

**Oracle® ZFS Storage Appliance 보안 설명  
서, 릴리스 OS8.7.0**

**ORACLE®**

부품 번호: E81237-01  
2017년 3월



부품 번호: E81237-01

Copyright © 2014, 2017, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 합의서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 합의서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 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 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 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, 라이선스 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 라이선스에 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 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 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=d0cacc>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

---

<b>Oracle ZFS Storage Appliance 보안 설명서</b> .....	7
첫번째 단계 .....	7
초기 설치 .....	8
물리적 보안 .....	8
관리 모델 .....	8
원격 관리 액세스 .....	8
제한된 사용자 권한 부여 .....	9
Oracle ZFS Storage Appliance RESTful API .....	9
시스템 업데이트 .....	9
지연 업데이트 .....	10
지원 번들 .....	10
구성 백업 .....	10
어플라이언스 사용자 .....	10
관리 사용자 역할 .....	11
관리 범위 .....	11
액세스 제어 목록 .....	11
ACL 상속 .....	12
ACL 액세스 결정 .....	12
SMB 공유 레벨 ACL .....	12
ZFS ACL 등록 정보 .....	12
데이터 서비스 .....	12
NFS 인증 및 암호화 옵션 .....	14
iSCSI 데이터 서비스 .....	15
SMB 데이터 서비스 .....	16
FTP 데이터 서비스 .....	18
HTTP 데이터 서비스 .....	19
NDMP 데이터 서비스 .....	20
원격 복제 데이터 서비스 .....	20
데이터 암호화 작업 .....	21
새도우 마이그레이션 데이터 서비스 .....	22

SFTP 데이터 서비스 .....	23
TFTP 데이터 서비스 .....	23
SAN(Storage Area Network) .....	23
디렉토리 서비스 .....	23
네트워크 정보 서비스 .....	24
LDAP(Lightweight Directory Access Protocol) .....	24
ID 매핑 .....	25
시스템 설정 .....	26
Phone Home .....	26
서비스 태그 .....	26
Kerberos 서비스 .....	27
SMTP(Simple Mail Transport Protocol) .....	27
SNMP(Simple Network Management Protocol) .....	27
Syslog 메시지 .....	28
시스템 ID .....	28
디스크 스크러빙 .....	28
삭제 금지 .....	28
보안 로그 .....	29
감사 로그 .....	29
Phone Home 로그 .....	29
추가 정보 .....	30

# Oracle ZFS Storage Appliance 보안 설명서

---

이 설명서는 보안 스토리지 시스템을 만들고 특정 보안 목표를 팀 전체가 이해하는 데 필요한 보안 고려 사항을 탐색, 검토 및 강조합니다. 사용 가능한 보안 기능을 활용하고 필요한 보안 레벨을 만들 수 있도록 어플라이언스를 구성하기 전에 이 설명서를 읽어보는 것이 좋습니다.

이 설명서를 참조하여 Oracle ZFS Storage Appliance의 다양한 기능에 대한 자세한 보안 고려 사항을 살펴볼 수도 있습니다. 어플라이언스 구성 절차는 [Oracle ZFS Storage Appliance 관리 설명서](#)를 참조하십시오.

다음 절에서는 Oracle ZFS Storage Appliance 보안 기능 및 권장 사항에 대해 설명합니다.

- **첫번째 단계** - 어플라이언스를 처음 설치하는 중 로그인 보안 및 시스템의 물리적 보안에 대한 권장 사항에 대해 설명합니다.
- **관리 모델** - CLI 및 BUI를 통한 원격 액세스, CLI 및 BUI에 대한 액세스 제한, 시스템 패치 적용 모델, 지연 업데이트, 지원 번들 및 구성 백업에 대해 설명합니다.
- **어플라이언스 사용자** - 어플라이언스를 관리하고 사용자 권한 부여를 관리할 수 있는 관리 역할에 대해 설명합니다.
- **액세스 제어 목록** - 파일 및 디렉토리에 대한 액세스를 허용 또는 거부하는 메커니즘에 대해 설명합니다.
- **데이터 서비스** - 어플라이언스에서 지원하는 데이터 서비스 및 여러 데이터 서비스에서 제공하는 보안에 대해 설명합니다.
- **디렉토리 서비스** - 어플라이언스에 대해 구성할 수 있는 디렉토리 서비스 및 해당 보안 영향에 대해 설명합니다.
- **시스템 설정** - Phone Home, 서비스 태그, Kerberos, SMTP, SNMP, Syslog, 시스템 ID, 디스크 스크러빙, 삭제 금지 등의 시스템 설정에 대해 설명합니다.
- **보안 로그** - 보안 관련 로그 유형에 대해 설명합니다.

## 첫번째 단계

이 절에서는 어플라이언스를 처음 설치하는 중 로그인 보안 및 시스템의 물리적 보안에 대한 권장 사항에 대해 설명합니다.

## 초기 설치

Oracle ZFS Storage Appliance는 어플라이언스 소프트웨어가 사전 설치되어 있는 상태로 제공됩니다. 따라서 소프트웨어 설치가 필요하지 않으므로 매체를 제공하지 않습니다.

초기 설치의 기본 계정 이름과 암호를 사용하여 수행되며, 기본 루트 암호는 설치 후 변경해야 합니다. Oracle ZFS Storage Appliance가 출하 시 기본값으로 재설정되면 루트 암호도 어플라이언스 및 서비스 프로세서에 대한 기본값으로 재설정됩니다.

Oracle ZFS Storage Appliance를 처음 설치하는 동안에는 시스템 서비스 프로세서와 연관된 기본 계정 이름과 암호가 있습니다. 시스템 관리자가 먼저 이 기본 계정을 사용하여 어플라이언스에 처음으로 액세스할 수 있으며, 그런 다음 관리자가 초기 설치 단계를 수행해야 합니다. 필요한 단계 중 하나는 어플라이언스 관리 암호를 새로 설정하는 것입니다. 그러면 기본 서비스 프로세서 암호도 동일한 값으로 재설정됩니다.

## 물리적 보안

시스템에 대한 액세스를 제어하려면 컴퓨터 환경의 물리적 보안을 유지 관리해야 합니다. 예를 들어, 로그인되어 있는 상태에서 아무도 없는 시스템은 허용되지 않은 액세스 위험에 노출됩니다. 컴퓨터의 주변 및 컴퓨터 하드웨어를 허용되지 않은 액세스로부터 물리적으로 항상 보호해야 합니다.

제한된 접근만 허용하도록 만들어진 Oracle ZFS Storage Appliance는 보안 수단(예: 열쇠, 자물쇠, 도구, 배지 접근)을 통해서 접근이 제어되며, 접근이 허용된 사람은 준수해야 할 예방 조치 및 제한 사항의 근거에 대해 교육을 받은 사람입니다.

## 관리 모델

이 절에서는 Oracle ZFS Storage Appliance 관리 모델에 대한 보안에 대해 설명합니다.

### 원격 관리 액세스

이 절에서는 Oracle ZFS Storage Appliance 원격 액세스 보안에 대해 설명합니다.

#### 브라우저 사용자 인터페이스

BUI(브라우저 사용자 인터페이스)는 일반 어플라이언스 관리에 사용됩니다. BUI 서비스 화면에서는 원격 액세스 서비스 및 설정을 확인하고 수정할 수 있습니다.

관리는 보안 HTTP(HTTPS) 브라우저 세션을 통해 수행됩니다. HTTPS 세션은 초기 설치 시 Oracle ZFS Storage Appliance마다 고유하게 생성되는 자체 서명 인증서로 암호화됩니다. HTTPS 세션의 사용자정의 가능한 기본 세션 시간 초과는 15분입니다.

### 명령줄 인터페이스

CLI(명령줄 인터페이스)에서는 BUI에서 수행할 수 있는 대부분의 동일한 관리 작업을 수행할 수 있습니다.

SSH(보안 셸) 서비스를 사용하면 사용자가 CLI에 대한 SSL(Secure Sockets Layer) 연결을 통해 Oracle ZFS Storage Appliance에 로그인할 수 있습니다. SSH는 일일 로그 또는 분석 통계를 검색하는 등 원격 호스트에서 자동화된 스크립트를 실행하기 위한 수단으로도 사용할 수 있습니다.

## 제한된 사용자 권한 부여

관리 액세스는 루트 사용자, 관련 권한으로 정의된 로컬 관리자, LDAP(Lightweight Directory Access Protocol) 및 NIS(Network Information Service) 등의 ID 서버를 통해 권한이 부여된 관리자로 제한됩니다.

또한 어플라이언스는 BUI, CLI 및 RESTful API를 통해 관리 로그인을 하거나 NFS, HTTP, FTP, SFTP 및 SSH 등의 서비스에 액세스할 수 있도록 사용자를 인증하는 데 Kerberos를 사용할 수 있습니다. Kerberos는 “[NFS 인증 및 암호화 옵션](#)” [14]에 설명된 대로 NFS 프로토콜을 사용하는 개별 공유에 대해 보안을 설정하는 데도 사용할 수 있습니다.

## Oracle ZFS Storage Appliance RESTful API

Oracle ZFS Storage Appliance RESTful API를 사용하여 Oracle ZFS Storage Appliance를 관리할 수 있습니다. RESTful 아키텍처는 계층화된 클라이언트-서버 모델을 기반으로 하며, 클라이언트 구성 없이 표준 허브, 라우터 및 기타 네트워크 시스템을 통해 서비스를 투명하게 재지정할 수 있도록 해줍니다.

Oracle ZFS Storage Appliance RESTful API는 BUI 및 CLI와 동일한 인증 자격 증명을 사용합니다. 외부 클라이언트에서 들어오는 모든 요청은 어플라이언스 자격 증명을 사용하여 개별적으로 인증되며, 포트 215에서 HTTPS 연결을 통해 수행됩니다. RESTful API는 사용자정의 가능한 기본 시간 초과가 15분으로 설정된 HTTPS 세션을 지원합니다.

RESTful API를 사용하여 Oracle ZFS Storage Appliance를 관리하는 방법은 [Oracle ZFS Storage Appliance RESTful API 설명서](#)를 참조하십시오.

## 시스템 업데이트

최신 보안 개선 사항을 사용하려면 시스템 소프트웨어를 최신 상태로 유지하는 것이 좋습니다.

시스템 업데이트는 시스템 소프트웨어의 전체 바이너리 대체로 적용됩니다. 업데이트하기 전에 실행 중인 시스템 플의 스냅샷이 생성됩니다. 이렇게 하면 관리자가 필요한 경우 이전 상태로 롤백할 수 있습니다.

## 지연 업데이트

지연 업데이트는 시스템 업데이트의 일부지만 시스템 업데이트가 수행될 때 활성화되지 않는 기능입니다. 관리자는 지연 업데이트의 적용 여부 또는 시간을 결정합니다. 시스템 업데이트 중에 적용되지 않은 업데이트는 연속 시스템 업데이트 중에도 사용 가능합니다. 지연 업데이트를 적용하도록 선택한 경우 적용할 개별 업데이트를 선택할 수 없습니다. 업데이트를 모두 적용하거나 적용하지 않을 수 있습니다. 업데이트를 적용한 후에는 이전 시스템 소프트웨어 버전으로 롤백할 수 없습니다.

## 지원 번들

시스템이 Phone Home 지원을 사용하도록 등록되어 있고 시스템에 중요한 결함이 있는 경우 시스템 상태가 My Oracle Support로 전송되어 엔지니어링 지원 담당자가 시스템 상태를 확인하고 지원 번들을 만들 수 있습니다. My Oracle Support로 전송되는 시스템 상태 정보에는 사용자 데이터가 포함되어 있지 않습니다. 구성 정보만 전송됩니다.

## 구성 백업

나중에 복원할 수 있도록 시스템 구성을 로컬에 저장할 수 있습니다. 이러한 백업에는 사용자 데이터가 포함되지 않습니다. 구성 설정만 저장됩니다.

## 어플라이언스 사용자

Oracle ZFS Storage Appliance 사용자 유형에는 다음 두 가지가 있습니다.

- 데이터 서비스 사용자 – NFS(네트워크 파일 시스템), SMB(Server Message Block), 광 섬유 채널, iSCSI(Internet Small Computer System Interface), HTTP(Hypertext Transfer Protocol), FTP(File Transfer Protocol) 등의 지원되는 프로토콜을 사용하여 파일 및 블록 리소스에 액세스하는 클라이언트입니다
- 관리 사용자 - 어플라이언스의 구성과 서비스를 관리하는 사용자입니다.

이 절은 관리 사용자에게만 적용됩니다.

## 관리 사용자 역할

관리자에게 사용자정의 역할을 지정하여 권한을 부여할 수 있습니다. 역할은 관리자에게 지정할 수 있는 권한 모음입니다. 다양한 관리자 역할과 운영자 역할을 만들고 각각에 서로 다른 권한 부여 레벨을 지정할 수 있습니다. 직원에게는 불필요한 권한을 지정하지 않고 필요에 맞는 역할을 지정해야 합니다.

역할을 사용하는 것이 모든 권한을 가진 공유 관리자 암호를 사용(예: 모든 사람에게 루트 암호 제공)하는 것보다 훨씬 안전합니다. 역할은 정의된 권한 부여 세트로 사용자를 제한합니다. 또한 사용자 역할은 감사 로그에서 개인 사용자 이름으로 추적 가능합니다. 기본적으로 최소한의 권한 부여를 포함하는 "기본 관리"라는 역할이 있습니다.

관리 사용자는 다음일 수 있습니다.

- 로컬 사용자 – 모든 계정 정보가 Oracle ZFS Storage Appliance에 저장됩니다.
- 디렉토리 사용자 – 기존 NIS 또는 LDAP 계정을 사용하고 추가 권한 부여 설정을 어플라이언스에 저장합니다. 어플라이언스에 대한 액세스 권한을 기존 NIS/LDAP 사용자에게 명시적으로 부여해야 합니다. 그러면 이 사용자가 어플라이언스에 로그인하여 관리할 수 있습니다. 액세스 권한은 기본적으로 부여될 수 없습니다.

## 관리 범위

권한 부여를 통해 사용자는 공유 만들기, 어플라이언스 재부트, 시스템 소프트웨어 업데이트 등의 특정 작업을 수행할 수 있습니다. 권한 부여 그룹을 범위라고 합니다. 각 범위에는 권한 부여 수를 줄이는 선택적 필터 세트가 포함될 수 있습니다. 예를 들어 권한 부여로 모든 서비스를 다시 시작하는 대신 필터를 사용하여 HTTP 서비스만 다시 시작하도록 허용할 수 있습니다.

## 액세스 제어 목록

Oracle ZFS Storage Appliance는 ACL(액세스 제어 목록)을 통해 파일 액세스를 제어합니다. ACL은 특정 파일 또는 디렉토리에 대한 액세스를 허용 또는 거부하는 메커니즘입니다.

Oracle ZFS Storage Appliance에서 제공하는 ACL 모델은 Windows ACL 의미에서 파생된 NFSv4 ACL 모델을 기반으로 합니다. 또한 파일 및 디렉토리에 대한 세분화된 액세스를 제공하는 뛰어난 ACL 모델입니다. 스토리지 어플라이언스 내의 모든 파일과 디렉토리에 ACL이 있으며, SMB 및 NFS에 대한 모든 액세스 제어 결정은 파일 및 디렉토리에 대한 액세스를 허용 또는 거부할 사용자를 결정할 때와 동일한 알고리즘을 거칩니다.

ACL은 하나 이상의 ACE(액세스 제어 항목)로 구성됩니다. 각 ACE에는 ACE에서 부여하거나 거부하는 권한, ACE가 적용될 사용자 및 사용되는 상속 레벨 플래그에 대한 항목이 포함되어 있습니다.

## ACL 상속

NFSv4 ACL을 사용하면 새로 만든 파일과 디렉토리가 개별 ACE를 상속합니다. ACE 상속은 처음 구성 시 관리자가 ACL에 대해 설정하는 몇 가지 상속 레벨 플래그를 통해 제어됩니다.

## ACL 액세스 결정

NFSv4 ACL은 순서에 따라 달라지며 맨 위에서 맨 아래 순서로 처리됩니다. 권한이 부여되면 후속 ACE를 제거할 수 없습니다. 권한이 거부되면 후속 ACE에 권한을 부여할 수 없습니다.

## SMB 공유 레벨 ACL

SMB 공유 레벨 ACL은 파일의 유효한 권한을 결정하기 위해 공유에 있는 파일 또는 디렉토리 ACL과 결합되는 ACL입니다. 공유 레벨 ACL은 파일 ACL 위의 다른 액세스 제어 계층을 제공하며 보다 정교한 액세스 제어 구성을 제공합니다. 공유 레벨 ACL은 SMB 프로토콜을 사용하여 파일 시스템을 내보낼 때 설정됩니다. SMB 프로토콜을 사용하여 파일 시스템을 내보내지 않은 경우 공유 레벨 ACL을 설정해도 아무런 영향이 없습니다. 기본적으로 공유 레벨 ACL은 모든 사람에게 모든 권한을 부여합니다.

## ZFS ACL 등록 정보

ACL 동작 및 상속 등록 정보는 NFS 클라이언트에만 적용할 수 있습니다. SMB 클라이언트의 경우 Windows 의미를 사용하며 ZFS 등록 정보보다 우선적으로 사용됩니다. NFS는 POSIX 의미를 사용하며 SMB 클라이언트는 사용하지 않는다는 점이 다릅니다. 이 등록 정보는 주로 POSIX와 호환됩니다.

## 데이터 서비스

다음 표는 각 데이터 서비스에 대한 설명 및 사용된 포트를 보여줍니다.

표 1 데이터 서비스

서비스	설명	사용된 포트
NFS	NFSv3 및 NFSv4 프로토콜을 통한 파일 시스템 액세스	111 및 2049
iSCSI	iSCSI 프로토콜을 통한 LUN 액세스	3260 및 3205

서비스	설명	사용된 포트
SMB	SMB 프로토콜을 통한 파일 시스템 액세스	SMB-over-NetBIOS 139 SMB-over-TCP 445 NetBIOS Datagram 138 NetBIOS Name Service 137
바이러스 검사	파일 시스템 바이러스 검사	
FTP	FTP 프로토콜을 통한 파일 시스템 액세스	21
HTTP	HTTP 프로토콜을 통한 파일 시스템 액세스	80
HTTPS	수신 보안 연결용	443
NDMP	NDMP 호스트 서비스	10000
원격 복제	원격 복제	216 및 217
암호화	파일 시스템 및 LUN에 대한 투명 암호화	
새도우 마이그레이션	새도우 데이터 마이그레이션	
SFTP	SFTP 프로토콜을 통한 파일 시스템 액세스	218
TFTP	TFTP 프로토콜을 통한 파일 시스템 액세스	
SAN(Storage Area Network)	SAN(Storage Area Network) 대상 및 개시자 그룹	

### 필요한 최소 포트

네트워크에서 보안을 제공하기 위해 방화벽을 만들 수 있습니다. 포트 번호는 방화벽을 만드는 데 사용되며 호스트 및 서비스를 지정하여 네트워크에서 트랜잭션을 고유하게 식별합니다.

다음 목록은 방화벽을 만드는 데 필요한 최소 포트를 보여 줍니다.

### 인바운드 포트

- icmp/0-65535(PING)
- tcp/1920(EM)
- tcp/215(BUI)
- tcp/22(SSh)
- udp/161(SNMP)

HTTP 파일 공유가 사용되는 경우(대개 사용되지 않음) 추가 인바운드 포트

- tcp/443(SSL WEB)
- tcp/80(WEB)

### 아웃바운드 포트

- tcp/80(WEB)

---

주 - 복제의 경우 가능하면 GRE(Generic Routing Encapsulation) 터널을 사용하십시오. 이렇게 하면 트래픽이 백엔드 인터페이스에서 실행될 수 있고 트래픽이 느려질 수 있는 곳에서 방화벽을 피할 수 있습니다. NFS 코어에서 GRE 터널을 사용할 수 없는 경우 프론트 엔드 인터페이스에서 복제를 실행해야 합니다. 이 경우 포트 216 및 포트 217도 열려 있어야 합니다.

---

## NFS 인증 및 암호화 옵션

Kerberos를 사용하여 관리 로그인 및 서비스 액세스를 위해 사용자를 인증하는 어플라이언스의 기능 이외에도, Kerberos를 사용하여 NFS 프로토콜을 사용하는 개별 공유에 대해서도 보안을 설정할 수 있습니다.

NFS 공유는 기본적으로 AUTH\_SYS RPC 인증을 사용하여 할당됩니다. Kerberos 보안을 사용하여 공유되도록 구성할 수도 있습니다. AUTH\_SYS 인증을 사용할 경우 클라이언트의 UNIX UID(사용자 ID) 및 GID(그룹 ID)가 NFS 서버를 통해 네트워크에서 인증되지 않은 상태로 전달됩니다. 이 인증 메커니즘은 클라이언트에서 루트 액세스 권한을 가진 사용자에 의해 쉽게 무효화되므로, 사용 가능한 다른 보안 모드를 사용하는 것이 가장 좋습니다.

특정 호스트, DNS 도메인 또는 네트워크에 대해 공유에 대한 액세스를 허용 또는 거부하도록 공유별로 추가 액세스 제어를 지정할 수 있습니다.

### 보안 모드

보안 모드는 공유별로 설정됩니다. 다음 목록은 사용 가능한 Kerberos 보안 설정에 대해 설명합니다.

- **krb5** - Kerberos V5를 통한 최종 사용자 인증
- **krb5i** - krb5 및 통합 보호(데이터 패킷이 변조 방지됨)
- **krb5p** - krb5i 및 개인 정보 보호(데이터 패킷이 변조 방지되고 암호화됨)

Kerberos 유형 조합을 보안 모드 설정에 지정할 수도 있습니다. 조합된 보안 모드를 통해 클라이언트가 나열된 Kerberos 유형을 사용하여 마운트할 수 있습니다.

### Kerberos 유형

- **sys** - 시스템 인증
- **krb5** - Kerberos v5 전용입니다. 클라이언트가 이 유형을 사용하여 마운트해야 합니다.
- **krb5:krb5i** - Kerberos v5(무결성 포함)입니다. 클라이언트가 나열된 유형을 사용하여 마운트할 수 있습니다.
- **krb5i** - Kerberos v5 무결성 전용입니다. 클라이언트가 이 유형을 사용하여 마운트해야 합니다.

- **krb5:krb5i:krb5p** - Kerberos v5(무결성 또는 프라이버시 포함)입니다. 클라이언트가 나열된 유형을 사용하여 마운트할 수 있습니다.
- **krb5p** - Kerberos v5 프라이버시 전용입니다. 클라이언트가 이 유형을 사용하여 마운트해야 합니다.

## iSCSI 데이터 서비스

Oracle ZFS Storage Appliance에 LUN을 구성할 경우 해당 볼륨을 iSCSI(Internet Small Computer System Interface) 대상으로 내보낼 수 있습니다. iSCSI 서비스를 사용하면 iSCSI 개시자가 iSCSI 프로토콜을 사용하여 대상에 액세스할 수 있습니다.

이 서비스는 iSNS 프로토콜을 사용하여 검색, 관리 및 구성을 지원합니다. iSCSI 서비스는 CHAP(Challenge-Handshake Authentication Protocol)를 사용하여 단방향(대상이 개시자 인증) 및 양방향(대상 및 개시자가 상호 인증) 인증을 지원합니다. 또한 RADIUS(Remote Authentication Dial-In User Service) 데이터베이스의 CHAP 인증 데이터 관리를 지원합니다.

시스템에서 먼저 인증을 수행하고 권한 부여를 나중에 수행하는 2단계 방식을 사용합니다. 로컬 개시자에 CHAP 이름 및 CHAP 암호가 있으면 시스템에서 인증을 수행합니다. 로컬 개시자에 CHAP 등록 정보가 없으면 시스템에서 인증을 수행하지 않으므로 모든 개시자가 권한 부여 대상이 됩니다.

iSCSI 서비스를 사용하면 개시자 그룹 내에서 사용할 수 있는 전역 개시자 목록을 지정할 수 있습니다. iSCSI 및 CHAP 인증을 사용할 경우, 선택한 RADIUS 서버에 대한 모든 CHAP 인증을 지연하는 iSCSI 프로토콜로 RADIUS를 사용할 수 있습니다.

## RADIUS 지원

RADIUS는 CHAP 인증을 수행하기 위해 스토리지 노드 대신 중앙 집중식 서버를 사용하는 시스템입니다. iSCSI 및 CHAP 인증을 사용하는 경우 iSCSI 프로토콜로 RADIUS를 선택할 수 있습니다. RADIUS는 iSCSI와 iSER(iSCSI Extensions for RDMA)을 모두 적용하며 모든 CHAP 인증을 선택한 RADIUS 서버로 전송합니다.

Oracle ZFS Storage Appliance가 RADIUS를 사용하여 CHAP 인증을 수행할 수 있게 하려면 다음 정보가 일치해야 합니다.

- 어플라이언스는 이 RADIUS 서버와 통신할 때 사용할 RADIUS 서버의 주소와 암호를 지정해야 합니다.
- RADIUS 서버에는 어플라이언스의 주소를 제공하고 위와 동일한 암호를 지정하는 항목(예: 클라이언트 파일에 있음)이 있어야 합니다.
- RADIUS 서버에는 CHAP 이름을 제공하고 각 개시자에 대한 CHAP 암호와 일치하는 항목(예: 사용자 파일에 있음)이 있어야 합니다.

- 개시자의 IQN 이름을 CHAP 이름으로 사용(권장 구성)하고 어플라이언스에서 개시자 상자마다 별도의 개시자 항목이 필요하지 않은 경우 RADIUS 서버가 모든 인증 단계를 수행할 수 있습니다.
- 개시자가 별도의 CHAP 이름을 사용하는 경우에는 해당 개시자에 대해 IQN 이름에서 CHAP 이름으로의 매핑을 지정하는 개시자 항목이 어플라이언스에 있어야 합니다. 이 개시자 항목은 개시자의 CHAP 암호를 지정할 필요가 없습니다.

## SMB 데이터 서비스

SMB 프로토콜(CIFS(Common Internet File System)라고도 함)은 주로 Microsoft Windows 네트워크에서 파일에 대한 공유 액세스를 제공합니다. 또한 인증도 제공합니다.

다음 SMB 옵션은 보안에 영향을 미칠 수 있습니다.

- **Restrict Anonymous Access to share list(익명 액세스를 공유 목록으로 제한)** - 이 옵션을 사용하려면 공유 목록을 받기 전에 SMB를 사용하여 클라이언트를 인증해야 합니다. 이 옵션을 사용 안함으로 설정하면 익명 클라이언트에서 공유 목록에 액세스할 수 있습니다. 이 옵션은 기본적으로 사용 안함으로 설정됩니다.
- **SMB Signing Enabled(SMB 서명 사용)** - 이 옵션을 사용하면 SMB 서명 기능을 통해 SMB 클라이언트와의 상호 운용이 가능합니다. 이 옵션이 사용으로 설정된 경우 서명된 패킷에 확인된 서명이 있습니다. 이 옵션이 사용 안함으로 설정된 경우 서명 확인 없이도 서명되지 않은 패킷이 허용됩니다. 이 옵션은 기본적으로 사용 안함으로 설정됩니다.
- **SMB Signing Required(SMB 서명 필요)** - SMB 서명이 필요한 경우 이 옵션을 사용할 수 있습니다. 이 옵션이 사용으로 설정된 경우 모든 SMB 패킷에 서명이 있어야 하며 그렇지 않은 경우 거부됩니다. SMB 서명을 지원하지 않는 클라이언트는 서버에 연결할 수 없습니다. 이 옵션은 기본적으로 해제되어 있습니다.
- **Enable Access-based Enumeration(액세스 기반 열거 사용)** - 이 옵션을 설정하면 클라이언트의 자격 증명을 기반으로 디렉토리 항목이 필터링됩니다. 클라이언트가 파일 또는 디렉토리에 액세스할 수 없는 경우 클라이언트로 반환된 항목 목록에서 해당 파일이 생략됩니다. 이 옵션은 기본적으로 사용 안함으로 설정됩니다.

## Active Directory 도메인 모드 인증

도메인 모드에서는 사용자가 Microsoft AD(Active Directory)에 정의됩니다. SMB 클라이언트는 Kerberos 또는 NTLM 인증을 사용하여 Oracle ZFS Storage Appliance에 연결할 수 있습니다.

사용자가 정규화된 Oracle ZFS Storage Appliance 호스트 이름을 통해 연결된 경우 동일한 도메인 또는 신뢰할 수 있는 도메인에 있는 Windows 클라이언트는 Kerberos 인증을 사용하고, 그렇지 않은 경우 NTLM 인증을 사용합니다.

SMB 클라이언트가 NTLM 인증을 사용하여 어플라이언스에 연결한 경우 사용자의 자격 증명 이 인증을 위해 AD 도메인 컨트롤러로 전달됩니다. 이를 통과 인증이라고 합니다.

NTLM 인증을 제한하는 Windows 보안 정책이 정의된 경우 Windows 클라이언트는 정규화된 호스트 이름을 통해 어플라이언스에 연결해야 합니다. 자세한 내용은 다음 Microsoft Developer Network 문서를 참조하십시오.

<http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx>

인증 후 사용자의 SMB 세션에 대해 "보안 컨텍스트"가 설정됩니다. 보안 컨텍스트로 표시되는 사용자에게는 고유한 보안 설명자(SID)가 지정됩니다. SID는 파일 소유권을 나타내며 파일 액세스 권한을 결정하는 데 사용됩니다.

## 작업 그룹 모드 인증

작업 그룹 모드에서는 사용자가 Oracle ZFS Storage Appliance에 로컬로 정의됩니다. SMB 클라이언트가 작업 그룹 모드에서 어플라이언스에 연결된 경우 해당 사용자의 사용자 이름 및 암호 해시를 사용하여 로컬에서 사용자를 인증합니다.

LM(LAN Manager) 호환성 레벨은 어플라이언스가 작업 그룹 모드에 있는 경우 인증에 사용될 프로토콜을 지정하는 데 사용됩니다.

다음 목록은 각 LM 호환성 레벨에 대한 Oracle ZFS Storage Appliance 동작을 보여줍니다.

- 레벨 2: LM, NTLM 및 NTLMv2 인증을 허용합니다.
- 레벨 3: LM, NTLM 및 NTLMv2 인증을 허용합니다.
- 레벨 4: NTLM 및 NTLMv2 인증을 허용합니다.
- 레벨 5: NTLMv2 인증만 허용합니다.

작업 그룹 사용자가 성공적으로 인증되면 보안 컨텍스트가 설정됩니다. 머신의 SID와 사용자의 UID를 조합하여 어플라이언스에 정의된 사용자에 대해 고유 SID가 만들어집니다. 모든 로컬 사용자는 UNIX 사용자로 정의됩니다.

## 로컬 그룹 및 권한

로컬 그룹은 추가 권한을 해당 사용자에게 제공하는 도메인 사용자 그룹입니다. 관리자는 파일 소유권을 변경하는 파일 권한을 무시할 수 있습니다. 백업 운영자는 파일 백업 및 복원 시 파일 액세스 제어를 무시할 수 있습니다.

## Microsoft Management Console을 통한 관리 작업

적합한 사용자만 관리 작업에 액세스할 수 있도록 하기 위해 MMC(Microsoft Management Console)를 통해 원격으로 수행되는 작업에 대한 액세스 제한 사항이 있습니다.

다음 목록은 사용자 및 허용된 작업을 보여줍니다.

- 일반 사용자 - 공유 나열
- 관리자 그룹의 구성원 - 열린 파일 및 닫힌 파일 나열, 사용자 연결 끊기, 서비스 및 이벤트 로그 보기 관리자 그룹의 구성원은 공유 레벨 ACL을 설정하고 수정할 수도 있습니다.

## 바이러스 검사

바이러스 검사 서비스는 파일 시스템 레벨에서 바이러스가 있는지 검사합니다. 프로토콜을 통해 파일에 액세스할 경우 바이러스 검사 서비스가 먼저 파일을 검사하고, 바이러스가 발견되면 액세스를 거부하고 파일을 격리합니다. 검사는 Oracle ZFS Storage Appliance가 연결되는 외부 엔진에 의해 수행됩니다. 외부 엔진은 어플라이언스 소프트웨어에 포함되지 않습니다.

최신 바이러스 정의를 사용하여 파일을 검사하고 나면 다음에 수정될 때까지 다시 검사하지 않습니다. 바이러스 검사는 주로 바이러스가 유입될 가능성이 있는 SMB 클라이언트에 제공됩니다. NFS 클라이언트도 바이러스 검사를 사용할 수 있지만, NFS 프로토콜의 작동 방식 때문에 SMB 클라이언트에서 신속하게 바이러스를 찾아내지 못할 수 있습니다.

## 타이밍 공격 방지용 지연 엔진

SMB는 타이밍 공격을 방지하기 위한 지연 엔진을 구현하지 않으며, Oracle Solaris 암호화 프레임워크에 의존합니다.

## 전송 중 데이터 암호화

SMB 서비스는 전송 중 데이터 암호화를 지원하지 않는 SMB 프로토콜의 버전 1을 사용합니다.

## FTP 데이터 서비스

FTP는 FTP 클라이언트에서의 파일 시스템 액세스를 허용합니다. FTP 서비스는 익명 로그인을 허용하지 않으므로 구성된 이름 서비스를 사용하여 사용자를 인증해야 합니다.

FTP에서 지원하는 보안 설정은 다음과 같습니다. 이러한 보안 설정은 FTP 프로토콜 액세스가 가능한 모든 파일 시스템에서 공유됩니다.

- **Enable SSL/TLS(SSL/TLS 사용) - SSL/TLS 암호화된 FTP 연결을 허용하며 FTP 트랜잭션이 암호화됩니다.** 이 옵션은 기본적으로 사용 안함으로 설정됩니다. FTP 서버는 자체 서명된 보안 인증서나 고객이 제공한 인증서를 사용합니다.

- **Permit root login(루트 로그인 허용)** - 루트 사용자의 FTP 로그인을 허용합니다. FTP 인증은 네트워크 스니핑 공격을 받을 수 있는 보안 위험이 있는 일반 텍스트를 사용하므로 기본적으로는 해제되어 있습니다.
- **Maximum Number of Allowable Login Attempts(최대 허용 가능한 로그인 시도 횟수)** - FTP 연결이 끊어지기 전까지 실패한 로그인 시도의 횟수이며, 사용자는 재연결을 다시 시도해야 합니다. 기본값은 3입니다.
- **Logging Level(로깅 레벨)** - 로그의 상세 정보 표시 수준입니다.

FTP에서 지원하는 로그는 다음과 같습니다.

- **proftpd** - 성공한 로그인 및 실패한 로그인 시도를 포함한 FTP 이벤트입니다.
- **proftpd\_xfer** - 파일 전송 로그입니다.
- **proftpd\_tls** - SSL/TLS 암호화와 관련된 FTP 이벤트입니다.

## HTTP 데이터 서비스

HTTP는 HTTP, HTTPS 프로토콜 및 HTTP 확장 WebDAV(Web-based Distributed Authoring and Versioning)를 사용하여 파일 시스템에 대한 액세스를 제공합니다. 이를 통해 클라이언트는 웹 브라우저를 통해 또는 클라이언트 소프트웨어에서 지원하는 경우 로컬 파일 시스템으로 공유 파일 시스템에 액세스할 수 있습니다.

HTTPS 서버는 자체 서명된 보안 인증서나 고객이 제공한 인증서를 사용합니다. 고객이 제공한 인증서를 얻으려면 CSR(인증서 서명 요청)을 생성하고 CA(인증 기관)에 보내어 서명을 받아야 합니다. CA로부터 서명된 인증서가 반환되면 어플라이언스에 설치할 수 있습니다. 비루트 CA가 인증서에 서명한 경우 이차/상급 CA에서도 인증서를 얻어야 합니다. 인증서 관리에 대한 자세한 내용은 *Oracle ZFS Storage Appliance* 관리 설명서를 참조하십시오.

다음 등록 정보를 사용할 수 있습니다.

- **Require Client Login(클라이언트 로그인 필요)** - 공유 액세스를 허용하려면 먼저 클라이언트를 인증해야 하며, 사용자가 파일을 만들면 소유권을 갖게 됩니다. 이를 설정하지 않으면 만들어진 파일은 HTTP 서비스로 사용자 "nobody"가 소유합니다.
- **Protocols(프로토콜)** - 지원할 액세스 방법(HTTP, HTTPS 또는 둘 다)을 선택합니다.
- **HTTP Port (for incoming connections)(HTTP 포트(수신 연결용))** - HTTP 포트입니다. 기본 포트는 80입니다.
- **HTTPS Port (for incoming secure connections)(HTTPS 포트(수신 보안 연결용))** - HTTPS 포트입니다. 기본 포트는 443입니다.

클라이언트 로그인 필요가 사용으로 설정된 경우 Oracle ZFS Storage Appliance는 로컬 사용자, NIS 사용자 또는 LDAP 사용자의 유효한 인증 자격 증명을 제공하지 않는 클라이언트에 대한 액세스를 거부합니다. Active Directory 인증은 지원되지 않습니다. 기본 HTTP 인증만 지원됩니다. HTTPS를 사용하지 않는 경우에는 사용자 이름 및 암호가 암호화되지 않은 상태

로 전송되므로 모든 환경에 적합하지 않을 수 있습니다. Require Client Login(클라이언트 로그인 필요)이 사용 안함으로 설정된 경우 어플라이언스가 자격 증명을 인증하지 않습니다.

인증에 관계없이 만들어진 파일 및 디렉토리에서 권한이 숨겨지지 않습니다. 새로 만든 파일에는 모든 사용자에게 의한 읽기 및 쓰기 권한이 있습니다. 새로 만든 디렉토리에는 모든 사용자에게 의한 읽기 및 쓰기 및 실행 권한이 있습니다.

## NDMP 데이터 서비스

NDMP(네트워크 데이터 관리 프로토콜)는 Oracle ZFS Storage Appliance가 DMA(데이터 관리 응용 프로그램)라는 원격 NDMP 클라이언트에서 제어하는 NDMP 기반의 백업 및 복원 작업을 수행할 수 있게 해줍니다. NDMP를 사용하여 어플라이언스 사용자 데이터(예: 어플라이언스에서 관리자가 만든 공유에 저장된 데이터)를 테이프 드라이브와 원격 시스템과 같은 로컬에 연결된 장치 모두에 백업 및 복원할 수 있습니다. 로컬에 연결된 장치도 DMA를 통해 백업 및 복원할 수도 있습니다.

## 원격 복제 데이터 서비스

Oracle ZFS Storage Appliance 원격 복제를 사용하면 프로젝트 및 공유 복제가 쉬워집니다. 이 서비스를 사용하여 어떤 어플라이언스가 데이터를 특정 어플라이언스로 복제했는지 확인하고 특정 어플라이언스가 어떤 어플라이언스로 복제될 수 있는지 제어할 수 있습니다.

이 서비스를 사용으로 설정하면 어플라이언스는 다른 어플라이언스에서 복제 업데이트를 수신하고 구성된 작업에 따라 로컬 프로젝트와 공유에 대한 복제 업데이트를 전송합니다. 이 서비스를 사용 안함으로 설정하면 수신 복제 업데이트가 실패하고 로컬 프로젝트와 공유가 복제되지 않습니다.

어플라이언스에 대해 원격 복제 대상을 구성하려면 원격 어플라이언스에 대한 루트 암호가 필요합니다. 이러한 대상은 어플라이언스의 통신을 가능하게 하는 복제 피어 연결을 설정하는 데 사용됩니다.

대상 만들기 중 루트 암호는 요청 신뢰성을 확인하고 이후 통신에서 어플라이언스를 식별하는 데 사용할 보안 키를 생성하고 교환하는 데 사용됩니다.

생성된 키는 어플라이언스 구성의 일부로 영구 저장됩니다. 루트 암호는 영구 저장되지 않으며 암호화되지 않은 상태로 전송되지 않습니다. 이 초기 ID 교환을 포함한 모든 어플라이언스 통신은 SSL을 사용하여 보호됩니다.

Oracle ZFS Storage Appliance 오프라인 복제 기능을 사용하면 제한된 대역폭의 네트워크를 통해 대량의 데이터 세트를 복제할 때 시간, 리소스와 잠재적 데이터 오류를 줄일 수 있습니다. 오프라인 복제에서 복제 스트림을 NFS 서버의 파일로 내보내서 물리적으로 원격 대상 사이트로 이동하거나 선택적으로 배송용 외부 매체로 복사할 수 있습니다. 대상 사이트에서 관리자는 복제 스트림을 포함하는 파일을 대상 어플라이언스로 가져옵니다.

내보낸 복제 스트림에 대한 액세스를 제한하려면 소스 및 대상 어플라이언스의 IP 주소로만 NFS 공유를 노출시킵니다. 데이터를 암호화하려면 NFS 서버에서 NFS 공유에 대한 온디스크 암호화를 사용으로 설정합니다. 자세한 내용은 NFS 서버 설명서를 참조하십시오. 내보낸 복제 스트림은 어플라이언스에서 암호화되지 않습니다.

## 데이터 암호화 작업

라이선스 공지: 암호화에 대한 평가는 무료로 가능하지만 해당 기능을 운용에 사용하려면 별도로 독립 라이선스를 구매해야 합니다. *Oracle ZFS Storage ZS5-4, Oracle ZFS Storage ZS5-2, Oracle ZFS Storage ZS4-4, Oracle ZFS Storage ZS3-4* 라이선스가 있어야 암호화를 사용할 수 있습니다. 평가 기간 후에는 이 기능에 대해 라이선스를 취득하거나 기능을 비활성화해야 합니다. Oracle은 라이선스 준수 여부를 언제든지 감사할 수 있는 권한을 보유하고 있습니다. 자세한 내용은 "Oracle 소프트웨어 라이선스 계약("SLA") 및 통합된 소프트웨어 옵션을 사용하는 하드웨어 시스템에 대한 자격"을 참조하십시오.

Oracle ZFS Storage Appliance는 개별 공유(파일 시스템 및 LUN) 및 프로젝트 내에 만든 공유에 대해 투명한 데이터 암호화를 제공합니다.

### 암호화 키 관리

어플라이언스는 내장 LOCAL 키 저장소 및 OKM(Oracle Key Manager) 시스템에 연결할 수 있는 기능을 제공합니다. 암호화된 각 프로젝트 또는 공유에는 LOCAL 또는 OKM 키 저장소의 래핑 키가 필요합니다. 데이터 암호화 키는 스토리지 어플라이언스에 의해 관리되며 LOCAL 또는 OKM 키 저장소의 래핑 키에 의해 암호화되어 영구적으로 저장됩니다.

OKM은 급증하는 엔터프라이즈의 스토리지 기반 데이터 암호화에 대한 요구에 부응하는 포괄적인 KMS(키 관리 시스템)입니다. 개방형 표준을 준수하도록 개발된 이 기능은 널리 배포된 이기종 스토리지 기반구조에서 중앙 집중식으로 암호화 키를 관리할 수 있는 용량, 확장성 및 상호 운용성을 제공합니다.

OKM은 다음과 같은 스토리지 키 관리만의 문제를 해결합니다.

- **장기 키 보존** - OKM은 아카이브 데이터를 항상 사용할 수 있도록 보장하며, 전체 데이터 수명 주기 동안 암호화 키를 안전하게 보존합니다.
- **상호 운용성** - OKM은 단일 스토리지 키 관리 서비스를 통해 메인프레임 또는 개방형 시스템에 연결된 다양한 범위의 스토리지 장치를 지원하는 데 필요한 상호 운용성을 제공합니다.
- **고가용성** - OKM은 어플라이언스가 같은 지점에 모여 있는지 전 세계에 분포되어 있는지에 상관없이 활성 N 노드 클러스터링, 동적 로드 균형 조정, 자동화된 페일오버를 통해 고가용성을 제공합니다.
- **고용량** - OKM은 수많은 스토리지 장치와 그보다 더 많은 수의 스토리지 키를 관리합니다. 단일 클러스터화된 어플라이언스는 수천 개의 스토리지 장치 및 수백 개의 스토리지 키에 대한 키 관리 서비스를 제공할 수 있습니다.

- 유연한 키 구성 - OKM 클러스터마다 키를 자동으로 생성하거나, LOCAL 또는 OKM 키 저장소에 대해 개별적으로 키를 생성할 수 있습니다. 보안 관리자가 키 이름을 제공합니다. 키 이름을 키 저장소와 함께 사용할 경우 제공된 래핑 키가 프로젝트 또는 공유와 연관됩니다.

## 키 유지 관리

비활성 상태의 OKM 키를 사용하는 공유 및 프로젝트에는 계속 액세스할 수 없습니다. OKM 키가 사용되지 않도록 하려면 OKM 관리자가 명시적으로 해당 키를 삭제해야 합니다.

암호화된 공유 및 프로젝트에 액세스할 수 있도록 하려면 어플라이언스 구성 및 LOCAL 키 저장소 키 값을 백업하십시오. 키를 사용할 수 없는 경우 해당 키를 사용하는 공유 또는 프로젝트에 액세스할 수 없게 됩니다. 프로젝트 키를 사용할 수 없는 경우 해당 프로젝트에 공유를 새로 만들 수 없습니다.

키는 다음과 같은 방법으로 사용할 수 없게 만들 수 있습니다.

- 키 삭제
- 암호화를 지원하지 않는 릴리스로 롤백
- 키가 구성되지 않은 릴리스로 롤백
- 공장 초기화 재설정
- OKM 서버를 사용할 수 없음

## 암호화 키 수명 주기

데이터 서비스를 오프라인으로 전환하지 않고 언제든지 키를 변경할 수 있을 정도로 암호화 키 수명 주기는 유연합니다.

키가 키 저장소에서 삭제되면 해당 키를 사용하는 모든 공유가 마운트 해제되고 해당 데이터에 액세스할 수 없게 됩니다. OKM 키 저장소에 있는 키의 백업은 OKM 백업 서비스를 사용하여 수행해야 합니다. LOCAL 키 저장소 키의 백업은 시스템 구성 백업의 일부로 포함됩니다. LOCAL 키 저장소의 경우 키를 만들 때 키 값을 제공하여 외부 시스템에 해당 키를 에스크로할 수도 있습니다. 이렇게 하면 키별 백업/복원 기능을 대체할 수 있습니다.

## 새도우 마이그레이션 데이터 서비스

새도우 마이그레이션은 외부 또는 내부 소스에서 자동 데이터 마이그레이션을 허용하며 자동 백그라운드 마이그레이션을 제어합니다. 서비스가 사용으로 설정되어 있는지 여부와 상관없이 데이터는 인밴드 요청에 대해 동기식으로 마이그레이션됩니다. 서비스의 주 목적은 백그라운드 마이그레이션 전용 스레드 수의 세부 조정을 허용하는 것입니다.

NFS 소스의 NFS 마운트는 Oracle ZFS Storage Appliance 사용자가 제어할 수 없습니다. 새도우 마이그레이션 마운트는 보안되지 않으므로 서버에서 Kerberos 또는 이와 유사한 요청이 있을 경우 소스 마운트가 거부됩니다.

## SFTP 데이터 서비스

SFTP(SSH File Transfer Protocol)를 사용하면 SFTP 클라이언트에서 파일 시스템에 액세스할 수 있습니다. 익명 로그인이 허용되지 않으므로 구성된 이름 서비스를 사용하여 사용자 인증해야 합니다.

SFTP 키를 만드는 경우 사용자 지정이 유효한 사용자 등록 정보를 포함해야 합니다. SFTP 키는 사용자별로 그룹화되며 SFTP를 통해 사용자의 이름으로 인증됩니다.

---

주 - 보안을 위해 사용자 등록 정보를 포함하지 않는 기존 SFTP 키는 인증되더라도 다시 만드는 것이 좋습니다.

---

## TFTP 데이터 서비스

TFTP(Trivial File Transfer Protocol)는 단순 파일 전송 프로토콜입니다. 소형이고 구현하기 쉽게 설계되었지만 FTP의 보안 기능이 대부분 없습니다. TFTP는 원격 서버에서 파일을 읽고 쓰기만 합니다. 디렉토리를 나열할 수 없으며, 현재 사용자 인증에 대한 규정도 없습니다.

## SAN(Storage Area Network)

SAN(Storage Area Network)에서 대상 및 개시자 그룹은 LUN(논리적 장치 번호)과 연관될 수 있는 일련의 대상 및 개시자를 정의합니다. 대상 그룹과 연관된 LUN은 해당 그룹의 대상을 통해서만 액세스할 수 있습니다. 개시자 그룹과 연관된 LUN은 해당 그룹의 개시자를 통해서만 액세스할 수 있습니다. LUN을 만들 때 개시자 그룹과 대상 그룹을 LUN에 적용하십시오. 적어도 한 개의 대상 그룹과 한 개의 개시자 그룹을 정의해야 LUN 만들기를 성공적으로 완료할 수 있습니다.

iSCSI/iSER 개시자 액세스 경우에만 선택할 수 있는 CHAP(Challenge-Handshake Authentication Protocol) 인증 이외에 수행되는 인증이 없습니다.

---

주 - 기본 개시자 그룹을 사용할 경우 원치 않거나 충돌하는 LUN 개시자가 발생할 수 있습니다.

---

## 디렉토리 서비스

이 절에서는 어플라이언스에 대해 구성할 수 있는 디렉토리 서비스 및 해당 보안 영향에 대해 설명합니다.

## 네트워크 정보 서비스

NIS(네트워크 정보 서비스)는 중앙 집중식 디렉토리 관리의 이름 서비스입니다. Oracle ZFS Storage Appliance는 NIS 사용자가 FTP 및 HTTP/WebDAV에 로그인할 수 있도록 사용자 및 그룹에 대해 NIS 클라이언트 역할을 수행할 수 있습니다. NIS 사용자에게 어플라이언스 관리를 위한 권한을 부여할 수도 있습니다. 어플라이언스는 자체 권한 설정으로 NIS 정보를 보완합니다.

## LDAP(Lightweight Directory Access Protocol)

Oracle ZFS Storage Appliance는 LDAP(Lightweight Directory Access Protocol)을 사용하여 관리 사용자와 일부 데이터 서비스 사용자를 인증합니다(FTP, HTTP). SSL을 통한 LDAP 보안은 어플라이언스에서 지원됩니다. LDAP은 사용자 및 그룹에 대한 정보를 검색하는 데 사용되며, 다음과 같은 방식으로 사용됩니다.

- 사용자 및 그룹에 대한 이름을 허용하고 표시하는 사용자 인터페이스를 제공합니다.
- 이름을 사용하는 데이터 프로토콜(예: NFSv4)에 대해 사용자 및 그룹에 이름을 매핑합니다.
- 액세스 제어에 사용할 그룹 구성원을 정의합니다.
- (선택사항) 관리 및 데이터 액세스 인증에 사용되는 인증 데이터를 전달합니다.

LDAP 연결을 인증 메커니즘으로 사용할 수 있습니다. 예를 들어 Oracle ZFS Storage Appliance에 대해 사용자를 인증하려고 하면 어플라이언스가 인증을 확인하는 메커니즘으로 LDAP 서버에 대해 해당 사용자를 인증하려고 합니다.

LDAP 연결 보안을 위한 여러 컨트롤이 있습니다.

- 어플라이언스 및 서버 간 인증:
  - 어플라이언스가 익명입니다.
  - 어플라이언스가 사용자의 Kerberos 자격 증명을 사용하여 인증됩니다.
  - 어플라이언스가 지정된 "프록시" 사용자 및 암호를 사용하여 인증됩니다.
- 서버 및 어플라이언스 간 인증(올바른 서버에 연결되었는지 확인):
  - 비보안
  - 서버가 Kerberos를 사용하여 인증됩니다.
  - 서버가 TLS 인증서를 사용하여 인증됩니다.

Kerberos 또는 TLS를 사용하는 경우 LDAP 연결을 통해 전달되는 데이터가 암호화되지만, 그렇지 않은 경우 암호화되지 않습니다. TLS를 사용하는 경우 구성 시 첫번째 연결이 보안되지 않습니다. 서버 인증서는 구성 시 수집되어 나중에 프로덕션 연결을 인증하는 데 사용됩니다.

여러 LDAP 서버를 인증하는 데 사용할 인증 기관 인증서는 가져올 수 없습니다. 또한 특정 LDAP 서버의 인증서를 수동으로 가져올 수 없습니다.

원시 TLS(LDAPS)만 지원됩니다. 비보안 LDAP 연결에서 시작되어 보안 연결로 진행되는 STARTTLS 연결은 지원되지 않습니다. 클라이언트 인증서가 필요한 LDAP 서버는 지원되지 않습니다.

## ID 매핑

클라이언트는 SMB 또는 NFS를 사용하여 Oracle ZFS Storage Appliance에서 파일 리소스에 액세스할 수 있으며, 각 클라이언트에는 고유한 사용자 식별자가 지정됩니다. SMB/Windows 사용자의 경우 SID(보안 설명자)가 지정되고 UNIX/Linux 사용자의 경우 UID(사용자 ID)가 지정됩니다. 사용자는 또한 그룹의 구성원일 수도 있는데, 이 경우 그룹 SID(Windows 사용자의 경우) 또는 GID(그룹 ID)(UNIX/Linux 사용자의 경우)로 식별됩니다.

두 프로토콜을 모두 사용하여 파일 리소스에 액세스하는 환경에서는 대개 ID 동일성을 설정하는 것이 좋습니다. 예를 들어 UNIX 사용자는 Active Directory 사용자에게 해당합니다. 이는 어플라이언스에서 파일 리소스에 대한 액세스 권한을 결정하는 데 중요합니다.

Active Directory, LDAP, NIS 등의 디렉토리 서비스와 관련된 몇 가지 유형의 ID 매핑이 있습니다. 사용 중인 디렉토리 서비스에 대한 보안 모범 사례를 따를 때는 주의해야 합니다.

## Unix용 ID 관리

Microsoft는 IDMU(Identity Management for UNIX)라는 기능을 제공합니다. 이 소프트웨어는 Windows Server 2003에서 사용할 수 있으며 Windows Server 2003 R2 이상과 함께 번들로 제공됩니다. 이 기능은 예전에 Services for UNIX라고 불린 번들되지 않은 형태의 일부였습니다.

IDMU의 주요 용도는 Windows를 NIS/NFS 서버로 지원하는 것입니다. IDMU를 사용하면 관리자가 여러 UNIX 관련 매개변수(그룹에 대한 UID, GID, 로그인 셸, 홈 디렉토리 등)를 지정할 수 있습니다. 이러한 매개변수는 RFC 2307과 비슷하지만 똑같지는 않은 스키마 및 NIS 서비스를 통해 AD에서 사용할 수 있습니다.

IDMU 매핑 모드를 사용하면 ID 매핑 서비스가 이러한 UNIX 속성을 사용하여 Windows 및 UNIX ID 사이에 매핑을 설정합니다. 이 방법은 ID 매핑 서비스가 사용자정의 스키마를 허용하는 대신 IDMU 소프트웨어가 설정한 등록 정보 스키마를 질의한다는 점만 제외하면 디렉토리 기반 매핑과 매우 비슷합니다. 이 방법을 사용할 경우 다른 디렉토리 기반 매핑은 사용할 수 없습니다.

## 디렉토리 기반 매핑

디렉토리 기반 매핑은 ID가 반대 플랫폼에서 동일한 ID로 매핑되는 방법에 대한 정보로 LDAP 또는 Active Directory 객체에 주석을 다는 방식입니다. 객체와 연관된 이러한 추가 속성은 반드시 구성해야 합니다.

## 이름 기반 매핑

이름 기반 매핑은 ID를 이름별로 매핑하는 다양한 규칙을 만드는 방법입니다. 이러한 규칙은 Windows ID 및 UNIX ID 사이에 동일성을 설정합니다.

## 임시 매핑

특정 사용자에게 이름 기반 매핑 규칙이 적용되지 않으면 해당 사용자는 거부 매핑에 의해 차단된 경우를 제외하고 임시 매핑을 통해 임시 자격 증명을 받습니다. 임시 UNIX 이름을 보유한 Windows 사용자가 시스템에서 파일을 만들면 SMB를 사용하여 파일에 액세스하는 Windows 클라이언트에는 해당 Windows ID에 의해 파일이 소유되고 있다고 나타납니다. 그러나 NFS 클라이언트에는 "nobody"에 의해 파일이 소유되고 있다고 나타납니다.

## 시스템 설정

다음 절은 사용 가능한 시스템 보안 설정에 대해 설명합니다.

## Phone Home

Phone Home 서비스는 Oracle ZFS Storage Appliance 등록뿐 아니라 Phone Home 원격 지원 서비스를 관리하는 데 사용됩니다. 이 메시지에는 사용자 데이터나 메타데이터가 전송되지 않습니다.

등록은 Oracle 장비를 관리할 수 있는 Oracle 인벤토리 포털과 Oracle ZFS Storage Appliance를 연결합니다. 등록은 Phone Home 서비스를 사용하기 위한 필수 조건입니다.

Phone Home 서비스는 오라클 고객 지원 센터와 통신하여 다음을 지원합니다.

- **결함 보고** - 시스템이 자동화된 서비스 응답의 활성 문제를 Oracle에 보고합니다. 결함의 특성에 따라 지원 사례가 제공될 수 있습니다.
- **하트비트** - 하트비트 메시지는 시스템이 실행 중임을 나타내기 위해 매일 Oracle로 전송됩니다. 오라클 고객 지원 센터는 활성화된 시스템 중 하나가 오랜 시간 동안 하트비트를 보내지 못할 경우 계정을 기술 담당자에게 알릴 수 있습니다.
- **시스템 구성** - 현재 소프트웨어 및 하드웨어 버전과 구성은 물론 스토리지 구성에 대해 설명하는 주기적 메시지가 Oracle로 전송됩니다.

## 서비스 태그

서비스 태그는 Oracle ZFS Storage Appliance에서 다음과 같은 데이터를 질의할 수 있도록 허용하여 제품 인벤토리 및 지원을 용이하게 하는 데 사용됩니다.

- 시스템 일련 번호
- 시스템 유형
- 소프트웨어 버전 번호

서비스 태그를 오라클 고객 지원 센터에 등록하면 Oracle 장비를 쉽게 추적하고 서비스 호출을 빠르게 할 수 있습니다. 서비스 태그는 기본적으로 사용으로 설정되어 있습니다.

## Kerberos 서비스

Kerberos 서비스는 Kerberos 환경과 함께 사용될 경우 NFS, HTTP, FTP, SFTP, SSH 등의 서비스에 대한 액세스 및 어플라이언스 관리 로그인을 위해 인증을 제공합니다. 어플라이언스 사용자가 이러한 서비스에 대해 Kerberos 인증을 사용하려면 동일한 이름의 Kerberos 주체를 포함해야 합니다. Kerberos는 “[NFS 인증 및 암호화 옵션](#)” [14]에 설명된 대로 NFS 프로토콜을 사용하는 개별 공유에 대해 보안을 설정하는 데도 사용할 수 있습니다.

Kerberos와 Active Directory는 고유한 영역과 키를 포함하기 때문에 동시에 사용으로 설정할 수 있습니다. 두 가지 모두 활성화 상태이면 Kerberos 영역이 기본값입니다. Active Directory만 활성화 상태이면 이 영역이 기본값입니다.

## SMTP(Simple Mail Transport Protocol)

SMTP(Simple Mail Transport Protocol)는 보통 구성된 경보에 대한 응답으로 Oracle ZFS Storage Appliance에서 생성되는 모든 메일을 전송합니다. SMTP 서비스는 외부 메일을 허용하지 않으며 어플라이언스 자체에서 자동 생성된 메일만 전송합니다.

기본적으로 SMTP 서비스는 DNS(MX 레코드)를 사용하여 메일을 전송할 위치를 결정합니다. 어플라이언스의 도메인에 대해 DNS가 구성되어 있지 않거나 송신 메일의 대상 도메인에서 DNS MX 레코드가 올바르게 설정되어 있지 않으면 송신 메일 서버를 통해 모든 메일을 전달하도록 어플라이언스를 구성할 수 있습니다.

## SNMP(Simple Network Management Protocol)

SNMP(Simple Network Management Protocol)는 Oracle ZFS Storage Appliance에 대한 두 가지 기능을 제공합니다. 어플라이언스 상태 정보는 SNMP를 통해 제공될 수 있으며, SNMP 트랩을 전송하도록 경보를 구성할 수 있습니다. SNMP 버전 v1, v2c 및 v3은 이 서비스를 사용으로 설정할 경우 사용할 수 있습니다. 어플라이언스는 최대 128개의 물리적 및 논리적 네트워크 인터페이스를 지원합니다.

## Syslog 메시지

Syslog 메시지는 Oracle ZFS Storage Appliance에서 하나 이상의 원격 시스템으로 전송되는 작은 이벤트 메시지입니다. Syslog는 두 가지 어플라이언스 기능을 제공합니다.

- 하나 이상의 원격 시스템에 Syslog 메시지를 전송하도록 경보를 구성할 수 있습니다.
- Syslog가 지원되는 어플라이언스의 서비스의 경우 해당 Syslog 메시지를 원격 시스템으로 전달할 수 있습니다.

Syslog를 RFC 3164에서 설명한 기존 출력 형식으로 구성하거나 RFC 5424에서 설명한 최신 버전 출력 형식으로 구성할 수 있습니다. Syslog 메시지는 UDP 데이터그램으로 전송됩니다. 따라서 전송 시스템의 메모리가 부족하거나 네트워크가 혼잡해지기 시작하면 네트워크에 의해 삭제되거나 아예 전송되지 않을 수 있습니다. 이에 따라 관리자는 네트워크의 복잡한 실패 시나리오에 따라 일부 메시지가 누락될 수 있으며 삭제됨을 가정해야 합니다.

메시지에는 다음 요소가 포함됩니다.

- 기능 - 메시지를 보낸 시스템 구성요소의 유형을 설명합니다.
- 심각도 - 메시지와 연관된 상태의 심각도를 설명합니다.
- 시간 기록 - 연관된 이벤트의 시간을 UTC로 설명합니다.
- 호스트 이름 - 어플라이언스의 정식 이름을 설명합니다.
- 태그 - 메시지를 보낸 시스템 구성요소의 이름을 설명합니다.
- 메시지 - 이벤트 자체를 설명합니다.

## 시스템 ID

이 서비스는 시스템 이름과 위치에 대한 구성을 제공합니다. Oracle ZFS Storage Appliance를 다른 네트워크 위치로 이동하거나 용도를 바꾼 경우 시스템 이름과 위치를 변경해야 할 수 있습니다.

## 디스크 스크러빙

디스크 스크러빙을 정기적으로 수행해야 Oracle ZFS Storage Appliance가 디스크에서 손상된 데이터를 찾아 수정할 수 있습니다. 디스크 스크러빙은 유휴 기간 중 디스크를 읽어 자주 액세스하는 섹터에서 해결할 수 없는 읽기 오류를 찾아내는 백그라운드 프로세스입니다. 데이터 손실을 줄이기 위해서는 이러한 잠재된 섹터 오류를 시기 적절하게 찾아내는 것이 중요합니다.

## 삭제 금지

삭제 금지 기능이 사용으로 설정된 경우 공유 또는 프로젝트를 삭제할 수 없습니다. 이러한 삭제에는 종속 복제본을 통한 공유 삭제, 프로젝트 내 공유 삭제 또는 복제 패키지 삭제가 포함됩니다.

니다. 그러나 이는 복제 업데이트를 통해 삭제된 공유에 영향을 주지 않습니다. 이 등록 정보가 설정되어 있어도 복제에 대한 소스인 Oracle ZFS Storage Appliance에서 공유가 삭제되면 대상에서 해당되는 공유가 삭제됩니다.

공유를 삭제하려면 먼저 별도의 단계로 등록 정보를 명시적으로 해제해야 합니다. 이 등록 정보는 기본적으로 해제되어 있습니다.

## 보안 로그

이 절에서는 보안과 관련된 로깅 기능에 대해 설명합니다.

## 감사 로그

감사 로그는 BUI 및 CLI에 로그인 및 로그아웃을 비롯한 사용자 작업 이벤트와 관리 작업을 기록합니다. 다음 표는 BUI에 나타나는 감사 로그 항목의 예를 보여줍니다.

표 2 감사 로그 레코드

시간	사용자	호스트	요약	세션 주석
2013-10-12 05:20:24	루트	galaxy	FTP 서비스가 사용 안함으로 설정되었습니다.	
2013-10-12 03:17:05	루트	galaxy	사용자가 로그인했습니다.	
2013-10-11 22:38:56	루트	galaxy	브라우저 세션 시간이 초과되었습니다.	
2013-10-11 21:13:35	루트	<console>	FTP 서비스가 사용으로 설정되었습니다.	

## Phone Home 로그

Phone Home을 사용하는 경우 이 로그에는 오라클 고객 지원 센터와 관련된 통신 이벤트가 표시됩니다. 다음 표는 BUI에 나타나는 Phone Home 항목의 예를 보여줍니다.

표 3 Phone Home 로그 레코드

시간	설명	결과
2013-10-12 05:24:09	'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' 파일을 오라클 고객 지원 센터에 업로드했습니다.	성공

## 추가 정보

Oracle ZFS Storage Appliance에 대한 전체 제품 정보는 다음 위치에서 찾을 수 있습니다.

<https://docs.oracle.com>

BUI를 사용하여 Oracle ZFS Storage Appliance를 구성하는 경우 화면의 오른쪽 위에 있는 Help(도움말) 링크를 누르면 해당 화면에 대한 도움말이 표시됩니다.