보안

Tibero
보안 가이드

TSEP002

Website
www.tmaxtibero.com

안내서 정보
안내서 제목: Tibero 보안 가이드
발행일: 2024-02-14
소프트웨어 버전: Tibero7 FS02
안내서 버전: 1.0

제, 개정 이력

안내서 버전	개정일자	개정 사유 및 내용	비고
1.0	2024.02.14	최초 제정	

목록

제 1장 계정 관리

본 장에서는 계정 관리에 대한 위험 분석, 위험 영향, 해결 방안을 설명한다.

1.1. 개발 및 운영 시스템 분리 사용

- 위험 분석

  개발 시스템과 운영 시스템을 하드웨어적으로 분리하여 Link가 설정되지 않아야 하며, 운영 시스템의 데이터를 개발 시스템으로 이전할 때 중요 데이터의 삭제 같은 통제와 검증 절차를 거쳐야 한다.

- 위험 영향

  운영 시스템의 중요 데이터가 개발 시스템으로 누출될 가능성이 있다.

- 해결 방안

  개발 시스템과 운영 시스템의 분리를 회사의 정책으로 정의하고 개발자와 운영자를 원칙적으로 분리한다. 만약 분리할 수 없다면 개발자가 운영 시스템에 접근할 경우 통제 절차를 거치도록 해야 한다.

1.2. DBA 권한 제한

- 위험 분석

  인가되지 않은 사용자가 DBA 권한으로 DBMS를 오용 및 남용할 수 있다.

- 위험 영향

  DBA 권한을 사용하여 시스템 장애 및 데이터베이스를 변조할 가능성이 있다.

- 해결 방안

  DBA 권한이 있는 계정의 사용자와 필요성을 확인한다. 만약 불필요하게 DBA 권한이 허용된 계정이 있으면 계정을 없애거나 DBA 권한을 제거하고 데이터 누출 및 유실을 막기 위해 보안 정책을 수립한다.

  다음은 DBA 권한 제거 방법이다.

  ```
  SQL> REVOKE DBA FROM <username>;
  ```

1.3. 디폴트 계정 사용

- 위험 분석

  잘 알려진 디폴트 계정과 디폴트 패스워드를 이용하여 데이터베이스에 접근할 수 있다.

- 위험 영향

  데이터베이스 접근 또는 상위 권한을 획득하여 데이터를 열람, 수정, 삭제할 수 있다.

- 해결 방안

  – OS, DB 레벨에서 원천적으로 접근을 제한하기 위해 사용하지 않는 애플리케이션 계정을 삭제한다.
  – 계정은 다른 용도로 사용하고 특정 데이터베이스의 접근만 제한해야 하는 경우 SUPER USER 또는 설치 계정의 GROUP에서 삭제한다.

1.4. 디폴트 DB 패스워드 사용

- 위험 분석

  디폴트 생성 DB 사용자(SYSCAT, SYSGIS, OUTLN, TIBERO, TIBERO1)의 디폴트 패스워드를 이용하여 인가되지 않은 사용자가 DBMS에 접근할 수 있다.

- 위험 영향

  데이터베이스 접근 및 상위 권한을 획득하여 데이터를 열람, 수정, 삭제할 수 있다.

- 해결 방안

  사용하지 않는 디폴트 DB 계정은 삭제하거나 Lock 시키고 사용하는 계정이라면 디폴트 패스워드를 수정한다.

  – 계정 Lock

```
SQL> ALTER USER <username> ACCOUNT LOCK;
```

  – 패스워드 변경

```
SQL> ALTER USER <username> IDENTIFIED BY '<new_password>';
```

1.5. 무제한 로그인 시도 차단

- 위험 분석

  무제한으로 로그인 시도가 가능한 경우 Brute Force 공격으로 무제한 로그인 시도가 발생할 수 있다.

- 위험 영향

  Brute Force 공격의 피해가 발생한다.

- 해결 방안

  로그인 실패 횟수를 설정하는 FAILED_LOGIN_ATTEMPTS 항목을 설정하여 일정 횟수로 로그인을 실패할 경우 계정이 Lock 되게 한다.

  profile은 사용자 패스워드 관리 정책을 다양하게 생성하고 각각의 사용자에게 특정 정책을 사용하도록 지정함으로써 사용자별로 그룹화된 패스워드 정책을 관리할 수 있는 기능을 제공한다.

  – profile 생성

```
SQL> CREATE PROFILE <profile_name>
     LIMIT PASSWORD_VERIFY_FUNCTION verify_function
     FAILED_LOGIN_ATTEMPTS <횟수>;
```

– profile 변경

```
SQL> ALTER PROFILE <profile_name> LIMIT FAILED_LOGIN_ATTEMPTS <횟수>;
```

– profile 할당

```
SQL> ALTER USER <username> PROFILE <profile_name>;
```

1.6. 패스워드 Lock 기간 설정 점검

- 위험 분석

  악의적인 사용자의 Brute Force 공격으로 무제한 로그인 시도가 발생할 수 있다.

- 위험 영향

  Brute Force 공격의 피해가 발생한다.

- 해결 방안

  패스워드 Lock 기간을 설정하는 PASSWORD_LOCK_TIME 항목을 설정하여 일정 시간 동안 로그인을 할 수 없도록 계정이 Lock 되게 한다. (기본값 : UNLIMITED, 권장값 : 1 또는 2 또는 24)

  – profile 변경

  ```
  SQL> ALTER PROFILE <profile_name> LIMIT PASSWORD_LOCK_TIME <시간>;
  ```

  – profile 할당

  ```
  SQL> ALTER USER <username> PROFILE <profile_name>;
  ```

1.7. 패스워드 주기적 변경

- 위험 분석

  DBA_USERS 계정에 대해 주기적으로 패스워드를 변경하지 않고 취약한 패스워드로 설정할 경우 인증되지 않은 사용자에게 DBA 또는 USER 권한을 줄 수 있다.

- 위험 영향

  권한이 노출되어 남용될 수 있다.

- 해결 방안

  profile의 PASSWORD_LIFE_TIME 항목 설정값을 변경한다. (기본값 : UNLIMITED, 권장값 : 30 ~ 90days)

  – profile 변경

  ```
  SQL> ALTER PROFILE <profile_name> LIMIT PASSWORD_LIFE_TIME <일수>;
  ```

  – profile 할당

  ```
  SQL> ALTER USER <username> PROFILE <profile_name>;
  ```

1.8. DB 계정에 대한 패스워드 재사용 기간 설정 점검

- 위험 분석

  DBA_USERS 계정의 패스워드를 변경할 때 패스워드 재사용 기간을 설정하지 않고 동일 패스워드를 사용할 경우 인증되지 않은 사용자에게 DBA 권한을 줄 수 있다.

- 위험 영향

  권한이 노출되어 남용될 수 있다.

- 해결 방안

  PASSWORD_REUSE_TIME에 지정한 날짜 동안에는 전에 사용했던 패스워드를 재사용하지 못하게 profile의 PASSWORD_REUSE_TIME 항목 설정값을 변경한다. (기본값 : UNLIMITED, 권장값 : 30 ~ 90 days)

  – profile 변경

  ```
  SQL> ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_TIME <일수>;
  ```

  – profile 할당

  ```
  SQL> ALTER USER <username> PROFILE <profile_name>;
  ```

제 2장 권한 관리

본 장에서는 권한 관리에 대한 위험 분석, 위험 영향, 해결 방안을 설명한다.

2.1. 개발 및 운영 시스템 분리 사용

- 위험 분석

  개발 시스템과 운영 시스템을 하드웨어적으로 분리하고 DB Link가 설정되지 않도록 해야 하며, 운영 시스템의 데이터를 개발 시스템으로 이전할 때 중요 데이터의 삭제 같은 통제와 검증 절차를 거쳐야 한다.

- 위험 영향

  운영 시스템의 중요 데이터가 개발 시스템으로 누출될 가능성이 있다.

- 해결 방안

  개발 시스템과 운영 시스템의 분리를 회사의 정책으로 정의하고 개발자와 운영자를 원칙적으로 분리한다. 만약 분리할 수 없다면 개발자가 운영 시스템에 접근할 경우 통제 절차를 거치도록 해야 한다.

2.2. SYSDBA 권한 제한

- 위험 분석

  DBA가 SYS 패스워드를 입력하지 않고 접근하면 그룹을 가진 멤버들이 SYS 권한으로 로그인이 가능하므로 SYS 암호를 반드시 입력해야 한다.

- 위험 영향

  인증 없이 SYS 권한 획득이 가능하다.

- 해결 방안

  Tibero에는 Oracle의 sqlplus /as sysdba와 같은 접속 방법이 없으므로 해당사항이 없다.

2.3. Listener 패스워드 설정 점검

- 위험 분석

  Listener를 구동 또는 중지하는 작업은 DBA와 같은 특권자에게만 부여하며 Listener에 대한 접근 통제를 위해 Listener 접근 패스워드를 설정해야 한다.

- 위험 영향

  비인가자의 Listener 접근이 가능하다.

- 해결 방안

  Tibero는 Listener와 서버 프로세스가 동시에 기동되기 때문에 해당사항이 없다.

2.4. 환경설정 파일 보호 점검

- 위험 분석

운영하는데 중요한 환경 파일을 아무나 접근해서 수정할 경우 침입자가 환경 파일을 열어 설정값을 바꾼 뒤 DB 운영에 영향을 줄 수 있다.

- 위험 영향

  악의적인 목적으로 파일을 변조할 수 있다.

- 해결 방안

  – OS 계정에 의해 수정 및 관리되도록 하고 일반 계정의 접근을 금지한다.
  – $TB_HOME/config/$TB_SID.tip 파일의 퍼미션값을 변경한다. (권장값 : 600 또는 640)

2.5. 중요 파일 소유자 또는 그룹 설정 점검

- 위험 분석

  중요 파일에 불필요한 소유권 또는 그룹 권한이 주어질 경우 해당 파일로 인해 인증되지 않은 사용자가 정보를 획득할 수 있다.

- 위험 영향

  시스템 또는 네트워크 환경설정 파일의 권한이 취약하게 설정되어 있거나 Tibero 사용자가 소유권을 가져야 하는 파일이 권한 없는 사용자의 소유로 되어 있으면 비인가자가 시스템 권한을 획득하거나 중요 데이터를 파괴할 수 있다.

- 해결 방안

  $TB_HOME/client/config/tbdsn.tbr 파일의 퍼미션값을 변경한다. (권장값 : 600 또는 640)

2.6. Public에 대한 권한 제한

- 위험 분석

  Object의 사용 권한을 Public에 부여하면 Object 사용 권한이 없는 모든 계정이 해당 Object에 접근 가능하고 Object의 정보를 획득할 수 있다.

- 위험 영향

  새로 생성된 계정의 Object 사용 권한이 Public에 불필요하게 부여된 경우 권한 남용의 위험이 있다.

참고

솔루션을 설치할 때 디폴트로 Object 사용 권한이 Public에 부여되거나 소유자가 시스템 계정인 경우에는 양호하다.

- 해결 방안

  Object의 사용 권한이 불필요하게 Public에 부여된 경우 권한을 제한한다.

  다음은 Public으로부터 권한을 제거하는 방법이다.

```
SQL> REVOKE <권한> ON <object> FROM PUBLIC
```

2.7. GRANT 옵션 사용 제한

- 위험 분석

  GRANT 옵션과 함께 권한을 받은 사용자는 해당 권한을 다른 사용자에게 부여할 수 있다.

- 위험 영향

  불필요하게 GRANT 옵션이 부여된 계정이 있는 경우 권한 남용의 위험이 있다. (담당자가 확인하여 권한이 필요하다고 인정하는 경우에는 제외)

- 해결 방안

  GRANT 옵션 권한 부여는 DBA만 할 수 있도록 제한한다. 불필요하게 GRANT 옵션이 부여된 계정은 권한을 제거하고 GRANT 옵션 없이 권한을 다시 부여한다.

  – 권한 REVOKE

  ```
  SQL> REVOKE <권한> ON <object명> FROM <user_name>;
  ```

  – 권한 GRANT

  ```
  SQL> GRANT <권한> ON <object명> TO <user_name>;
  ```

2.8. ADMIN 옵션 사용 제한

- 위험 분석

  ADMIN 옵션과 함께 시스템 권한을 받은 사용자는 해당 권한을 다른 사용자에게 부여할 수 있다.

- 위험 영향

  불필요하게 ADMIN 옵션이 부여된 계정이 있는 경우 권한 남용의 위험이 있다. (담당자가 확인하여 권한이 필요하다고 인정하는 경우에는 제외)

- 해결 방안

  ADMIN 옵션 권한 부여는 DBA만 할 수 있도록 제한한다. 불필요하게 ADMIN 옵션이 부여된 계정은 권한을 제거하고 ADMIN 옵션 없이 권한을 다시 부여한다.

  – 권한 REVOKE

  ```
  SQL> REVOKE <권한> ON <object명> FROM <user_name>;
  ```

  – 권한 GRANT

  ```
  SQL> GRANT <권한> ON <object명> TO <user_name>;
  ```

제 3장 DBMS 보안 설정

본 장에서는 DBMS 보안 설정에 대한 위험 분석, 위험 영향, 해결 방안을 설명한다.

3.1. 데이터 Dictionary 보호 설정 점검

- 위험 분석

  데이터 Dictionary는 물리적 및 논리적 구조, 객체 정의 및 공간 할당, 사용자, 룰, 권한, 감사 등 데이터베이스의 핵심에 해당하는 정보를 담고 있으므로 사용자 및 외부로부터 보호해야 한다. 보호되지 않을 경우 누구나 DROP ANY TABLE 명령어로 데이터 Dictionary의 내용을 삭제할 수 있다.

- 위험 영향

  데이터 Dictionary 정보의 삭제가 가능하다.

- 해결 방안

  Tibero는 해당 기능이 없으므로 해당사항이 없다.

3.2. Listener logging 설정 점검

- 위험 분석

  Listener logging 기능이 활성화 되어있지 않으면 공격자에 의한 악의적인 Listener command 사용 또는 Listener 패스워드를 알아내기 위한 Brute Force 공격의 파악이 불가능하게 된다.

- 위험 영향

  침해 사고 또는 장애 발생의 경우 원인 파악이 어렵다.

- 해결 방안

  $TB_HOME/instance/$TB_SID/log/lsnr/trace_list.log 파일을 디폴트로 남긴다.

3.3. tbdsn.tbr 설정 및 보호 점검

- 위험 분석

  Listener는 클라이언트로부터 접속 요구를 감시하는 프로세스로 클라이언트는 Listener를 통해 데이터베이스에 접속한다. Listener 설정 파일은 Listener가 기동할 때 읽혀져 클라이언트의 접근을 가능하게 하며 악의적인 사용자에 의해 사용될 경우 원격으로 Listener의 구성 설정을 변경할 수 있다.

- 위험 영향

  버퍼 오버플로우, 정보 유출, 악의적인 목적으로 파일을 변조할 수 있다.

- 해결 방안

  Tibero는 Oracle과 아키텍처 차이로 Listener가 별도로 존재하지 않는다.

참고

tbdsn.tbr 보호 점검에 대한 자세한 내용은 "2.4. 환경설정 파일 보호 점검"과 "4.5. TIP(Tibero Initialize Parameter) 파일 접근 권한 설정"을 참고한다.

3.4. 백업 관리

- 위험 분석

  백업 관리를 통해 장애 및 외부 침입에 대해서 대비해야 한다.

- 위험 영향

  데이터베이스의 장애가 발생할 경우 복구가 불가능하다.

- 해결 방안

  백업 정책을 수립하여 주기적인 백업 또는 각기 다른 미디어에 복사본을 보유하고 시스템 유지 보수, Upgrade, Migration 등의 서비스 운휴 및 수정 작업의 경우는 가장 가까운 시간까지의 백업본을 보유한다.

3.5. 로그 관리

- 위험 분석

  침해 사고가 발생할 경우 계정별 수행 Query와 시스템 및 응용 애플리케이션에 대한 로그를 관리한다.

- 위험 영향

  침해 사고 또는 장애 발생의 경우 원인 파악이 어렵다.

- 해결 방안

  데이터베이스에서 발생하는 각종 로그는 원격지 관리 시스템을 통해 일정 기간(3개월 이상) 저장 관리하여 특이사항이 발생할 경우 원활한 분석이 가능하도록 지원해야 한다.

3.6. PSM 패키지 사용

- 위험 분석

  UTL_FILE, UTL_SMTP 등 여러 PL/SQL 패키지는 시스템과 데이터베이스에 영향을 미치는 취약점을 가지고 있으므로 해당 패키지의 사용 권한이 Public에 부여되는 것을 제한해야 한다.

- 위험 영향

  파일 시스템의 접근 또는 내부 파일의 외부 유출이 가능하다.

- 해결 방안

  아래와 같은 패키지의 실행 권한을 사용하지 않는 경우 Public role에서 '실행 권한'을 제거한다.

```
UTL_HTTP, UTL_FILE, DBMS_RANDOM, DBMS_LOB, DBMS_SQL, DBMS_JOB,
DBMS_OBFUSCATION_TOOLKIT
```

- 패키지의 실행 권한 제거

```
SQL> REVOKE EXECUTE ON <패키지명> FROM PUBLIC;
```

제 4장 환경 파일 점검

본 장에서는 환경 파일 점검에 대한 위험 분석, 위험 영향, 해결 방안을 설명한다.

4.1. OS 명령어 히스토리 검사

- 위험 분석

  Tibero를 사용하여 DBMS에 접근할 경우 명령어 행의 계정 및 패스워드를 붙여서 사용하면 쉘 히스토리 (.history 또는 .sh_history) 파일에 사용한 계정과 패스워드의 기록이 남는다.

- 위험 영향

  계정 및 패스워드가 유출될 가능성이 있다.

- 해결 방안

  Tibero 명령을 사용할 경우 명령어 행에 계정과 패스워드를 Line Mode가 아닌 Interactive Mode로 실행한다.

  쉘 히스토리(.history 또는 .sh_history) 파일에 대한 보호를 위하여 접근 권한 설정을 600으로 설정한다.

참고

$ tbsql <username>/<password>로 접속하지 않는다.

4.2. UTL_FILE_DIR 사용 제한

- 위험 분석

  UTL_FILE_DIR은 UTL_FILE을 통해 호스트의 파일 시스템 접근 허용 디렉터리를 제한한다. 만약 UTL_FILE_DIR의 설정값이 '*'로 설정된 경우 전체 파일 시스템에 접근이 가능하므로 '*'로 설정할 경우에는 매우 제한적으로 사용해야 한다.

- 위험 영향

  호스트의 전체 파일 시스템에 접근이 가능하다.

- 해결 방안

  '*' 설정값을 제거한다.

4.3. UTL_SMTP 사용 제한

- 위험 분석

  UTL_SMTP 패키지를 Public 그룹에서 사용할 수 있도록 권한을 부여하면 허가받지 않은 메일의 전송이 발생할 수 있다.

- 위험 영향

  시스템 내부의 파일을 외부로 전송할 수 있다.

- 해결 방안

Public 그룹과 같은 사용자에게 권한을 부여하지 않고 특정 사용자에게 부여하여 해당 사용자에게만 메일이 전송될 수 있게 한다.

4.4. Sample DB 제거

- 위험 분석

  Tibero DBMS를 초기에 설치할 경우 디폴트로 포함되는 Sample DB(TEST DB)를 제거하여 DBMS 운영정보 관련 공격이 침투할 때 환경 정보를 제거한다.

- 위험 영향

  데이터베이스의 운영 환경정보 노출 가능성이 있다.

- 해결 방안

  Sample DB를 제거한다.

4.5. TIP(Tibero Initialize Parameter) 파일 접근 권한 설정

- 위험 분석

  Tibero의 중요 파일 중에 하나인 initialization 파일의 변경으로 시스템 장애가 발생한다.

- 위험 영향

  DB 기동 및 운영에 위협적인 영향을 줄 수 있다.

- 해결 방안

  $ chmod 640 $TB_HOME/config/$TB_SID.tip 파일의 접근 권한을 설정한다. (권장값 : 600 또는 640)

4.6. Control 파일, Redo 로그 파일, 데이터 파일 접근 제한

- 위험 분석

  Tibero의 중요 파일인 Control 파일, Redo 로그 파일, 데이터 파일의 삭제 및 변경으로 시스템 장애가 발생한다.

- 위험 영향

  DB 운영 정지 및 데이터의 유실 위험이 있다.

- 해결 방안

  Control 파일, Redo 로그 파일, 데이터 파일의 접근 권한을 설정한다. (권장값 : 600 또는 640)
  다음은 접근 권한을 640으로 설정했을 경우이다.

  ```
  $ chmod 640 [Control 파일|Redo 로그 파일|데이터 파일]
  ```

제 5장 보안 감사 설정

본 장에서는 보안 감사 설정에 대한 위험 분석, 위험 영향, 해결 방안을 설명한다.

5.1. 일반 계정의 System Catalog 접근 제한

- 위험 분석

  일반 계정으로 데이터베이스의 관리 및 통계 등의 Meta 데이터를 가지고 있는 System Catalog에 접근하여 데이터베이스의 정보를 획득할 수 있다.

- 위험 영향

  데이터베이스의 System Catalog 정보 유출 가능성이 있다.

- 해결 방안

  데이터베이스의 Meta 데이터를 가지고 있는 System Catalog는 소수의 데이터베이스 관리자만 사용할 수 있도록 설정한다.

  다음은 Public으로부터 권한을 제거하는 방법이다.

  ```
  REVOKE <privilege> ON <system catalog object> FROM PUBLIC;
  ```

5.2. 네트워크 액세스 제한

- 위험 분석

  원격 서버로부터 DBMS 정보가 노출될 수 있다.

- 위험 영향

  인가되지 않은 IP 주소 사용자에게 정보 유출 가능성이 있다.

- 해결 방안

  $TB_SID.tip 파일에 아래의 항목들을 정의하여 접근 허용 및 접근 제한 IP 주소를 지정한다.

  ```
  LSNR_INVITED_IP
  LSNR_DENIED_IP
  LSNR_INVITED_IP_FILE
  LSNR_DENIED_IP_FILE
  ```

  – 다음은 LSNR_INVITED_IP 항목의 등록 예제이다.

  ```
  LSNR_INVITED_IP="192.168.20.0/24;192.168.10.101"
  ```

  위와 같이 등록하면 $TB_HOME/instance/$TB_SID/log/lsnr/trace_list.log 파일에 다음과 같이 등록된다.

```
*** listener started and got into main loop ***
[INVITED-IP] 192.168.20.0 / 255.255.255.0
[INVITED-IP] 192.168.10.101 / 255.255.255.255
```

– 다음은 LSNR_INVITED_IP_FILE 항목의 등록 예제이다.

```
LSNR_INVITED_IP_FILE="/home/tibero/tibero7/invited.list"
```

위와 같이 등록한 후 LSNR_INVITED_IP_FILE 항목에 등록한 파일(invited.list)에 허용할 IP 주소 List를 작성한다.

```
# WAS_JEUS
192.168.22.20
192.168.44.10
### END OF FILE ###
```

5.3. DB Link 암호화 설정 점검

- 위험 분석

  DB Link는 클라이언트 또는 현재의 데이터베이스에서 네트워크 상의 다른 데이터베이스에 접속하기 위한 접속 설정을 정의하는 Tibero 객체이다. 클라이언트와 데이터베이스 간의 DB Link가 암호화되지 않으면 원격 서버에 접근할 경우 패스워드와 같은 중요 정보가 노출될 수 있다.

- 위험 영향

  악의가 있는 사용자가 스니핑 등의 네트워크 공격을 통해 패스워드를 노출할 가능성이 있다.

- 해결 방안

  Tibero는 DB Link를 설정할 때 원격 서버의 패스워드가 암호화되므로 해당사항이 없다.

5.4. Audit Trail 기록 설정

- 위험 분석

  감사를 수행할 수 있게 설정하여 사용자에 의한 문장, 권한, 객체에 대해 감사를 수행할 수 있다. 침해 사고 및 장애가 발생할 때 감사 자료를 이용하여 정확한 분석을 할 수 있다.

- 위험 영향

  침해 사고 또는 장애 발생의 경우 원인 파악이 어렵다.

- 해결 방안

  감사를 활성화하기 위하여 TIP 파일에 'AUDIT_TRAIL'의 값을 { NONE | DB | DB_EXTENDED | OS } 중에서 하나 선택한다.

  다음은 $TB_HOME/config/$TB_SID.tip 파일의 설정 예제이다.

```
#AUDIT Setting
AUDIT_TRAIL=OS
AUDIT_SYS_OPERATIONS=Y
AUDIT_FILE_DEST=/tibero/tbdata/audit/
```

5.5. Audit 로그 파일 접근 제한

- 위험 분석

  감사 로그를 다른 사용자가 읽기, 쓰기 할 수 있는 경우 서버의 중요 정보가 노출될 위험성이 있다.

- 위험 영향

  비인가 사용자에 의한 파일의 변조 및 노출이 가능하다.

- 해결 방안

  AUDIT_FILE_DEST에 설정된 경로의 디렉터리 권한을 750 또는 700 이하로 설정한다.