Oracle® Solaris Cluster 4.3 보안 설명서

부품 번호: E62325
2015년 10월

ORACLE

부품 번호: E62325

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 Solaris Cluster의 보안에 대한 개요, 보안 설치 및 구성에 대한 정보, 보안 기능 및 개발자에 대한 보안 고려 사항을 제공합니다.
- **대상** - 기술자, 시스템 관리자 및 공인 서비스 공급자
- **필요한 지식** - 전문적인 하드웨어 문제 해결 및 교체 경력

제품 설명서 라이브러리

이 제품과 관련 제품들에 대한 설명서 및 리소스는 http://www.oracle.com/pls/topic/lookup?ctx=E62282에서 사용할 수 있습니다.

피드백

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

♦ ♦ ♦ 1 장

1 Oracle Solaris Cluster 보안 소개

Oracle Solaris Cluster 제품은 고가용성의 확장 가능한 서비스를 만드는 데 사용할 수 있는 통합 하드웨어 및 소프트웨어 솔루션입니다. 이 설명서에서는 Oracle Solaris Cluster의 보안 개요, 보안 설치 및 구성에 대한 정보, 보안 기능 및 개발자에 대한 보안 고려 사항을 제공합니다. 전체 Oracle Solaris Cluster 설명서 세트와 함께 제공되는 이 설명서에서는 Oracle Solaris Cluster 소프트웨어에 대한 전체적인 개요를 제공합니다.

Geographic Edition 소프트웨어는 Oracle Solaris Cluster 소프트웨어의 계층화된 확장입니다. Geographic Edition 프레임워크는 원거리에 지리적으로 흩어진 여러 클러스터를 사용하여 예상치 않은 서비스 중단으로부터 응용 프로그램을 보호합니다. 이러한 클러스터에는 클러스터 간에 복제된 데이터를 관리하는 Geographic Edition 기반구조의 복사본이 포함됩니다.

이 장은 다음 절로 구성됩니다.

Oracle Solaris OS(운영 체제) 보안에 대한 자세한 내용은 *Oracle Solaris 11* 보안 및 강화 지침 및 *Oracle Solaris 11.3*에서 시스템 및 연결된 장치의 보안 을 참조하십시오.

Oracle Solaris Cluster 및 보안 개요

Oracle Solaris Cluster 환경은 Oracle Solaris 운영 체제를 클러스터 운영 체제로 확장합니다. 클러스터는 해당 모음에 배타적으로 속하는 하나 이상의 노드에 대한 모음입니다.

Oracle Solaris Cluster 소프트웨어의 이점은 다음과 같습니다.

- 소프트웨어 또는 하드웨어 오류로 인한 시스템 중단 시간 감소 또는 제거

- 정상적으로 단일 서버 시스템을 종료하는 종류의 오류에 관계없이 최종 사용자에게 데이터 및 응용 프로그램의 가용성 보장
- 클러스터에 노드를 추가하고 로드 균형을 조정하여 서비스를 추가 프로세서까지 확장함으로써 응용 프로그램 처리량 증가
- 전체 클러스터를 종료하지 않고 유지 관리를 수행할 수 있도록 하여 시스템 가용성 향상

클러스터는 기존 단일 서버 시스템보다 여러 가지 이점을 제공합니다. 이러한 이점에는 페일오버 및 확장 가능한 서비스에 대한 지원, 모듈식 증가에 대한 용량, 노드의 로드 한계 설정 기능 및 기존 하드웨어 결함 허용 시스템 대비 낮은 가격 등이 있습니다.

Oracle Solaris OS를 실행하는 클러스터에서 전역 클러스터 및 영역 클러스터는 클러스터 유형입니다. 클러스터는 전역 클러스터, 영역 클러스터이거나 이 둘이 조합된 클러스터일 수 있습니다. 영역 클러스터 구성의 이점에 대한 내용은 *Oracle Solaris Cluster 4.3 Concepts Guide* 를 참조하십시오.

Geographic Edition 및 보안 개요

Geographic Edition 소프트웨어는 Oracle Solaris Cluster 소프트웨어의 계층화된 확장입니다. 데이터 복제 소프트웨어를 사용하면 Geographic Edition 클러스터에서 실행 중인 응용 프로그램이 지리적으로 떨어진 보조 클러스터로 서비스를 마이그레이션함으로써 재해를 극복할 수 있습니다. 지진, 화재 또는 폭풍우와 같은 재해는 기본 사이트에 있는 클러스터를 사용하지 못하게 할 수 있습니다.

재해가 발생할 경우 Geographic Edition 클러스터는 다음과 같은 중복성 레벨을 사용하여 계속해서 서비스를 제공할 수 있습니다.

- 보조 클러스터
- 보조 클러스터에 복제된 응용 프로그램 구성
- 보조 클러스터에 복제된 데이터

Geographic Edition 소프트웨어는 사이트 간 서비스 마이그레이션을 사용하여 지리적으로 떨어진 클러스터를 관리하고 구성할 수 있는 도구 모음을 제공합니다. 클러스터는 전역 클러스터, 영역 클러스터이거나 이 둘이 조합된 클러스터일 수 있습니다. Geographic Edition 소프트웨어는 강력한 보안, 응용 프로그램 서비스 마이그레이션 및 데이터 복제를 통해 여러 물리적 위치 사이에서 가용성을 관리함으로써 엔터프라이즈 시스템에 걸쳐 발생하는 재해를 극복할 수 있습니다.

일반적인 보안 원칙

다음 원칙은 Oracle Solaris Cluster 응용 프로그램을 안전하게 사용하기 위한 기본 요소입니다.

- 소프트웨어를 최신으로 유지
- 중요 서비스에 대한 네트워크 액세스 제한
- 최소 권한 원칙 준수
- 시스템 작업 모니터링
- Oracle 보안 정보를 최신으로 유지

Oracle Solaris Cluster의 보안 설치 및 구성

이 절에서는 Oracle Solaris Cluster의 보안 설치 및 구성을 계획하고 실행하기 위한 링크를 제공합니다.

- **설치** - Oracle Solaris 11 AI(자동 설치 프로그램)를 사용하여 Oracle Solaris Cluster 소프트웨어를 설치할 수 있습니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 “소프트웨어 설치”를 참조하십시오.
- **Cluster 패키지** - Oracle Solaris Cluster 패키지는 Oracle Solaris IPS(이미지 패키징 시스템) 패키지 이름을 사용합니다.

  Oracle Solaris Cluster 코어, 데이터 서비스 및 Geographic Edition 패키지 목록을 보려면 *Oracle Solaris Cluster 4.3 Package Group Lists* 를 참조하십시오.
- **구성** - 전역 클러스터 및 영역 클러스터를 구성하고 관리할 수 있습니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 3 장, “전역 클러스터 설정”, *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 6 장, “영역 클러스터 만들기”, *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 1 장, “Oracle Solaris Cluster 관리 방법 소개”를 참조하십시오.

  전역 클러스터 노드를 설정하기 위한 모든 방법에서 하나의 지정 스폰서 노드의 사전 권한 부여가 필요하므로 해당 지정 시스템만 구성할 노드에 액세스할 수 있습니다. 원하는 경우 보다 안전한 구성을 위해 DES 암호화를 사용할 수 있습니다. 자세한 내용은 `clauth`(1CL) 매뉴얼 페이지를 참조하십시오.
- **공통 에이전트 컨테이너 취약성** - 공통 에이전트 컨테이너와 일부 이전 Java 버전 조합을 사용하면 Oracle Solaris Cluster 소프트웨어의 보안 취약성이 노출됩니다. 이 취약성이 시스템에 존재하는지 여부를 식별하고 이를 수정하는 방법에 대한 자세한 내용은 My Oracle Support 참조 문서 *CVE-2014-3566 Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Oracle Solaris Cluster (Doc ID 1999997.1)* (`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1`)를 참조하십시오. 이 문서를 보려면 My Oracle Support 로그인이 필요합니다.
- **Kerberos V5로 HA for NFS 보안** - HA for NFS 데이터 서비스로 관리되는 NFS 서비스에 보안 액세스가 필요한 경우 Kerberos V5 클라이언트가 HA for NFS 데이터 서비스를 보안하도록 구성할 수 있습니다. 모든 클러스터 노드에서 논리 호스트 이름을 통해 NFS용 Kerberos 주체를 추가하면 됩니다. 자세한 내용은 *Oracle Solaris Cluster Data Service for NFS Guide* 의 “Securing HA for NFS With Kerberos V5”를 참조하십시오.

Geographic Edition의 보안 설치 및 구성

이 절에서는 Geographic Edition 소프트웨어의 보안 설치 및 구성을 계획하고 실행하기 위한 링크를 제공합니다.

- **설치** - Geographic Edition 소프트웨어는 Oracle Solaris 운영 체제 및 Oracle Solaris Cluster 소프트웨어를 실행 중인 클러스터에 설치해야 합니다. Oracle Solaris AI(자동 설치 프로그램)를 사용하여 Oracle Solaris Cluster 소프트웨어와 동시에 또는 나중에 Geographic Edition 소프트웨어를 설치합니다. Geographic Edition 프레임워크 구성은 Oracle Solaris Cluster 소프트웨어 구성과 동일합니다. *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* 의 2 장, “Installing and Configuring the Geographic Edition Software”를 참조하십시오.
- **Geographic Edition 패키지** - Geographic Edition 패키지는 Oracle Solaris IPS(이미지 패키징 시스템) 패키지 이름을 사용합니다. 패키지 목록을 보려면 *Oracle Solaris Cluster 4.3 Package Group Lists* 를 참조하십시오.
- **구성** - 노드나 클러스터 장애를 유발하지 않으면서 Geographic Edition 프레임워크를 실행 중인 클러스터에서 모든 관리 작업을 수행할 수 있습니다. 작동 중인 클러스터에서 Geographic Edition 소프트웨어를 설치, 구성, 시작, 사용, 중지 및 제거할 수 있습니다. *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* 의 4 장, “Administering RBAC”를 참조하십시오.

Oracle Solaris Cluster 보안 기능

이 절에는 Oracle Solaris Cluster에서 제공하는 특정 보안 방식에 대한 정보가 나와 있습니다.

보안 설치는 다음 중요 보안 기능을 사용합니다.

- **RBAC(Role-Based Access Control)** - 클러스터에 액세스하려면 `solaris.cluster.modify`, `solaris.cluster.admin` 및 `solaris.cluster.read`의 RBAC 권한 부여를 사용합니다. 역할에 대한 대부분의 보안 속성을 변경하려면 User Security 권한 프로파일이 지정된 관리자여야 합니다. 자세한 내용은 *Oracle Solaris 11.3*의 사용자 및 프로세스 보안 의 “권한 사용 관리” 및 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “Oracle Solaris Cluster RBAC 권한 프로파일”를 참조하십시오.
- **새 노드** - 클러스터에 노드를 추가할 수 있는 권한이 있는 `claccess` 명령 또는 `clsetup` 유틸리티를 사용합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 8 장, “클러스터 노드 관리”를 참조하십시오.

  액세스 상태에 대한 기본 설정은 `claccess deny-all`입니다. 새 노드 추가와 같이 권한이 필요한 작업을 수행하려는 경우에만 이를 변경해야 합니다. 완료되면 `deny-all` 상태를 복원해야 합니다. 클러스터 구성을 자주 변경해야 하는 경우 `/usr/cluster/bin/claccess -p protocol=authentication-protocol` 명령을 사용하여 더 안전한 인증 프로토콜을 선택함으로써 새 시스템을 최대한 신뢰할 수 있습니다. 자세한 내용은

claccess(1CL) 매뉴얼 페이지 및 *Oracle Solaris 11.3*의 *Kerberos* 및 기타 인증 서비스 관리 의 10 장, “네트워크 서비스 인증 구성”을 참조하십시오.

- **Trusted Extensions** - Oracle Solaris Trusted Extensions 기능은 영역 클러스터에서 사용하도록 사용으로 설정할 수 있습니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 “영역 클러스터의 Trusted Extensions에 대한 지침” 및 *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 “Trusted Extensions를 설치하고 구성하는 방법”를 참조하십시오.
- **영역 클러스터** - 영역 클러스터는 `cluster` 속성으로 설정된 `solaris` 브랜드, `solaris10` 브랜드 또는 `labeled` 브랜드에 대한 하나 이상의 비전역 영역으로 구성됩니다. `labeled` 브랜드 영역 클러스터는 Oracle Solaris 소프트웨어의 Trusted Extensions 기능 전용입니다.

  `clzonecluster` 명령이나 `clsetup` 유틸리티를 사용하여 영역 클러스터를 만듭니다. Oracle Solaris 영역에서 제공하는 격리를 사용하여 전역 클러스터와 유사한 영역 클러스터에서 지원되는 서비스를 실행할 수 있습니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 소프트웨어 설치 설명서 의 “영역 클러스터 만들기 및 구성” 및 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “영역 클러스터 작업”을 참조하십시오.
- **클러스터 콘솔에 대한 보안 연결** - 클러스터 노드 콘솔에 대한 보안 셸 연결을 설정해야 합니다. `pconsole` 유틸리티에 대한 자세한 내용은 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “클러스터 콘솔에 보안 연결을 설정하는 방법”을 참조하십시오.
- **공통 에이전트 컨테이너** - Oracle Solaris Cluster GUI Manager는 강력한 암호화 기술을 사용하여 각 클러스터 노드의 Oracle Solaris Cluster 관리 스택 간 보안 통신을 수행할 수 있습니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “Oracle Solaris Cluster Manager 문제 해결”을 참조하십시오.
- **로깅** - Oracle Solaris Cluster 소프트웨어는 `syslogd` 명령을 사용하여 오류 및 상태 메시지를 기록합니다. 메시지가 저장된 위치를 제어하도록 `/etc/syslog.conf` 파일을 설정했는지 확인하십시오. `/var/adm/messages` 파일과 같은 로그 파일도 안전하게 보호해야 합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “클러스터 관리”를 참조하십시오.
- **감사** - Oracle Solaris Cluster는 Oracle Solaris OS에 있기 때문에 기본적으로 사용으로 설정됩니다. 감사는 실행된 모든 명령을 `/var/cluster/logs/commandlog` 파일에 저장하므로 파일에 대한 보호를 적합하게 설정해야 합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3* 시스템 관리 설명서 의 “Oracle Solaris Cluster 명령 로그의 내용을 보는 방법”을 참조하십시오.
- **Oracle Solaris OS 강화** - Oracle Solaris Cluster는 보안 강화 기술을 사용하여 Oracle Solaris OS를 강화된 상태로 재구성합니다. 또한 Oracle Solaris 시스템 감사를 활성화할 수 있습니다.

Geographic Edition 보안 기능

이 절에는 Geographic Edition에서 제공하는 특정 보안 방식에 대한 정보가 나와 있습니다.

보안 설치는 다음 중요 보안 기능을 사용합니다.

- **RBAC(Role-Based Access Control)** - Geographic Edition 소프트웨어는 Oracle Solaris Cluster 소프트웨어에서 사용되는 RBAC 권한 프로파일을 해당 RBAC 프로파일의 기준으로 합니다. 역할에 대한 대부분의 보안 속성을 변경하려면 User Security 권한 프로파일이 지정된 관리자여야 합니다. 클러스터에 액세스하려면 루트 역할을 맡고 `solaris.cluster.geo.modify`, `solaris.cluster.geo.admin` 및 `solaris.cluster.geo.read`의 RBAC 역할을 사용합니다. 자세한 내용은 *Oracle Solaris 11.3*의 사용자 및 프로세스 보안 및 *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* 의 "Modifying a User's RBAC Properties"를 참조하십시오.
- **보안 인증서** - 설치 중에 클러스터는 보안 인증서(같은 클러스터 내의 노드는 동일한 보안 인증서를 공유해야 함)를 사용하여 클러스터 통신을 보안하도록 구성됩니다. Geographic Edition 파트너쉽에서 클러스터 간 통신은 보안 인증서를 사용하여 SSL(Secure Sockets Layer)과 함께 JMX(Java Management Extensions) 포트를 통해 보안됩니다. 자세한 내용은 *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* 의 "Configuring Trust Between Partner Clusters"를 참조하십시오.
- **공통 에이전트 컨테이너** - 영역 클러스터가 Oracle Solaris Cluster 파트너쉽의 멤버로 작동하도록 하려면 영역 클러스터 내에서 공통 에이전트 컨테이너를 수동으로 구성해야 합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* 의 "Preparing a Zone Cluster for Partner Membership"을 참조하십시오.
- **IPsec(IP Security Architecture)** - IPsec을 사용하여 파트너 클러스터 간 보안 TCP/UDP 하트비트 통신을 구성합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* 의 "Securing Inter-Cluster Communication"을 참조하십시오.

개발자에 대한 보안 고려 사항

이 절에는 Oracle Solaris Cluster를 사용하는 응용 프로그램을 만드는 개발자에게 유용한 정보가 나와 있습니다. 개발자는 Oracle Solaris Cluster API를 사용합니다. 자세한 내용은 *Oracle Solaris Cluster 4.3 Concepts Guide* 의 3 장, "Key Concepts for System Administrators and Application Developers"을 참조하십시오.

개발자가 만드는 에이전트 응용 프로그램은 제품의 보안 프레임워크 내에서 작동해야 하므로 다음 보안 기능을 고려해야 합니다.

- **에이전트 콜백 메소드** - Oracle Solaris Cluster는 응용 프로그램의 시작, 중지, 프로빙 및 검증을 제어하기 위한 콜백 메소드 세트로 구현되는 다양한 응용 프로그램 에이전트를 지원합니다. `Start`, `Stop` 또는 `Validate`와 같은 콜백 메소드는 항상 루트로 실행됩니다. 비루트 사용자가 실행 가능한 메소드 파일 중 하나를 쓸 수 있는 경우 비루트 사용자가 콜백 메소드에 코드를 삽입하여 권한이 부여되지 않은 권한 상승을 수행할 수 있는 취약성이 생길 수 있습니다. Oracle Solaris Cluster는 이러한 실행 가능한 콜백 메소드의 소유권 및 권한을 확인합니다. 확인은 `resource_security` 클러스터 등록 정보 설정에 의해 제어됩니다. `resource_security`가 `SECURE`로 설정되고 비루트에서 메소드 코드를 쓸 수 있음을 확인하는 경우 메소드 실행이 실패합니다.

에이전트 메소드는 응용 프로그램 특정 관리 명령과 같은 외부 프로그램을 차례로 실행합니다. 에이전트 메소드는 외부 프로그램이 가장 적은 권한으로 실행되고 있음을 확인하기 위해 래퍼를 사용하여 이러한 모든 외부 프로그램을 실행해야 합니다. Oracle Solaris Cluster는 `application_user` 및 `resource_security` 등록 정보와 `scha_check_app_user` API를 제공하여 응용 프로그램이 안전하게 실행되고 있음을 확인하도록 데이터 서비스를 사용으로 설정합니다. 구성된 `Application_user` 및 `Resource_security` 설정에 대해 사용자 이름을 확인하기 위해 스크립트에서 `scha_check_app_user` 명령을 호출할 수 있습니다. 자세한 내용은 `scha_check_app_user`(1HA), `r_properties`(5) 및 `cluster`(1CL) 매뉴얼 페이지를 참조하십시오.

- **응용 프로그램에 대한 보안 액세스** - 관리 또는 구성 명령을 실행할 때 응용 프로그램에 대한 보안 액세스가 필요한 경우가 있습니다. 이 보안 액세스는 Oracle Wallet Manager와 같은 자격 증명 기반 메소드로 수행되어야 합니다. 암호를 제공해야 하는 경우 암호는 안전하게 사용되어야 하며 복잡한 형식으로 저장되어야 합니다. 예를 들어 `ps` 명령을 통해 사용자가 볼 수 있는 명령줄에 전달되면 안됩니다. Oracle Solaris Cluster는 인코딩된 암호를 클러스터에 안전하게 저장하고 암호를 관리 작업 수행에 사용해야 하는 경우 검색하는 데 사용할 수 있는 개인 문자열을 만들 수 있도록 해 주는 `clpstring` 명령을 제공합니다. 이 명령에 대한 자세한 내용은 `clpstring`(1CL) 매뉴얼 페이지를 참조하십시오.

데이터 서비스를 개발할 때 이러한 보안 기능을 사용하는 방법에 대한 자세한 내용은 *Oracle Solaris Cluster Data Services Developer's Guide* 를 참조하십시오.

색인

ㅋ

ㅍ