  - TACACS+(Terminal Access Controller Access-Control System)
- IDS(침입 방지 시스템) 액세스를 위해 스위치의 포트 미러링 기능을 사용합니다.
- MAC 주소를 기반으로 액세스를 제한하려면 포트 보안을 구현합니다. 모든 포트에서 오토 트렁킹을 사용 안함으로 설정합니다.

네트워크 보안에 대한 자세한 내용은 Oracle ILOM 설명서 라이브러리에 포함된 *Oracle ILOM* 보안 설명서를 참조하십시오. Oracle ILOM 설명서는 다음 웹 사이트에서 확인할 수 있습니다.

`http://www.oracle.com/goto/ILOM/docs`

데이터 보호 및 보안

데이터 보호 및 보안을 최대화하려면 다음 지침을 따릅니다.

- 외장 하드 드라이브 또는 USB 저장 장치 등의 장치를 사용하여 중요한 데이터를 백업합니다. 안전한 별도의 오프사이트 위치에 백업된 데이터를 보관합니다.
- 데이터 암호화 소프트웨어를 사용하여 기밀 정보를 하드 드라이브에 안전하게 보관합니다.
- 이전 하드 드라이브를 폐기할 때는 물리적으로 드라이브를 파괴하고 드라이브의 모든 데이터를 완전히 지웁니다. 파일이 삭제되거나 드라이브가 다시 포맷된 후에도 드라이브에서 정보를 복구할 수 있습니다. 파일을 삭제하거나 드라이브를 다시 포맷하면 드라이브의 주소 테이블만 제거됩니다. 따라서 드라이브의 모든 데이터를 완전히 지우려면 디스크 완전 삭제 소프트웨어를 사용합니다.
- 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. 적절하며 사용 가능한 경우 물리적 소자 도구를 사용할 수도 있습니다.

- 하드 드라이브에 포함된 정보가 매우 중요하여 분쇄 또는 소각을 통해 하드 드라이브를 물리적으로 폐기하는 것만이 적절한 정리 방법인 경우도 있습니다.
- 조직에서는 관련 데이터 보호 정책을 참조하여 가장 적절한 하드 드라이브 정리 방법을 결정해야 합니다.

주의 - 데이터 액세스 관리 방식으로 인해 디스크 완전 삭제 소프트웨어를 사용하여 최신 하드 드라이브, 특히 SSD(반도체 드라이브)의 일부 데이터를 삭제하지 못할 수도 있습니다.

로그 유지 관리

정기적으로 로그 파일을 검사하고 유지 관리합니다. 다음 방법으로 로그 파일을 보안할 수 있습니다.

- 로깅을 사용으로 설정하고 전용 보안 로그 호스트로 로그를 보냅니다.
- NTP(Network Time Protocol) 및 시간 기록을 사용하여 정확한 시간 정보가 포함되도록 로깅을 구성합니다.
- 예약을 통해 네트워크 장치 로그에서 비정상적인 네트워크 작업 또는 액세스를 정기적으로 검사합니다.
- 발생 가능한 문제에 대비하여 로그를 검토하고 보안 정책에 따라 아카이브합니다.
- 로그 파일이 적당한 크기를 초과할 경우 주기적으로 로그 파일을 처분합니다. 나중에 참조하거나 통계 분석에 사용할 수 있도록 처분할 파일의 복사본을 유지 관리합니다.