Oracle® Solaris 11.2용 Oracle Hardware Management Pack 보안 설명서

부품 번호: E56554-02
2015년 9월

ORACLE®

부품 번호: E56554-02

Copyright © 2014, 2015, Oracle and/or its affiliates. All rights reserved.

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

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

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이센스한 개인이나 법인에게 배송하는 경우, 다음 공지사항이 적용됩니다.

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

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

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

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

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제3자로부터 제공되는 컨텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 컨텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 컨텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다. 단, 사용자와 오라클 간의 합의서에 규정되어 있는 경우는 예외입니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`에서 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=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

목차

제품 및 응용 프로그램 보안 개요 7
Oracle Solaris용 Oracle Hardware Management Pack 정보 7
기본 보안 원칙 8
Oracle Hardware Management Pack 보안 요약 8

Oracle Hardware Management Pack 보안 11
호스트-ILOM 상호 연결 인터페이스 11
자격 증명을 파일에 저장하도록 선택 11
SNMP 보안 설정 선택 12

Oracle Hardware Management Pack 구성 요소 설치 또는 제거 13
구성 요소 설치 13
구성 요소 제거 13

제품 및 응용 프로그램 보안 개요

이 절에서는 Oracle Solaris용 Oracle HMP(Hardware Management Pack) 제품 및 기본 응용 프로그램 보안에 대해 간략하게 설명합니다.

다음 항목을 다룹니다.

- "Oracle Solaris용 Oracle Hardware Management Pack 정보" [7]
- "기본 보안 원칙" [8]
- "Oracle Hardware Management Pack 보안 요약" [8]

Oracle Solaris용 Oracle Hardware Management Pack 정보

Oracle Solaris용 Oracle Hardware Management Pack은 여러 Oracle x86 기반 서버 및 일부 SPARC 기반 서버에서 사용할 수 있습니다. Oracle Hardware Management Pack에는 SNMP 모니터링 에이전트 및 서버 관리를 위한 CLI 도구(명령줄 인터페이스 도구) 모음의 두 구성 요소가 있습니다.

Hardware Management Agent SNMP 플러그인과 함께 SNMP를 사용하면 데이터 센터에서 Oracle 서버 및 서버 모듈을 모니터할 수 있으며 2개의 관리 지점인 호스트와 Oracle ILOM에 연결하지 않아도 된다는 장점이 있습니다. 이 기능을 통해 단일 IP 주소(호스트의 IP)를 사용하여 여러 서버 및 서버 모듈을 모니터할 수 있습니다.

Hardware Management Agent SNMP 플러그인은 Oracle 서버의 호스트 운영체제에서 실행됩니다. SNMP 플러그인은 Oracle 하드웨어 저장소 액세스 라이브러리를 사용하여 서비스 프로세서와 통신합니다. Hardware Management Agent에서 서버의 현재 상태에 대한 정보를 자동으로 불러옵니다. Hardware Management Agent에 대한 자세한 내용은 *Oracle Server Management Agent* 사용 설명서를 참조하십시오.

Oracle Server CLI 도구를 사용하여 Oracle 서버를 구성할 수 있습니다. 도구 목록은 *Oracle Server CLI Tools User's Guide*를 참조하십시오.

기능 및 사용법에 대한 자세한 내용은 Oracle Solaris용 Oracle Hardware Management Pack 설명서를 참조하십시오.

- Oracle Solaris용 Oracle Hardware Management Pack 설명서 라이브러리: `http://www.oracle.com/goto/ohmp/solarisdocs`
- 일반 Oracle ILOM 정보는 `http://www.oracle.com/goto/ilom/docs`를 참조하십시오.

기본 보안 원칙

액세스, 인증, 권한 부여 및 계정 관리의 네 가지 기본 보안 원칙이 있습니다.

- 액세스

  침입으로부터 하드웨어나 데이터를 보호하려면 물리적 제어 및 소프트웨어 제어를 사용합니다.

  - 하드웨어의 경우 액세스 제한은 일반적으로 물리적 액세스 제한을 의미합니다.
  - 소프트웨어의 경우 액세스 제한은 일반적으로 물리적 수단 및 가상 수단을 의미합니다.
  - 펌웨어는 Oracle 업데이트 프로세스를 통해서만 변경될 수 있습니다.
- 인증

  사용자가 실제로 등록된 사용자인지 확인할 수 있도록 사용 중인 플랫폼 운영체제에서 암호 시스템 등의 인증 기능을 모두 설정하십시오.

  인증은 배지 및 암호와 같은 수단을 통해 다양한 수준의 보안을 제공합니다. 예를 들어, 담당자가 컴퓨터실에 출입할 때는 사원 명찰을 사용하도록 하십시오.
- 권한 부여

  권한 부여를 통해 회사 직원이 자신들이 사용하기 위해 교육 받고 인증 받은 하드웨어 및 소프트웨어만 작업하도록 할 수 있습니다.

  예를 들어, 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어하십시오.
- 계정

  고객 IT 담당자는 Oracle 소프트웨어 및 하드웨어 기능을 사용하여 로그인 작업을 모니터하고 하드웨어 인벤토리를 유지 관리할 수 있습니다.

  - 시스템 로그를 사용하여 사용자 로그인을 모니터할 수 있습니다. 특히, 시스템 관리자 및 서비스 계정은 강력한 명령에 액세스할 수 있으므로 시스템 로그를 통해 이러한 계정을 추적하십시오.
  - 고객사 정책에 따라 적당한 크기를 초과할 경우 주기적으로 로그 파일을 폐기합니다. 로그는 일반적으로 장기간 보관되므로 유지 관리가 매우 중요합니다.
  - 구성 요소 일련 번호를 사용하여 인벤토리 용도로 시스템 자산을 추적합니다. Oracle 부품 번호는 모든 카드, 모듈 및 마더보드에 전자적으로 기록되어 있습니다.

Oracle Hardware Management Pack 보안 요약

모든 시스템 관리 도구를 구성할 때 기억해야 할 중요한 보안 항목은 다음과 같습니다.

- 시스템 관리 제품을 사용하여 부트 가능한 루트 환경을 얻을 수 있습니다.

  부트 가능한 루트 환경에서는 Oracle ILOM 액세스, Oracle System Assistant 액세스 및 하드 디스크 액세스를 얻을 수 있습니다.

- 시스템 관리 제품에는 관리자나 루트 권한으로 실행해야 하는 강력한 도구가 있습니다.

  이 액세스 레벨에서는 하드웨어 구성 변경 및 데이터 지우기가 가능합니다.

Oracle Hardware Management Pack 보안

Oracle Solaris의 경우 가장 자주 사용되는 Oracle Hardware Management Pack 구성 요소가 사전 설치되어 있습니다. 확실한 보안을 위해 추가 구성이 필요할 수 있습니다.

- "호스트-ILOM 상호 연결 인터페이스" [11]
- "자격 증명을 파일에 저장하도록 선택" [11]
- "SNMP 보안 설정 선택" [12]

호스트-ILOM 상호 연결 인터페이스

호스트-ILOM 상호 연결 인터페이스를 사용할 경우 호스트 운영체제의 클라이언트가 내부 고속 상호 연결을 통해 Oracle ILOM과 통신할 수 있습니다. 이 상호 연결은 IP 스택을 실행하는 내부 Ethernet-over-USB 연결로 구현됩니다. 이 채널을 통해 통신하기 위해 Oracle ILOM과 호스트에는 경로 지정할 수 없는 내부 IP 주소가 지정됩니다. 이 연결은 기본적으로 Oracle Solaris 운영체제에서 사용으로 설정됩니다.

호스트-ILOM 상호 연결을 통해 Oracle ILOM에 연결하려면 네트워크를 통해 Oracle ILOM 관리 포트로 들어오는 연결과 마찬가지로, 인증이 필요합니다. 관리 네트워크에서 노출되는 모든 서비스나 프로토콜은 호스트에 대한 LAN 상호 연결을 통해 사용 가능하게 됩니다. 예를 들어, 호스트의 웹 브라우저를 사용하여 Oracle ILOM 웹 인터페이스에 액세스하거나 보안 셸 클라이언트를 사용하여 Oracle ILOM CLI에 연결할 수 있습니다. 모든 경우에 LAN 상호 연결을 사용하려면 유효한 사용자 이름과 암호를 제공해야 합니다.

Oracle은 네트워크가 RFC 3927을 지원하고 Link-Local IPv4 주소를 사용할 수 있도록 지원할 것을 권장합니다. 또한 운영체제가 브리지나 라우터로 작동하지 않도록 주의를 기울여야 합니다. 이렇게 하면 호스트와 Oracle ILOM 간의 관리 트래픽이 호스트-ILOM 상호 연결을 통해 비밀로 유지됩니다.

- Oracle Solaris용 Oracle Hardware Management Pack 설명서 라이브러리: `http://www.oracle.com/goto/ohmp/solarisdocs`

자격 증명을 파일에 저장하도록 선택

*Oracle Solaris 11.2 SRU 14*를 기준으로 현재 이 기능은 사용 안함으로 설정되었습니다.

Oracle Solaris용 Oracle Hardware Management Pack에 속하는 `ilomconfig` 및 `fwupdate` 도구는 고속 호스트-ILOM 상호 연결을 사용하여 Oracle ILOM에 연결할 수 있습니다. 호스트-ILOM 상호 연결에는 인증이 필요하므로 이러한 도구를 호출할 때마다 Oracle ILOM에 대해 인증해야 합니다. 편의상, 자격 증명을 파일에 캐싱하면 도구에서 자동으로 사용할 수 있습니다. 이렇게 하면 Oracle Hardware Management Pack 도구를 사용하는 스크립트에 일반 텍스트 암호를 내장할 필요가 없습니다.

`ilomconfig` 도구를 사용하여 루트 읽기 전용의 암호화된 파일에 사용자 이름과 암호를 저장할 수 있습니다. `ilomconfig` 또는 `fwupdate`를 사용하여 Oracle ILOM에 액세스할 때 이 파일이 감지된 경우 캐시된 자격 증명이 사용됩니다. 다른 방법으로, 도구를 호출할 때마다 명령줄에 사용자 이름과 암호를 지정할 수 있습니다.

사용된 암호화 알고리즘은 시스템마다 다릅니다. 그러나 키가 발견된 경우 파일이 해독되어 사용자 이름과 암호가 노출될 수 있습니다.

훼손된 암호는 다른 Oracle ILOM 시스템에 사용할 수 없도록 각 Oracle ILOM마다 고유한 암호를 만들 것을 권장합니다.

자격 증명을 파일에 저장하는 방법에 대한 지침은 *Oracle CLI Tools for Oracle Solaris User's Guide*를 참조하십시오.

- Oracle Solaris용 Oracle Hardware Management Pack 설명서 라이브러리: `http://www.oracle.com/goto/ohmp/solarisdocs`

SNMP 보안 설정 선택

Oracle Hardware Management Pack에는 호스트 운영체제에서 고유 SNMP 에이전트를 확장하여 추가 Oracle MIB 기능을 제공하는 SNMP 플러그인 모듈이 들어 있습니다. 특히 Oracle Hardware Management Pack에 SNMP 에이전트 자체는 포함되지 않음에 유의해야 합니다. Oracle Solaris 운영체제의 경우 Solaris Management Agent에 모듈이 추가됩니다.

마찬가지로, Oracle Hardware Management Pack SNMP 플러그인의 경우 SNMP에 관련된 보안 설정은 고유 SNMP 에이전트나 서비스의 설정(플러그인이 아님)에 따라 결정됩니다. SNMP 설정에는 다음이 포함될 수 있습니다.

- SNMPv1/v2c. 이 버전은 암호화를 제공하지 않으며 커뮤니티 문자열을 인증 형식으로 사용합니다. 커뮤니티 문자열은 네트워크를 통해 일반 텍스트로 전송되며 일반적으로 개별 사용자가 전용으로 사용하는 것이 아니라 특정 사용자 그룹 내에서 공유됩니다.
- SNMPv3. 이 버전은 암호화를 사용하여 보안 채널을 제공하며 개별 사용자 이름과 암호를 사용합니다. SNMPv3 사용자 암호는 지역화되므로 관리 스테이션에 안전하게 저장할 수 있습니다.

Oracle은 고유 SNMP 에이전트에서 SNMPv3가 지원되는 경우 이를 사용할 것을 권장합니다. SNMPv3용 net-snmp 구성에 대한 지침은 Oracle Solaris 설명서를 참조하십시오.

Oracle Hardware Management Pack 구성 요소 설치 또는 제거

다음 항목을 다룹니다.

- "구성 요소 설치" [13]
- "구성 요소 제거" [13]

구성 요소 설치

Oracle Solaris용 Oracle Hardware Management Pack은 사전 설치된 일련의 도구로 구성되어 있습니다. 사전 설치되지 않은 추가 Oracle Hardware Management Pack 구성 요소 패키지는 Oracle Solaris IPS(Image Packaging System)를 사용하여 설치할 수 있습니다.

루트 권한이 있는 관리자만 Oracle Hardware Management Pack 패키지를 설치할 수 있습니다.

- Oracle Solaris용 Oracle Hardware Management Pack 설명서 라이브러리: `http://www.oracle.com/goto/ohmp/solarisdocs`

구성 요소 제거

Oracle Solaris용 Oracle Hardware Management Pack 패키지는 Oracle Solaris `pkg uninstall` 명령을 사용하여 제거할 수 있습니다.

주 - 호스트-ILOM 상호 연결을 사용한 Oracle ILOM 액세스를 돕기 위해 이전에 Oracle Hardware Management Pack `ilomconfig` 명령을 사용하여 호스트 자격 증명 캐시 파일을 저장한 경우에는 패키지를 제거할 때 이 파일이 삭제되지 않습니다. 이 경우 Oracle Hardware Management Pack 패키지를 제거하기 전에 `ilomconfig delete credential` 명령을 사용하여 이 파일을 삭제하십시오.

- Oracle Solaris용 Oracle Hardware Management Pack 설명서 라이브러리: `http://www.oracle.com/goto/ohmp/solarisdocs`