클라우드 취약점 점검 가이드

– 보안설정(CCE)

| 2020. 12 |

KISA 한국인터넷진흥원

클라우드 취약점 점검 가이드

〈 보안설정(CCE) 〉

2020. 12

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

1. 개요

2. 보안가이드

1. 개요

1.1. 개요

클라우드컴퓨팅서비스(이하 ‘클라우드서비스’) 보안인증제도는 클라우드서비스 제공자가 제공하는 서비스에 대해「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제23조 제2항에 따라 정보보호 기준의 준수여부를 확인을 인증기관에 요청하는 경우 인증기관이 이를 평가·인증하여 이용자들이 안심하고 클라우드서비스를 이용할 수 있도록 지원하는 제도입니다.

클라우드 보안 인증(CSAP)에서는 서면/현장평가, CCE*, CVE**, 시큐어코딩, 모의침투테스트에 대하여 평가를 진행하는데, CCE 취약점 점검은 시간이 많이 소요되고, 시스템에 대한 영향도 분석 및 각 시스템에 대한 조치방법 등을 충분히 숙지해야 평가 대응 및 조치가 가능하기에 시스템 담당자들의 어려움이 존재합니다. 이에 관련 담당자들의 이해를 돕고, 평가 대응 및 사전 준비가 용이하도록 CCE 취약점 가이드를 발간하게 되었습니다.

*CCE(Common Configuration Enumeration) : 취약한 설정에 대한 점검

**CVE(Common Vulnerabilities and Exposures) : OS, Application 고유의 취약점

1.2. 목적 및 활용

본 가이드는 클라우드 보안 인증 담당자 및 클라우드 담당자의 역량강화를 위해 CCE 취약점에 대한 기술적 보안 가이드를 제공합니다. 전체 21종의 보안 가이드를 제공하며, 각각은 진단항목, 항목설명, 진단기준, 진단방법, 조치방법으로 구성되어 있습니다. 클라우드 보안 인증을 위한 담당자 및 클라우드 서비스의 보안수준 향상을 위한 클라우드 정보보호 담당자 등이 취약점 보안조치 관련하여 본 가이드를 활용할 수 있습니다.

1.3. 유의 사항

본 가이드는 클라우드 인증 심사 시 취약점 점검(CCE) 평가 항목별 점검 기준 및 방법에 대한 이해를 돕기 위해 발간된 것으로, 수록된 점검 방법은 클라우드 인증 심사 기준이며 클라우드 환경에서 절대적이지 않습니다. 운영되는 서비스, 활용되는 기능 및 세부 버전 패치 등에 따라 점검 방법과 판단기준은 변경될 수 있습니다. 따라서 본 가이드에 수록된 내용 이외에도 다양한 점검 및 조치를 수행할 수 있습니다.

본 가이드의 수록된 판단기준은 클라우드 인증평가 시 사용되고 있는 사항이며, 양호 혹은 취약을 가르는 실제 판단기준은 각 클라우드 서비스 운영에 따라 다양한 환경, 정책 등 고려하여 심사원이 최종적으로 결정합니다. 예를 들어 가이드에 수록된 판단기준에 의하여 취약판단을 받게 되어도 환경, 정책 등 합당한 보안조치와 근거를 수반하고 있다면 양호로 판단할 수 있습니다.

1.4. 위험도 기준

상	장비의 관리자 권한을 직접 획득하거나 장비의 중요한 정보를 유출시켜 직접적인 영향을 줄 수 있는 취약점
중	간접적으로 접근경로를 제공하거나 정보유출의 가능성을 높일 수 있는 취약점
하	취약점 이용하여 해킹에 성공하더라도 장비 및 다른 장비에 주는 영향 및 효과를 줄 수 없는 취약점

2. 보안가이드

2.1. XenServer

계정 관리(7개 항목), 파일 시스템(12개 항목), 네트워크 서비스 및 주요 응용 설정(5개 항목), 하이퍼바이저 정책 설정(3개 항목), 패치 및 로그관리(6개 항목) 총 5개 영역에서 33개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	XE-01	Default 계정 관리	중
	XE-02	일반계정 root 권한 관리	상
	XE-03	passwd파일 권한 설정	상
	XE-04	group 파일 권한 설정	상
	XE-05	패스워드 사용규칙 적용	중
	XE-06	로그인이 불필요한 계정 shell 제한	중
	XE-07	SU(Select User)사용 제한	중
나. 파일 시스템	XE-08	사용자 UMASK(User mask) 설정	하
	XE-09	SUID(Set User-ID), SGID(Set Group-id)	하
	XE-10	xsconsole 파일 권한 설정	상
	XE-11	Crontab 파일 권한 설정 및 관리	하
	XE-12	/etc/profile 파일 권한 설정	중
	XE-13	/etc/hosts 파일 권한 설정	중
	XE-14	/etc/issue 파일 권한 설정	중
	XE-15	사용자 홈 디렉터리 및 파일 관리	하
	XE-16	주요 디렉터리 파일 권한 설정	중
	XE-17	PATH 환경변수 설정	중
	XE-18	/etc/service 파일 권한 설정	중
	XE-19	부팅스크립트 파일 권한 설정	상
다. 네트워크 서비스 및 주요 응용 설정	XE-20	서비스 Banner 관리	중
	XE-21	session timeout 설정	하
	XE-22	root 계정의 ssh 및 sftp 접근 제한	상
	XE-23	SSH(Secure Shell)버전 취약점	중
	XE-24	불필요한 서비스 제거	하
라. 하이퍼바이저 정책 설정	XE-25	관리용 원격 접근 제어	상
	XE-26	Remote Shell 접근 제어	상
	XE-27	Guest VM 네트워크 분리	상
마. 패치 및 로그관리	XE-28	SU 로그 설정	상
	XE-29	syslog 설정	상
	XE-30	syslog 전송 포트 차단	상
	XE-31	로깅 수준 설정	하
	XE-32	로그 파일 권한 설정	하
	XE-33	보안패치 적용	상

[표 1] XenServer 진단 체크리스트

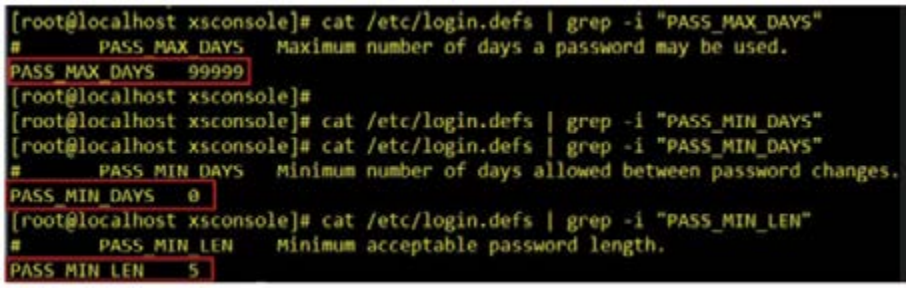
가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">XE-01. Default 계정 관리</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템에서 이용하지 않는 Default 계정 및 의심스러운 특이한 계정의 존재 유무를 검사하여 삭제한다. 대부분의 시스템에서 사용하지 않는 것이 확실한 아래의 계정들과 의심스러운 계정을 삭제하도록 하며 일반적으로 로그인이 필요치 않은 시스템 계정들은 로그인을 금지시킨다. OS나 Package 설치 시 Default로 생성되는 계정은 대부분 Default 패스워드를 사용하는 경우가 많으며 패스워드 추측공격에 악용될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">OS 나 Package 설치 시 기본으로 생성되는 불필요한 계정이 존재하지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">OS 나 Package 설치 시 기본으로 생성되는 불필요한 계정이 존재할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ lp, uucp, nuucp 의심스러운 특이한 계정(예. guest, test) 및 미사용 계정의 존재 유무 확인
cat /etc/passwd | egrep “lp|uucp|nuucp” | grep –v “lpd”</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ 불필요한 계정 삭제
userdel lp
userdel uucp
userdel nuucp</td></tr>
<tr><td>비고</td><td colspan="4">▪ 퇴직, 전배, 휴직, 계약해지자 계정 존재 시 삭제
▪ lp, uucp, nuucp, 의심스러운 특이한 계정(예. guest, test) 및 미사용 계정 삭제
▪ 로그인 쉘을 /bin/false로 수정하는 것은 보안상 문제가 발생할 수 있으므로 삭제를 권고함</td></tr>
</table>

진단항목	XE-02. 일반계정 root 권한 관리		취약도	상
항목설명	시스템 관리자는 root계정을 포함하여 모든 계정의 의심 가는 디렉터리 및 파일을 정기적으로 조사하여 삭제하며, 주기적으로 불필요한 사용자 계정을 조사하여 제거하는 것이 보안상 필요하다.			
진단기준	양호	root 및 시스템 계정(daemon, bin, adm, uucp, nuucp, lp, hpdb 등)을 제외하고 UID가 0인 계정이 존재하지 않는 경우		
	취약	root 및 시스템 계정(daemon, bin, adm, uucp, nuucp, lp, hpdb 등)을 제외하고 UID가 0인 계정이 존재하는 경우		
진단방법	<XenServer> ■ /etc/passwd파일의 필드 3번째 값 확인(UID:0인지 확인) # cat /etc/passwd (예시) test:x:101:101:test:/home/test:/bin/bash			
조치방법	<XenServer> ■ root, 시스템 계정의 UID가 0인 계정의 UID 값 변경 (예시) test 계정의 UID를 2002로 바꿀 경우 # usermod –u 2002 test			
비고				

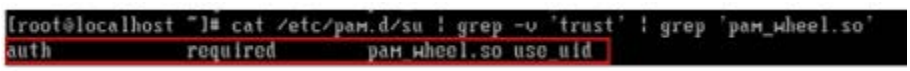
<table>
<tr><td>진단항목</td><td colspan="2">XE-03. passwd 파일 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">"/etc/passwd" 파일의 접근권한을 제한하고 있는지 점검한다. 파일의 설정 상의 문제점이나 파일 permission 등을 점검하여 관리자의 관리상의 실수나 오류로 발생할 수 있는 침해사고(일반 사용자 권한 /root 권한 획득)의 위험성을 점검한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 파일의 소유자가 root이고 권한이 644(rw-r--r--)인 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 파일의 소유자가 root가 아니거나 타사용자에게 쓰기 권한 및 접근권한이 존재할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/passwd 파일의 접근권한 확인
ls –al /etc/passwd
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/passwd 파일의 권한 변경
chmod 644 /etc/passwd
chown root /etc/passwd</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-04. group 파일 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Group파일을 일반사용자가 접근하여 변조하게 되면 인가되지 않은 사용자가 root 그룹으로 등록되어 인가되지 않은 사용자의 root권한 획득이 가능하다. Group 파일을 일반 사용자들이 수정할 수 없도록 제한하고 있는지 점검하여 타사용자의 쓰기 권한을 제한하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/group 파일의 소유자가 root(또는 bin)이고 권한이 644(rw-r—r--)인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/group 파일의 소유자가 root(또는 bin)가 아니거나 타사용자에게 쓰기 권한 및 접근 권한이 존재할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/group 파일의 접근권한 확인
ls –al /etc/group
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/group 파일의 권한 변경
chmod 644 /etc/group
chown root /etc/group</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-05. 패스워드 사용규칙 적용</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드 추측공격을 피하기 위하여 패스워드 최소길이가 설정되어 있는지 점검한다. 패스워드 최소길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 정책에 따른 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 정책에 따라 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ 패스워드 최대 사용기간, 최소 사용기간, 최소길이 설정 확인 (단위: 일)
cat /etc/login.defs | grep –i “PASS_MAX_DAYS”
cat /etc/login.defs | grep –i “PASS_MIN_DAYS”
cat /etc/login.defs | grep –i “PASS_MIN_LEN”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/login.defs에서 패스워드 최대 사용기간은 90일, 최소 사용기간은 1일 설정으로 변경 (단위: 일)
vi /etc/login.defs
PASS_MIN_LEN 8
PASS_MAX_DAYS 90
PASS_MIN_DAYS 1</td></tr>
<tr><td>비고</td><td colspan="4">■ 패스워드 최소길이 : 패스워드 추측공격을 피하기 위하여 패스워드 최소길이가 설정되어 있는지 점검. 패스워드 최소길이가 설정되어 있지 않거나 짧게 설정되어 있을 경우 취약한 패스워드를 사용함으로 인해 악의적인 사용자가 패스워드를 쉽게 유추 가능
■ 패스워드 최대 사용기간 : 패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검
■ 패스워드 최소 사용기간 : 패스워드를 변경하고 난 이후에 최소 사용기간 안에 패스워드를 변경할 수 없도록 설정</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-06. 로그인이 불필요한 계정 shell 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">접근이 거의 필요하지 않은 사용자들에게는 쉘을 제한함으로써 비인가적인 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">시스템 계정 중 로그인이 불필요한 계정에 대해 shell이 제한되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">시스템 계정 중 로그인이 불필요한 계정에 대해 shell이 제한되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ /etc/passwd 파일의 계정 별 shell 확인
cat /etc/passwd
(예시) nobody:x:65534:65534:nobody:/nonexistent:/bin/sh

※ 실행 쉘이 불필요한 계정 및 로그인이 필요하지 않은 계정에 nologin shell 부여 (daemon, bin, sys, listen, adm, nobody, nobody4, noaccess, diag, operator, games, gopher등 일반적으로 UID100 이하 60000 이상의 시스템 계정들)</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ 로그인이 필요 없는 계정의 shell 설정 변경
1) # vi /etc/passwd를 실행하여 아래와 같은 설정으로 변경 (단위:주)
예) daemon 계정이 로그인 하지 못하도록 설정
vi /etc/passed
daemon:x:1:1::/:/sbin/ksh (수정 전)
daemon:x:1:1::/:/bin/false (수정 후)</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-07. SU(Select User)사용 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">권한이 없는 일반 사용자가 su 명령을 사용한 Password Guessing을 통해 root 권한을 획득할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/pam.d/su 파일에 auth required pam_wheel.so use_uid 라인에 주석(#)이 없고 /etc/group 파일의 wheel 그룹에 계정이 제한되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/pam.d/su 파일에 auth required pam_wheel.so use_uid 라인에 주석(#)이 없고 /etc/group 파일의 wheel 그룹에 계정이 제한되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ /etc/pam.d/su에서 주석 여부 확인
cat /etc/pam.d/su | grep –v ‘trust’ | grep ‘pam_wheel.so’ | grep ‘use_uid’
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ SU 사용 제한 설정
1) /etc/pam.d/su 파일을 아래와 같이 설정.
auto sufficient /lib/security/pam_rootok.so
auto required /lib/security/pam_wheel.so use_uid
 

2) wheel group 생성
groupadd wheel
3) /etc/group 파일에서 wheel 그룹에 su 명령어를 사용할 사용자를 추가
usermod –G wheel username</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

나. 파일 시스템

<table>
<tr><td>진단항목</td><td colspan="2">XE-08. 사용자 UMASK(User Mask) 설정</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템 내에서 유저가 새로이 생성하는 파일의 접근 권한은 UMASK에 따라 달라진다. 현재의 유저에게 설정된 UMASK를 조회하려면, 명령 프롬프트에서 “umask”를 수행하면 된다. 그리고 UMASK 값이 “022”이기를 권장한다. UMASK값 “022”는 “rw-r--r--” 접근권한으로 파일이 생성된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">현재 시스템의 UMASK가 022 또는 027로 설정되어 있으며 Start Profile에 UMASK가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">현재 시스템의 UMASK가 설정되어 있지 않거나 022 또는 027이 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ UMASK 확인
1) /etc/pam.d/su 파일을 아래와 같이 설정
umask
cat /etc/profile | grep –i “umask”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ UMASK 변경
1) /etc/pam.d/su 파일을 아래와 같이 설정
umask 022
vi /etc/profile
umask 022 행 추가

※ 계정의 Start Profile(/etc/profile, /etc/default/login. .cshrc, .kshrc, .bashrc, .login, .profile등)에 명령을 추가하면, 유저가 로그인 후에도 변경된 UMASK 값을 적용 받음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-09. SUID(Set User-ID), SGID(Set Group-ID)</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">SUID(Set User-ID)와 SGID(Set Group-ID)가 설정된 파일의 경우, 특히 root 소유의 파일인 경우, BufferOverflow 공격과 Local 공격에 많이 사용되는 매우 보안상 관리가 필요한 파일들로 이들 파일들의 주기적인 관리가 필요하다. 보안에 취약한 root 소유의 setuid 파일들의 경우에는 꼭 필요한 파일을 제외하고는 그 외 setuid, setgid 파일에 대하여 setuid, setgid 속성을 제거해주고, 잘못 설정되어 보안 위협이 되고 있는지 주기적인 점검 및 관리가 요구된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 SUID, SGID가 설정되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 SUID, SGID가 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ SUID, SGID 검색
find / -user root –type f ₩(-perm –400 –o –perm –2000 ₩) -exec ls –lg {} ₩;
불필요한 Setuid, Setgid 목록
<table><tr><th colspan="3">XenServer</th></tr><tr><td>/sbin/dump</td><td>/usr/bin/lpd-lpd</td><td>/usr/bin/newgrp</td></tr><tr><td>/sbin/restore</td><td>/usr/bin/lpr</td><td>/usr/sbin/lpc</td></tr><tr><td>/sbin/Linux_chkpwd</td><td>/usr/bin/lpr-lpd</td><td>/usr/sbin/lpc-lpd</td></tr><tr><td>/usr/bin/at</td><td>/usr/bin/lprm</td><td>/usr/sbin/traceroute</td></tr><tr><td>/usr/bin/lpq</td><td>/usr/bin/lpm-lpd</td><td></td></tr></table></td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ 불필요한 SUID, SGID 제거
chmod –s [파일명]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-10. xsconsole 파일 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">xsconsole 파일에 대한 접근권한을 제한하고 있는지 점검한다. xsconsole은 XenServer Configuration 프로그램을 실행시켜주는 역할을 한다. xsconsole의 접근권한 설정이 잘못 설정되어 있을 경우 비 인가된 공격자가 설정을 변경할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/usr/bin/xsconsole 파일의 소유자가 root이고, 타사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/usr/bin/xsconsole 파일의 소유자가 root가 아니거나, 타사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /usr/bin/xsconsole 파일의 접근권한 확인
ls –al /usr/bin/xsconsole
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ xsconsole 파일 소유자를 root로 변경 및 타사용자 권한 제거
1) xsconsole 파일 소유자를 root로 변경
chown root /usr/bin/xsconsole
2) xsconsole 파일에 타사용자 권한을 제거
chmod o-w /usr/bin/xsconsole

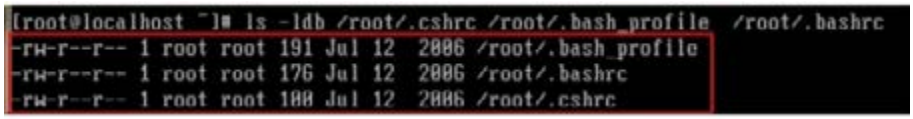
※ 해당 파일에 링크가 설정되어 있다면 링크된 원본 파일 소유자를 변경함</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-11. Crontab 파일 권한 설정 및 관리</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자가 cron관련 파일에 악의적으로 접근 권한을 제한하고 있는지 점검한다. Cron은 작업 스케줄링 기능을 제공하는 프로그램이며, 특정시간에 특정작업을 자동으로 수행하도록 하는 프로그램을 말한다. Cron 관련 파일의 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">cron 파일 소유자가 root이고, 타사용자의 쓰기권한이 없고 예약 실행 파일의 소유자가 root이고, 실행 파일이 744로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">cron 파일 소유자가 root가 아니거나, 타사용자의 쓰기권한이 존재하는 경우 또는 예약 실행 파일의 소유자가 root가 아니거나, 실행 파일이 744로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ Crontab 관련 파일의 소유자 및 권한 확인
(예시) # ls –al/etc/crontab
아래 파일의 소유자 및 권한 확인필요
/etc/crontab, /etc/cron.daily/*, /etc/cron.hourly/*, /etc/cron.monthly/*, /etc/cron.weekly/*, /var/spool/cron/*
■ Crontab 예약 실행 파일 소유자 및 권한 확인
(예시) # crontab –l
1 15 * * /backup/OS_backup.sh
30 * * * * /opt/sfm/vacuum
ls –al /backup/OS_backup.sh
ls –al /opt/sfm/vacuum</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ Crontab 관련 파일에 타사용자 쓰기 권한 제거
chmod o-w /etc/crontab
chmod o-w /etc/cron.daily/*
chmod o-w /etc/cron.hourly/*
chmod o-w /etc/cron.monthly/*
chmod o-w /etc/cron.weekly/*
chmod o-w /var/spool/cron/*
■ Crontab 예약 파일 소유자
ls -al [file]
chmod 744 [file]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-12. /etc/profile 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자 설정파일인 /etc/profile 파일에 대한 접근을 제한하고 있는지 점검한다. /etc/profile 파일은 로그인하는 모든 사용자들의 기본 사용 환경 설정을 위한 로그인 스크립트이다. /etc/profile 의 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/profile의 소유자가 root(또는 bin)이고, 타사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/profile의 소유자가 root(또는 bin)가 아니거나, 타사용자의 쓰기권한이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/profile 파일의 소유자 및 권한 확인
ls –al /etc/profile
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/profile 파일 소유자 변경 및 타사용자 쓰기 권한 제거
1) etc/profile 파일 소유자 변경
chown root /etc/profile
2) /etc/profile 타사용자 쓰기 권한 제거
chmod o-w /etc/profile</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-13. /etc/hosts 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">호스트네임 등록파일인 /etc/hosts/ 파일에 대한 접근 권한을 제한하고 있는지 점검한다. /etc/hosts 파일은 IP address 와 Host name을 매핑하는데 사용되는 파일이며 이 파일의 접근권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/hosts 파일의 소유자가 root (또는 bin)이고, 권한에 타사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/hosts 파일의 소유자가 root (또는 bin)가 아니거나, 권한에 타사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/hosts 파일의 소유자 및 권한 확인
ls –al /etc/hosts
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/hosts 파일 소유자 변경 및 타사용자 쓰기 권한 제거
1) /etc/hosts 파일 소유자 변경
chown root /etc/hosts
2) /etc/hosts 타사용자 쓰기 권한 제거
chmod o-w /etc/hosts</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-14. /etc/issue 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">터미널 설정과 관련된 /etc/issue 파일에 대한 접근 권한을 제한하고 있는지 점검 한다</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/issue 파일의 소유자가 root (또는 bin)이고 권한에 타사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/issue 파일의 소유자가 root (또는 bin)가 아니거나 권한에 타사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/issue 파일의 소유자 및 권한 확인
ls –al /etc/issue
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/issue 파일 소유자 변경 및 타사용자 쓰기 권한 제거
1) /etc/issue 파일 소유자 변경
chown root /etc/issue
2) /etc/issue 타사용자 쓰기 권한 제거
chmod o-w /etc/issue</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-15. 사용자 홈 디렉터리 및 파일 관리</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">각각의 사용자의 홈 디렉터리 내의 파일을 인가되지 않은 사용자가 접근하여 설정파일 및 파일을 변조하게 되면 정상적인 사용자의 서비스가 제한된다. 해당 홈 디렉터리의 계정 외의 일반 사용자들이 해당 홈 디렉터리를 수정할 수 없도록 제한하고 있는지 점검한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">User별 홈 디렉터리의 타 사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">User별 홈 디렉터리의 타 사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
<XenServer>
■ 사용자 홈 디렉터리 및 파일 권한 확인
1) /etc/passwd 파일에서 사용자 홈 디렉터리 확인
2) cd [사용자 홈 디렉터리]
3) ls –al [사용자 홈 디렉터리]
 

※ 사용자 홈 디렉터리 안의 아래 파일 확인
.profile", ".kshrc", ".cshrc", ".bashrc", ".bash_profile", ".login", ".exrc", ".netrc", ".dtprofile", ".Xdefaults"</td></tr>
<tr><td>조치방법</td><td colspan="4">
<XenServer>
■ 사용자 홈 디렉터리 안의 설정 파일에 타사용자 쓰기 권한 제거
chmod o-w [홈 디렉터리 경로] [파일명]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-16. 주요 디렉터리 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">주요 디렉터리의 파일 권한이 적절히 설정되어 있는지 점검한다. 주요 디렉터리 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">디렉터리의 권한을 root(또는 bin) 소유의 타 사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">디렉터리의 권한을 root(또는 bin) 소유의 타 사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ 주요 디렉터리의 권한 확인
ls –ldb /usr/bin/xsconsole /usr/lib/xsconsole /opt /sbin /etc/ /bin /usr/bin/ / usr/sbin/
 

주요 디렉터리 목록
<table><tr><th colspan="3">주요 디렉터리 목록</th></tr><tr><td>/usr/bin/xsconsole</td><td>/opt</td><td>/sbin</td></tr><tr><td>/usr/lib/xsconsole</td><td>/etc</td><td>/bin</td></tr><tr><td>/usr/sbin</td><td>/usr/bin</td><td></td></tr></table></td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ 디렉터리 소유자 변경 및 타사용자 쓰기 권한 제거
1) 디렉터리 소유자 변경
chown root [디렉터리명]
2) 디렉터리 권한 변경
chmod o-w [디렉터리명]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-17. PATH 환경변수 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">root 계정의 PATH 환경변수에 “.” (현재 디렉터리 지칭)가 포함되어 있으면, root 계정의 인가자로 인해 비의도적으로 현재 디렉터리에 위치하고 있는 명령어가 실행될 수 있다. 즉 “.”이 /usr/bin이나 /bin, /sbin 등 명령어들이 위치하고 있는 디렉터리보다 우선하여 위치하고 있을 경우, root 계정의 인가자가 어떠한 명령을 실행했을 때, 비인가자가 불법적으로 위치시킨 파일을 비의도적으로 실행하여, 예기치 않은 결과를 가져올 수 있다. 또한 “.” 뿐만 아니라 비인가자가 불법적으로 생성한 디렉터리를 우선적으로 가리키게 하여 예기치 않은 결과를 가져올 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">현재 위치를 의미하는 . 이 없거나, PATH 맨 뒤에 존재하는 경우</td></tr>
<tr><td>취약</td><td colspan="3">현재 위치를 의미하는 . 이 앞이나 중간에 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ PATH 설정 확인
echo $PATH
 
</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ root 계정의 환경변수 설정파일(.profile, .cshrc등)과 “/etc/profile” 등에서 PATH 환경변수에 포함되어 있는 현재 디렉터리를 나타내는 “.”을 제거</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-18. /etc/service 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Service 파일을 관리자가 아닌 일반사용자들이 접근 및 변경 가능하면 이를 통해 정상적인 서비스를 제한하거나 허용되지 않은 서비스를 실행시켜 침해사고의 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/service 파일의 소유자가 root (또는 bin)이고 권한에 타사용자의 쓰기권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/service 파일의 소유자가 root (또는 bin)가 아니거나 권한에 타사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/service 권한 확인
ls –alL /etc/services
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/services 소유자 변경 및 타사용자 쓰기 권한 제거
1) /etc/service 파일 소유자 변경
chown root /etc/service
2) /etc/service 파일 타사용자 쓰기 권한 제거
chmod o-w /etc/service</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-19. 부팅스크립트 파일 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">OS상에서 사용하는 기타 중요파일에 대하여 접근 권한을 제한하고 있는지 점검한다. 시스템 운영상 중요한 파일들의 접근권한은 반드시 필요한 사용자만 접근할 수 있도록 해야 한다. 기타 다음과 같은 중요파일의 권한 중 타사용자 쓰기 권한이 부여되어 있을 경우 제거한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">기타 중요파일의 소유자가 root (또는 bin)이고 권한에 타사용자의 쓰기 권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">기타 중요파일의 소유자가 root (또는 bin)가 아니거나 권한에 타사용자의 쓰기권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ 기타 중요파일 권한 확인
ls –alL /opt/*/*

기타 중요파일 목록
<table><tr><th colspan="3">기타 중요 파일 목록</th></tr><tr><td>/opt/*/*</td><td>/etc/rc*.d</td><td>/etc/inittab</td></tr><tr><td>/etc/syslog.conf</td><td>/etc/snmp/snmpd.conf</td><td>/etc/crontab</td></tr><tr><td>/etc/cron daily/*</td><td>/etc/cron hourly/*</td><td>/etc/cron monthly/*</td></tr><tr><td>/etc/cron weekly/*</td><td>/etc/spool/cron/*</td><td></td></tr></table></td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ 기타 중요 파일 소유자 변경 및 타사용자 쓰기 권한 제거
1) 기타 중요 파일 소유자 변경
chown root [기타 중요 파일]
2) 기타 중요 파일 타사용자 쓰기 권한 제거
chmod o-w [기타 중요 파일]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

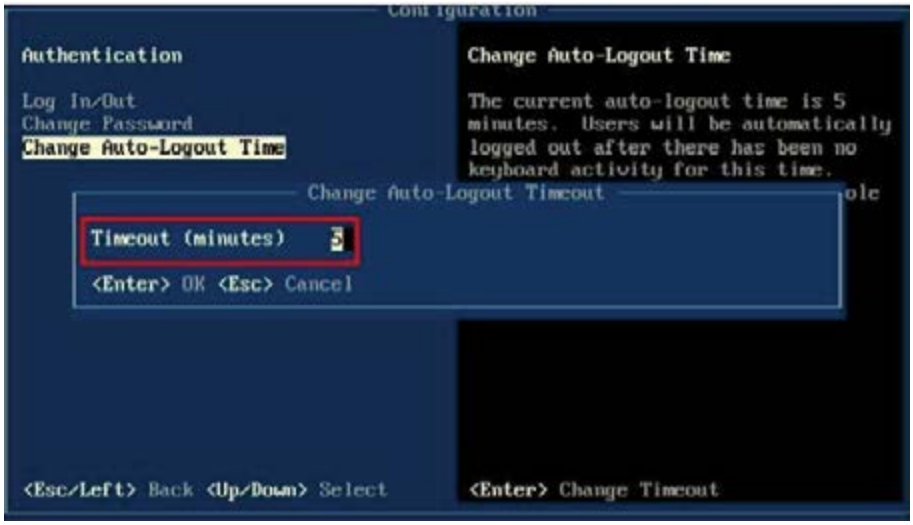
다. 네트워크 서비스 및 주요 응용 설정

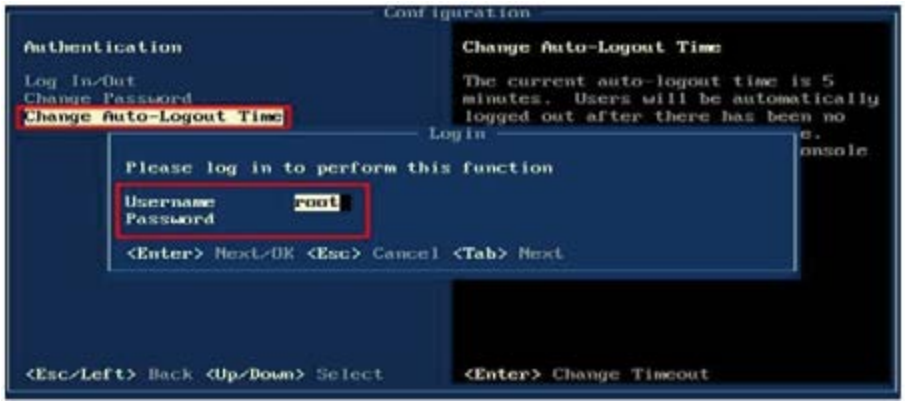
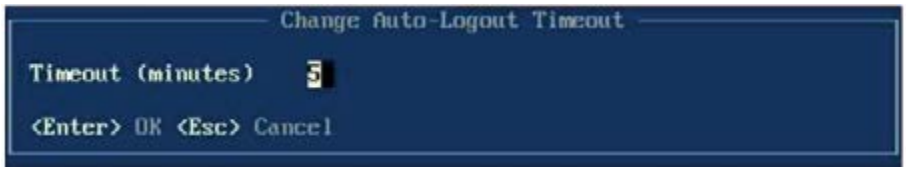
<table>
<tr><td>진단항목</td><td colspan="2">XE-20. 서비스 Banner 관리</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템에 일반적인 서비스(SSH, SFTP 등)의 접근 시 출력되는 Banner를 관리하여 서비스 버전 유출을 막는다. 서버 사용자 범위를 명시하고, 모든 활동이 모니터링 되고 있음을 표시한다. 해당 프로세스의 버전과 시스템의 호스트 명이 노출되지 않도록 배너를 설정한다.

※ sshd_config 설정에 따라 Banner 파일 위치가 다를 수 있음</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Banner에 경고 문구가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Banner에 경고 문구가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ Banner 확인
1) 배너파일이 존재하는 경로 확인
cat /etc/ssh/sshd_config | grep “Banner”
2) 위에서 확인한 경로에서 배너 내용 확인</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ /etc/ssh/sshd_config 파일에 Banner 설정
vi /etc/ssh/sshd_config
Banner /etc/issue.net
■ /etc/issue.net 파일을 생성하고 경고 메시지 삽입(예시)
##
This system is for the use of authorized users only.
Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
##</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-21. session timeout 설정</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">지정된 시간 동안 사용하지 않을 경우 접속된 session을 해당 서버에서 끊도록 설정하였는지 점검한다. 사용하지 않는 session에 대한 time out을 설정하지 않을 경우 기밀성뿐만 아니라 가용성 측면에서도 문제점을 발생 시킬 수 있다. 지정된 시간 동안 사용하지 않을 경우 접속된 session을 해당 서버에서 끊도록 설정하는 것이 필요하다. (300초 경과 시 timeout)</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"/etc/profile"과 "xsconsole"에 time out이 모두 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"/etc/profile"과 "xsconsole" 한쪽에만 time out이 설정되어 있거나 둘 다 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer 및 xsconsole>
■ /etc/profile에서 session timeout 설정 확인
1) # cat /etc/profile | grep "TMOUT"
 
■ xsconsole에서 session timeout 설정 확인
1) xsconsole > Authentication > Change Auto-Logout Time > Time out(minutes) 에서 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer 및 xsconsole>
■ /etc/profile 파일에서 설정
1) /etc/profile 파일 안에 time out 설정</td></tr>
</table>

	# vi /etc/profile TMOUT = 300 export TMOUT ■ xsconsole에서 설정 1) xsconsole > Authentication > Change Auto-Logout Time > 로그인  2) Timeout (minutes)에서 설정 
비고	

진단항목	XE-22. root 계정의 ssh 및 sftp 접근 제한	취약도	상
항목설명	root로 직접적인 원격 접근은 보안상 위험하므로, 일반 사용자를 통해 su 명령어를 이용하여, root로 접근할 수 있도록 하는 것이 보안상 필요하다. 어느 계정을 통해 root (슈퍼 user)로 접근했는지 알기 위해 보안상 필요하다.		
진단기준	양호	root 계정으로 ssh 및 sftp 접근이 제한되어 있는 경우	
	취약	root 계정으로 ssh 및 sftp 접근이 제한되어 있지 않은 경우	
진단방법	<XenServer> ■ root 계정 원격 접속 제한 설정 확인 1) /etc/pam.d/login 파일 설정 확인 # cat /etc/pam.d/login | grep "pam_securetty.so" auth required pam_securetty.so 또는, auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so 또는, auth required /lib/security/pam_securetty.so 2) /etc/ssh/sshd_config파일 설정 확인 # cat /etc/ssh/sshd_config | grep "PermitRootLogin" PermitRootLogin no		
조치방법	<XenServer> ■ root 원격 접속 제한 설정 1) /etc/pam.d/login 파일설정에 추가 설정 # vi /etc/pam.d/login auth required /lib/security/pam_securetty.so 2) /etc/ssh/sshd_config 파일 설정 수정(주석제거 또는 신규 삽입) # vi /etc/ssh/sshd_config PermitRootLogin no		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">XE-23. SSH(Secure Shell)버전 취약점</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">OpenSSh는 SSH(Secure SHell) 프로토콜을 구현한 오픈 소스 프로그램으로 telnet, ftp, rlogin, rsh 등을 대체하고 있다. OpenSSH는 네트워크 트래픽을 암호화하여 패킷 스니핑과 같은 공격으로부터 중요한 데이터를 보호할 수 있다. 그러나, OpenSSH의 낮은 버전에서는 다수의 취약점이 발견되고 있으며, 이러한 취약점으로 인해 root권한 획득, DoS공격 등 다양한 공격의 대상이 될 수 있다. Citrix에서는 Xenserver 서버에 접근하기 위한 프로토콜로서 SSH를 사용하고 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">벤더 사가 권장하는 OpenSSH 버전일 경우</td></tr>
<tr><td>취약</td><td colspan="3">취약한 OpenSSH 버전일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ ssh 버전 확인
1) /etc/pam.d/login 파일 설정 확인
ssh -V</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ ssh 서비스 필요 시
1) OpenSSH 업데이트 권장
■ ssh 서비스 불필요 시
1) 실행중인 서비스 중지
ps -ef | grep sshd
root 414 0.0 0.7 2672 1692 /usr/sbin/sshd
kill 9 414
2) SSH가 시작되지 않도록 시작스크립트의 파일 명 변경
※ OS마다 시작스크립트 위치 상이

ls –al /etc/rc*.d/* | grep sshdz (시작스크립트 파일 위치 확인)
mv /etc/rc2.d/s55sshd /etc/rc2.d/_S55sshd

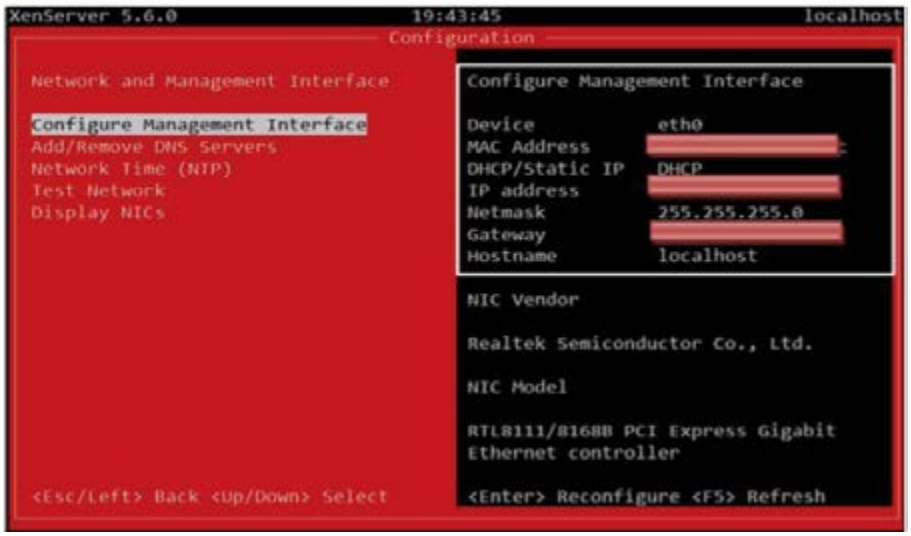
※ SSH 설정에 따라 /etc/ssh/sshd_config 파일 위치가 다를 수 있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

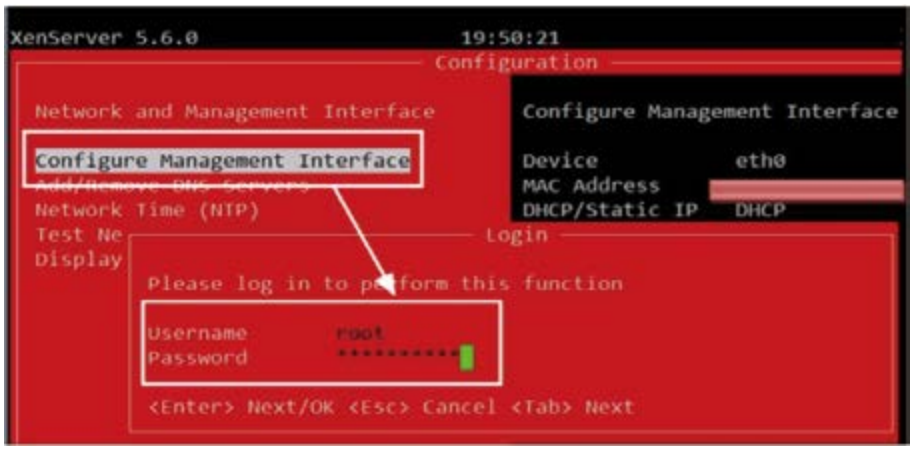
<table>
<tr><td>진단항목</td><td colspan="2">XE-24. 불필요한 서비스 제거</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">서버에 불필요한 서비스의 Port들이 열려 있는 경우 주요 시스템 정보 노출 및 서비스 거부(DOS)를 야기시킬 수 있다. Xenserver 이용한 클라우드 컴퓨팅 서비스를 위해 서버관리용으로 SSH와 VNC를 제공하고 있습니다. 클라우드 컴퓨팅 서비스에 불필요한 telnet, ftp, rlogin, rsh 등을 사용 할 경우 각각의 프로토콜에 대한 취약점으로 인해 root권한 획득, DoS공격 등 다양한 공경의 대상이 될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 서비스가 비활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 서비스가 활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
<XenServer>
■ 서비스 확인
ps –ef | grep [서비스 명]

불필요한 서비스 목록
<table>
<tr><th colspan="4">불필요한 서비스</th></tr>
<tr><td>echo(7)</td><td>chargen(19)</td><td>finger(79)</td><td>nntp(119)</td></tr>
<tr><td>netbios_dgm(138)</td><td>ldap(389)</td><td>ntalk(518)</td><td>ldaps(636)</td></tr>
<tr><td>nfsd(2049)-NFS미 사용시</td><td>discard(9)</td><td>time(37)</td><td>sftp(115)</td></tr>
<tr><td>ntp(123)</td><td>netbios_ssn(139)</td><td>printer(515)</td><td>uucp(540)</td></tr>
<tr><td>ingreslock(1524)</td><td>dtspcd(6112)</td><td>daytime(13)</td><td>tftp(69)</td></tr>
<tr><td>uucp-path(117)</td><td>netbios_ns(137)</td><td>bftp(152)</td><td>talk(517)</td></tr>
<tr><td>pcserver(600)</td><td>www-ldap-gw(1760)</td><td></td><td></td></tr>
<tr><th colspan="4">클라우드 컴퓨팅 서비스에 불필요한 서비스</th></tr>
<tr><td>FTP</td><td>NFS</td><td>RPC</td><td>SNMP</td></tr>
<tr><td>Sendmail</td><td>SWAT</td><td>Samba</td><td>NIS, NIS+</td></tr>
<tr><td>telnet</td><td>RLOGIN</td><td>RSH</td><td>기타</td></tr>
</table>
</td></tr>
<tr><td>조치방법</td><td colspan="4">
<XenServer>
■ 서비스 필요 시
1) 최신 버전 설치
■ 서비스 불필요 시
1) “/etc/xinetd.d” 디렉터리 내의 서비스 파일 수정
vi /etc/xinetd.d/ [서비스 파일명]
2) xinetd.d 디렉터리 내에서 필요 없는 서비스를 Disable을 yes로 설정
/etc/xinetd.d/chargen 파일
service chargen
</td></tr>
</table>

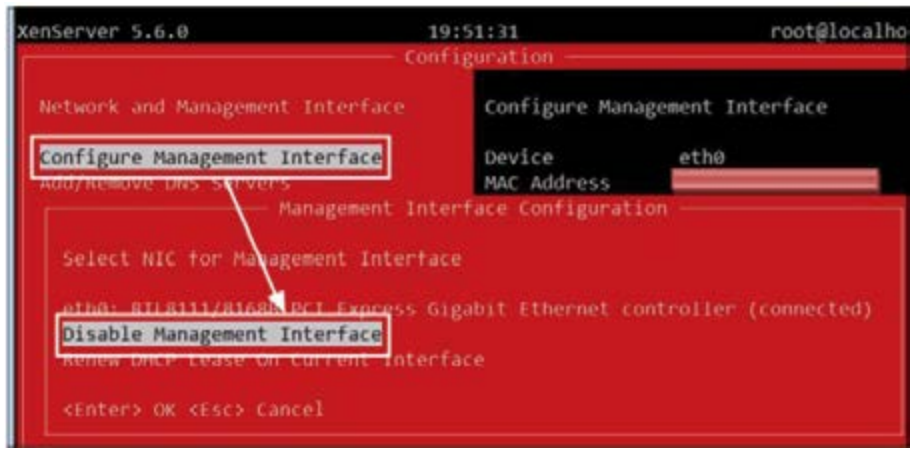
	{ Disable = yes ... 생 략 ... } 3) service 재시작 # service xinetd restart 클라우드 컴퓨팅 서비스에 불필요한 서비스 중지 # ps –ef | grep [서비스 명] # kill *9 [프로세스 ID]
비고	

라. 하이퍼바이저 정책 설정

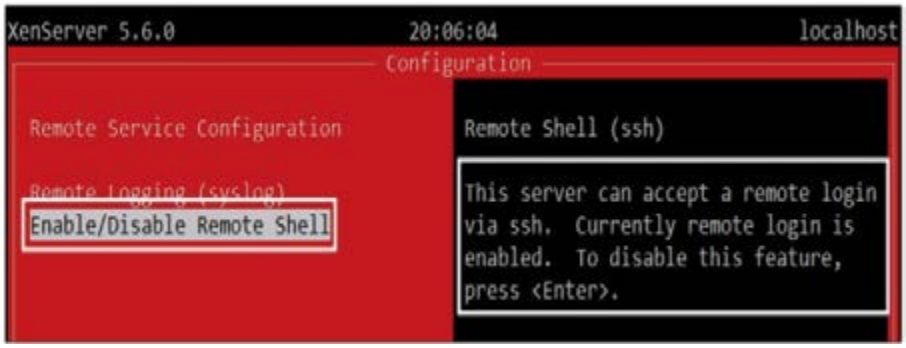
<table>
<tr><td>진단항목</td><td colspan="2">XE-25. 관리용 원격 접근 제어</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리용으로 SSH나 XenCenter를 이용하여 원격에서 XenServer에 접근이 가능하다. 관리자가 XenServer에 원격으로 접근이 불필요한 경우에는 관리자 원격 접근을 제한함으로써 비 인가적인 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">xsconsole의 [Network and Management Interface] 메뉴에서 “interface”가 설정되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">xsconsole의 [Network and Management Interface] 메뉴에서 “interface”가 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><xsconsole>
▪ 관리용 원격 접속 접근 제어 설정 확인
1) # xsconsole > Network and Management Interface > Configure Management Interface에서 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><xsconsole>
▪ 관리용 원격 접속 접근 제어 설정
1) xsconsole > Network and Management Interface > Configure Management Interface > Login</td></tr>
</table>



2) Login 후 나타나는 Management Interface Configuration 화면에서 Disable Management Interface를 선택하여 관리용도로 원격에서의 접근을 차단 설정

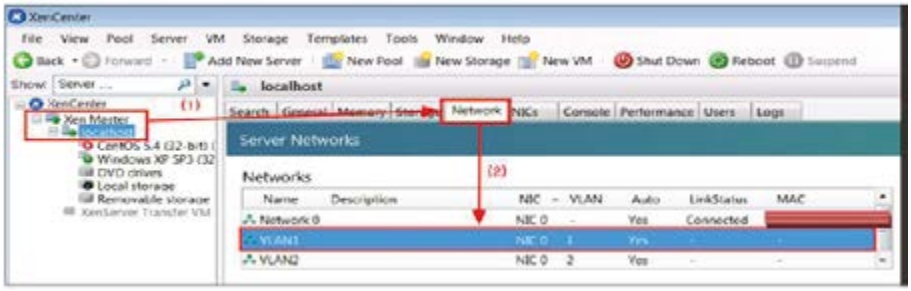
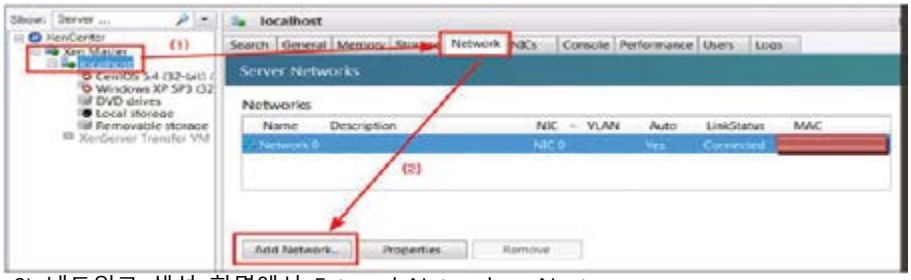


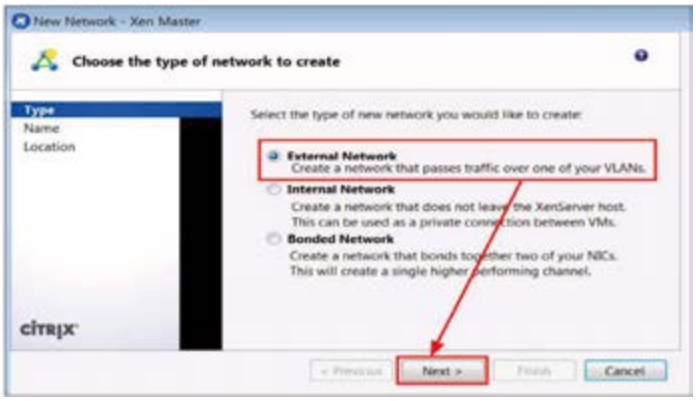
비고	

<table>
<tr><td>진단항목</td><td colspan="2">XE-26. Remote Shell 접근 제어</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">XenServer에 Remote Shell을 이용하여 원격에서의 접근이 가능하다. XenServer에 오직 XenCenter만을 이용하여 접근을 허용하고, Remote Shell을 이용하여 접근이 불필요한 경우에는 관리자 원격 접근을 제한함으로써 비 인가적인 시스템 사용을 방지하여 침해의 가능성을 줄일 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]이 Disable로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]이 Enable로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><xsconsole>
■ Remote Shell 접근 제어 설정 확인
1) # xsconsole > Remote Service Configuration > Enable/Disable Remote Shell 에서 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4"><xsconsole>
■ Remote Shell 접근 제어 설정
1) xsconsole의 [Remote Service Configuration] 메뉴에서 [Enable/Disable Remote Shell]을 선택한 후 Login</td></tr>
</table>

2) Login 후 나타나는 [Configure Remote Shell] 화면에서 "Disable"를 선택하여 원격에서의 Shell 접근 차단을 설정

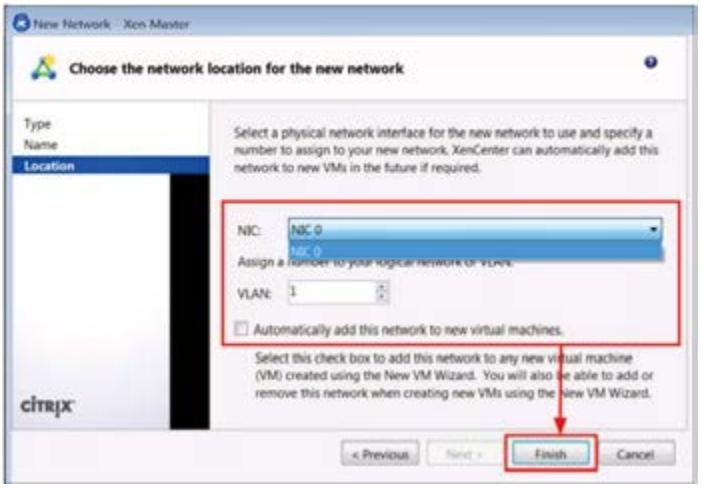
비고	

<table>
<tr><td>진단항목</td><td colspan="2">XE-27. Guest VM 네트워크 분리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Guest 네트워크는 VLAN을 이용하여 트래픽 분리가 가능하다. Guest OS(Virtual Machine) Group 간 네트워크가 연동될 경우 민감한 트래픽에 접근할 가능성이 있다. 반드시 분리되어야 하는 Guest OS(Virtual Machine) Group은 VLAN을 이용하여 트래픽을 분리하여 사용해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Guest OS (Virtual Machine) Group이 VLAN을 이용하여 트래픽이 분리되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Guest OS (Virtual Machine) Group이 VLAN을 이용하여 트래픽이 분리되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenCenter>
▪ Guest VM 네트워크 설정 확인
Xen Master > Xenserver > Network VLAN 확인 > 인터뷰를 통해 분리되어서 설정하고 있는지 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4"><xsconsole>
▪ Guest VM 네트워크 설정
1) XenCenter > XenServer > Network에서 Add Network 선택
 
2) 네트워크 생성 화면에서 External Network > Next</td></tr>
</table>



3) 생성하려는 VLAN의 이름, 설명을 입력 > Next

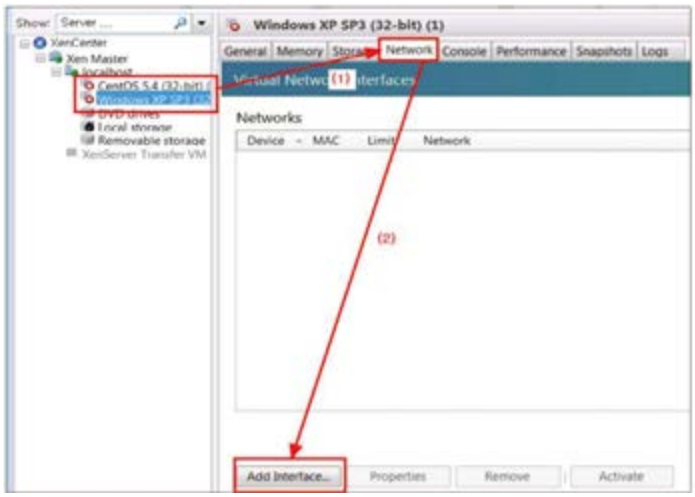
4) VLAN을 설정하는 물리적인 NIC 장치를 선택 > VLAN의 태그 선택 > Finish > VLAN 생성



※ 이미 사용 중인 태그는 설정이 불가능함

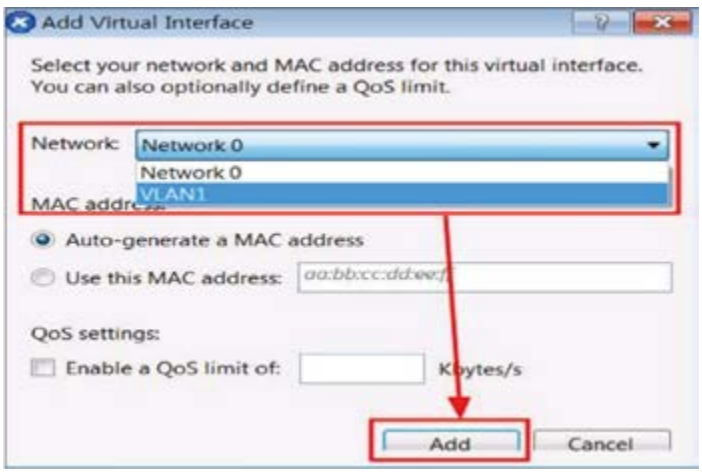
5) Server Networks에서 생성한 VLAN을 확인

6) 네트워크 분리가 필요한 Guest OS를 선택하고, [Network]를 선택 한 후 [Add Interface]를 선택함



※ Guest OS가 종료 되어야 설정이 가능함

7) Network에서 생성한 VLAN을 선택 > Add > Guest OS의 Network를 VLAN으로 설정

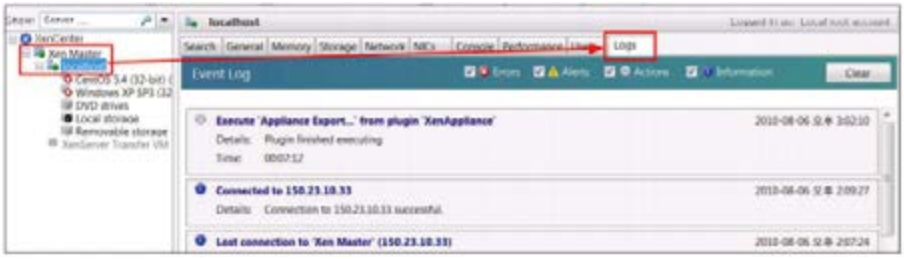
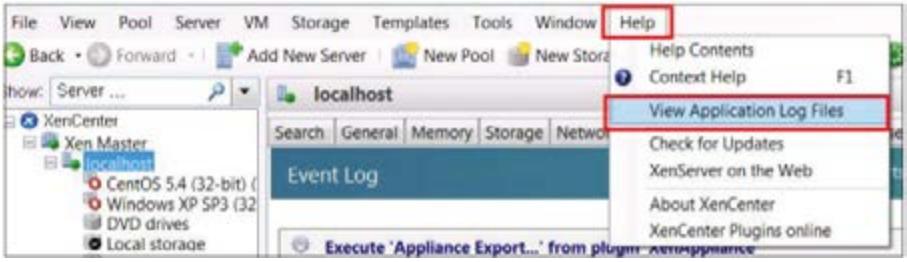


8) Virtual Network Interfaces에서 Guest OS에 설정된 네트워크를 확인 또는 현재

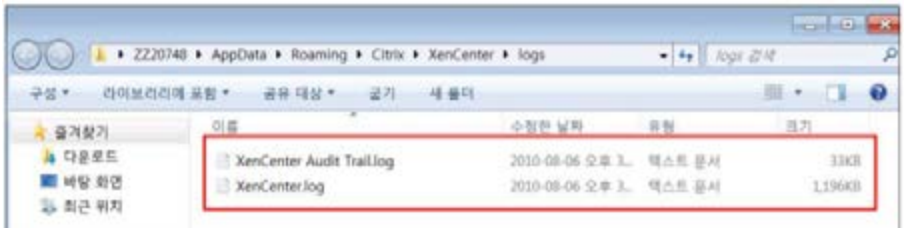
	VLAN으로 설정 확인 
비고	

마. 패치 및 로그관리

<table>
<tr><td>진단항목</td><td colspan="2">XE-28. SU 로그 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">기본적으로 일반 사용자에서 Super User로 사용되는 기록을 남기기 위해서 Su 사용로그를 남기도록 하는 보안 설정이 필요하다. 시스템의 가용성 및 무결성 등을 침해하는 사건이 발생할 경우, 일반적으로 Super User 권한으로 사건이 진행되기 때문에 Su의 로깅이 필요하다. Su 사용 로그를 기록하도록 syslog 설정 파일을 수정해야한다. Authpriv에 관련된 로그를 파일로 남기지 않고 있다면 아래와 같이 설정한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/var/log/secure 파일을 확인하여 su 기록이 남고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/var/log/secure 파일을 확인하여 su 기록이 남고 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ /etc/syslog.conf 파일에서 확인
cat /etc/syslog.conf | grep authpriv.*</td></tr>
<tr><td>조치방법</td><td colspan="4"><xsconsole>
■ /etc/syslog.conf 파일에서 설정
1) # vi /etc/syslog.conf 파일에서 아래와 같은 설정으로 변경
authpriv.* /var/log/secure
2) # /etc/rc.d/init.d/syslog restart</td></tr>
<tr><td>비고</td><td colspan="4">■ 버전 7, 8의 경우 "/etc/rsyslog.conf" 파일에서 확인 및 설정</td></tr>
</table>

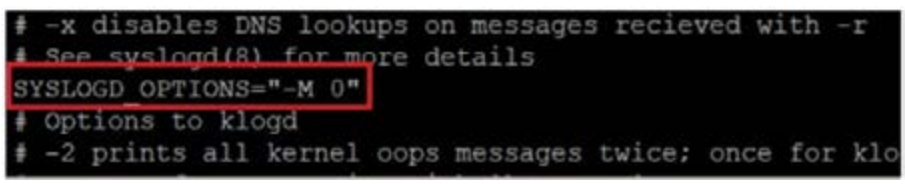
<table>
<tr><td>진단항목</td><td colspan="2">XE-29. syslog 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">기본적으로 시스템 운영 중 발생하는 Info 및 alert등에 대한 기록을 남기기 위한 “syslog.co” 파일의 보안 설정이 되었는지 점검한다. syslog 데몬은 시스템의 로그를 기록하는 전용 데몬으로 원격 또는 로컬 시스템의 커널메시지 및 시스템 로그를 감시하는 역할을 한다. 이 설정이 제대로 되어 있지 않을 경우 적절한 로그가 시스템 로그파일에서 남지 않아 침입자의 흔적이나 시스템 오류사항에 대해 분석을 할 수 없다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">syslog에 중요 로그 정보에 대한 설정이 되어 있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">syslog에 중요 로그 정보에 대한 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
<XenServer>
■ /etc/syslog.conf 파일을 점검하여, info, alert 등에 대한 로그파일 설정을 확인
1) # cat /etc/syslog.conf | grep “info|alert|notice|debug|warn|error” | egrep “var|log”
<XenCenter>
■ syslog 설정 확인
1) XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 로그를 확인

2) XenCenter의 메뉴에서 [Help]를 선택한 후 [View Application Log files] 메뉴에서 로그를 확인


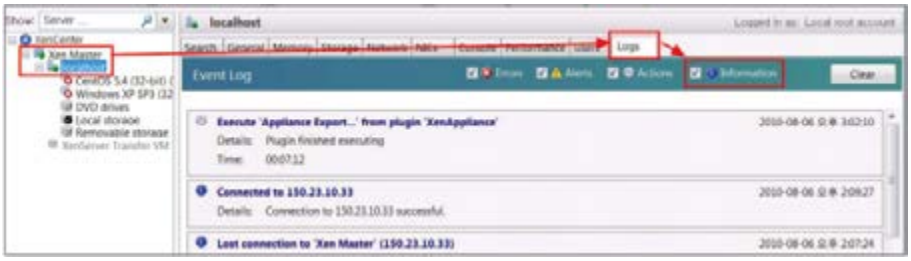
</td></tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>조치방법</td><td><XenServer>
■ XenServer 로그 파일 설정
1) /etc/syslog.conf 파일을 점검하여, info, alert 등에 대한 로그파일을 설정
vi /etc/syslog.conf
*.notice /var/log/messages
*.emerg *
*.alert /dev/console

Set info,warn,error to log to syslog by default
info;audit;syslog:local6
warn;;syslog:xapi
error;;syslog:xapi

Also print everything (debug<->error) into xensource.log for easier debugging
debug;;file:/var/log/xensource.log
info;;file:/var/log/xensource.log
warn;;file:/var/log/xensource.log
error;;file:/var/log/xensource.log
2) “syslog,conf”파일을 수정한 후에는 이것이 적용되도록 다음의 명령을 사용하여
syslogd restart
/etc/rc.d/init.d/syslog restart</td></tr>
<tr><td>비고</td><td>■ 버전 7, 8의 경우 ”/etc/rsyslog.conf” 파일에서 확인 및 설정</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-30. syslog 전송 포트 차단</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">UDP 514 Port는 Remote로 Syslog를 전송하는 Port로 사용되며, 사용 시 보안상 취약하며, 서비스 포트가 열려있으면 침해사고의 위험성이 있다. Remote Log서버를 사용하지 않을 경우 Syslog 전송 Port 차단을 권고한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Remote Log 서버를 사용하지 않을 경우 Syslog 전송 Port 차단한 경우</td></tr>
<tr><td>취약</td><td colspan="3">Remote Log 서버를 사용하지 않고 UDP 514 Port를 사용 중인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
▪ syslog 전송 포트 차단 설정 확인
1) 인터뷰를 통해 Remote Log 서버 사용 유무 확인
2) udp514 포트 확인
netstat –an | grep “udp” 또는 # netstat –an | grep “ udp” | egrep “514”
  </td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
▪ Remote Log 서버 필요시
1) Remote Log 사용 시 보안담당자 및 담당 매니저와의 협의 필요
▪ Remote Log 서버 불필요시
1) Syslog.conf 파일 수정(“/etc/sysconfig/syslog” 파일에 “SYSLOGD_OPTIONS”의 “-r” 옵션 삭제)
vi /etc/sysconfig/syslog
SYSLOGD_OPTIONS=”-m 0”
  </td></tr>
<tr><td>비고</td><td colspan="4">▪ 버전 7, 8의 경우 “/etc/sysconfig/rsyslog” 파일에서 수정</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-31. 로깅 수준 설정</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">기본적으로 시스템 운영 중 발생하는 Information 등에 대한 기록을 남기기 위한 로그 설정이 되었는지 점검한다. 시스템에 적절한 로그파일이 없을 경우, 침입자의 흔적이나 시스템 오류사항에 대해 분석할 수 없다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"/etc/syslog.conf" 파일에 "info" 설정이 되어 있거나 XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 "Information" 로그가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"/etc/syslog.conf" 파일에 "info" 설정이 되어 있지 않거나 XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 "Information" 로그가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ 로깅 수준 설정 확인
1) /etc/syslog.conf 파일에 "info" 설정 확인
cat /etc/syslog.conf | grep "info"
 
<XenCenter>
■ 로깅 수준 설정 확인
1) XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 Information 로그 설정 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ 로깅 수준 설정
1) "/etc/syslog.conf" 파일에 "info" 로그를 남기도록 설정
vi /etc/syslog.conf
info;;file:/var/log/xensource.log</td></tr>
</table>

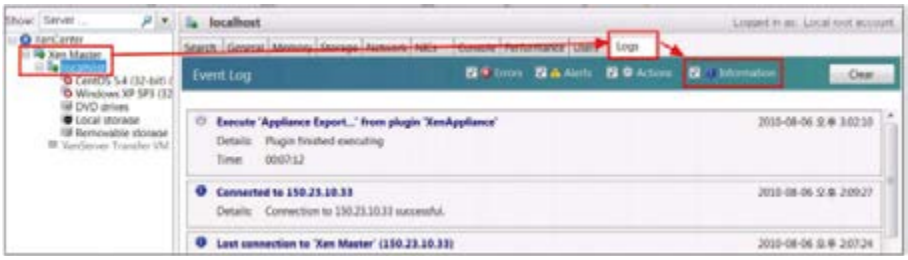
<table>
<tr><td></td><td>

```
# Also print everything (debug<->error)
debug;;file:/var/log/xensource.log
info;;file:/var/log/xensource.log
warn;;file:/var/log/xensource.log
error;;file:/var/log/xensource.log
```

<XenCenter>

■ 로깅 수준 설정

1) XenCenter에서 [XenServer]를 선택한 후 [Logs] 메뉴에서 “Information”에서 로그 설정



</td></tr>
<tr><td>비고</td><td>■ 버전 7, 8의 경우 “/etc/rsyslog.d/xenserver.conf” 파일에서 확인 및 설정</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-32. 로그 파일 권한 설정</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템의 기본 로깅 기록은 관리자 이외에 다른 일반 사용자에게 열람할 수 있는 권한을 부여할 필요가 없기 때문에 로깅 기록을 저장하는 파일의 소유자 및 읽기권한을 제한함으로써 보안을 강화하는 것이 필요하다. 아래의 로그 파일 권한은 시스템 사용자(root, adm, bin 등) 소유자의 타사용자 쓰기권한 제거를 설정한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로그파일의 소유자가 root이고, 타사용자의 쓰기권한이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로그파일의 소유자가 root가 아니거나, 타사용자의 쓰기권한이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ 로그 파일 확인
1) # ls –alL [로그파일명]

보안강화적용 대상 로그파일 목록
<table><tr><th>로그파일</th><th>XenServer</th><th>로그파일</th><th>XenServer</th></tr><tr><td>audit</td><td>/var/log/audit.log</td><td>btmp</td><td>/var/log/btmp</td></tr><tr><td>xenstored</td><td>/var/log/xenstored-access.log</td><td>secure</td><td>/var/log/secure</td></tr><tr><td>wtmp</td><td>/var/log/wtmp</td><td>messages</td><td>/var/log/messages</td></tr><tr><td>lastlog</td><td>/var/log/lastlog</td><td></td><td></td></tr></table></td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ 로깅 파일 소유자 및 권한 변경
1) 로그파일의 소유자 변경 설정
chown root [로그파일명]
2) 로그파일의 타사용자 쓰기 권한 제거 설정
chmod o-w [로그파일명]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">XE-33. 보안 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">XenServer 및 XenCenter Patch는 Xen 시스템을 Citrix에서 출시하고 난 뒤 Xen과 관련된 응용프로그램, 서비스, 실행파일 등의 오류나 보안취약점 등을 수정하여 적용한 Update 파일이다. Update Patch 발표 후 취약성을 이용한 공격도구가 먼저 출현할 수 있으므로, Update Patch는 발표 후 가능한 빨리 설치할 것을 권장한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패치 적용 정책을 수립하지 않거나 주기적으로 패치를 관리하고 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><XenServer>
■ 인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인</td></tr>
<tr><td>조치방법</td><td colspan="4"><XenServer>
■ 설정 기준 권고 (또는 정책기준)
1) 보안 취약점이 발표되면 시스템 영향도를 평가하고, 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응하는 것이 좋음
2) 패치를 수행할 시 시스템의 영향도에 따라 패치를 차등 수행하도록 함
3) 시스템 운영에 영향을 주지 않는 범위 내에서 주기적으로 패치를 수행할 것을 권고함</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

2.2. ESXi

계정 관리(4개 항목), 파일 시스템(18개 항목), 패치 관리(2개 항목) 총 3개 영역에서 24개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	ES-01	root 계정 원격 접속 제한	상
	ES-02	취약한 패스워드 사용 제한	상
	ES-03	계정 잠금 임계값 설정	상
	ES-04	사용자 계정 관리	상
나. 파일 시스템	ES-05	ESXi Shell 사용 제한	중
	ES-06	ESXi Shell 자동 종료	중
	ES-07	ESXi Shell 및 SSH 세션 타임아웃 설정	중
	ES-08	가상스위치 MAC 주소 변경정책 설정	상
	ES-09	가상스위치 Promiscuous 모드 정책 설정	상
	ES-10	가상스위치 Forged Transmits 모드 정책 설정	상
	ES-11	SSH 데몬 빈암호 사용 인증 허용 제한	상
	ES-12	SNMP 서비스 확인	중
	ES-13	SNMP Commutity String 복잡성 설정	중
	ES-14	접속 IP 및 포트 제한	상
	ES-15	FTP 비활성화	상
	ES-16	FTP root 접속 설정	상
	ES-17	FTP 기본 디렉터리 경로 확인	상
	ES-18	NTP 시간 동기화 설정	중
	ES-19	SSL 시간 초과 구성 설정 확인	상
	ES-20	이미지 프로필 및 VIB 승인 레벨 확인	상
	ES-21	MOB(Managed Object Browser) 비활성화	상
	ES-22	불필요한 서비스 제거	하
다. 패치 관리	ES-23	최신 보안패치 및 벤더 권고사항	상
	ES-24	로그의 정기적 검토 및 보고	상

[표 2] ESXi 진단 체크리스트

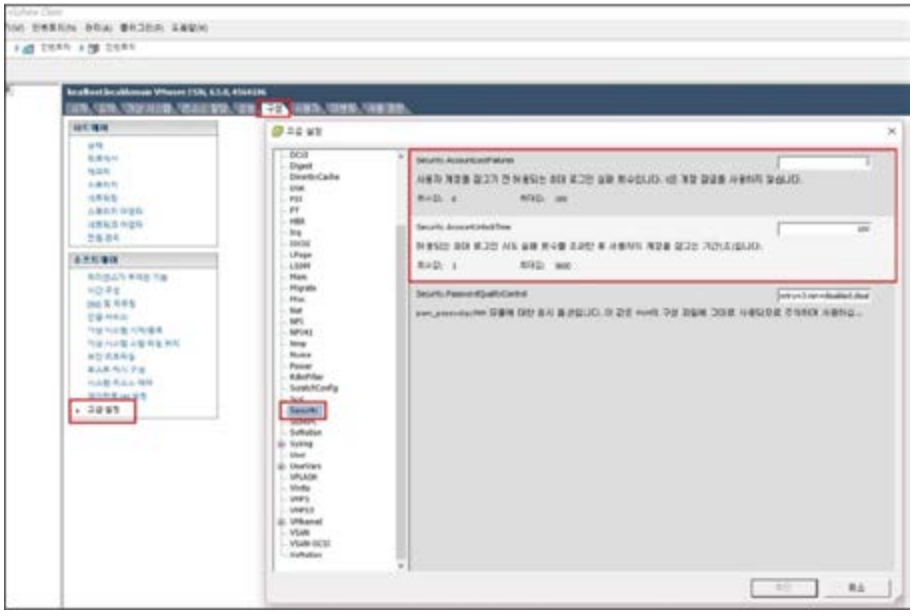
가. 계정 관리

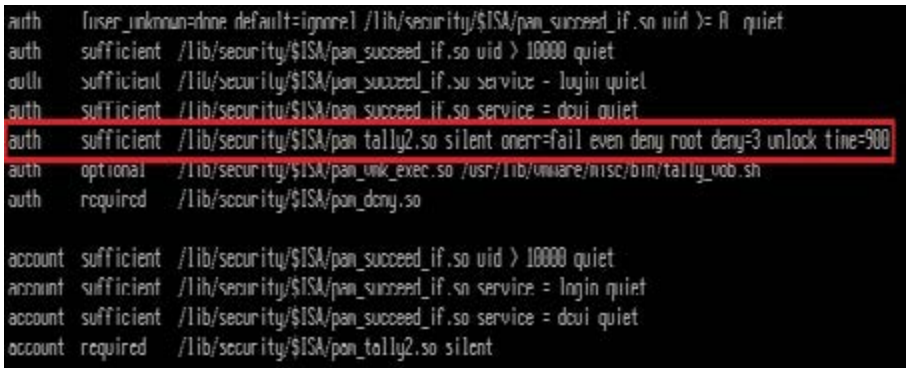
<table>
<tr><td>진단항목</td><td colspan="2">ES-01. root 계정 원격 접속 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">root 계정으로 직접 로그인 하도록 허용하면 불법적인 침입자의 목표가 될 수 있으므로 root 계정 원격 접속을 금지하여야 한다. 또한 일반 사용자 계정 접속 후 관리자 계정으로의 변경 시 로그가 남지만 관리자 계정으로 바로 접속하는 경우 어느 사용자가 접속했는지 알 수 없으므로 문제 발생 시 책임소재 파악이 용이하지 않다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">root 계정의 직접 접속이 제한되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">root 계정의 직접 접속이 제한되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ root 계정의 ssh 접속이 제한되어 있는지 확인
<CLI>
/etc/ssh/sshd_config 파일에서 “PermitRootLogin no”로 설정되어 있는지 확인
cat /etc/ssh/sshd_config | grep PermitRootLogin
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ root계정의 ssh 접속 제한 설정
<CLI>
1) vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후
vi /etc/ssh/sshd_config
2) 아래와 같이 설정 변경
PermitRootLogin no
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-02. 취약한 패스워드 사용제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자 계정(root 및 일반계정 모두)의 암호 설정 시, 일반적으로 유추하기 쉬운 암호를 설정하여, 비인가 사용자의 시스템 접근을 허용할 수 있다.
따라서 영문(대문자, 소문자), 숫자, 특수문자가 혼합된 8자리 이상의 패스워드로 설정하여 공격자가 추측하기 어려운 패스워드를 사용해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드를 영문, 숫자, 특수문자를 혼합 8자리 이상 사용하여 복잡하게 설정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드가 존재하지 않거나, 패스워드를 영문, 숫자, 특수문자를 혼합 사용하지 않거나 8자리 미만으로 설정한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 패스워드 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인
존 더 립퍼는 사전에 있는 모든 단어와 그 변화형을 패스워드로 시도하고, 단어 하나하나를 암호화하면서 이미 암호화된 패스워드와 비교하는 방식으로, 취약한 패스워드로 설정되어 있는 사용자들을 찾아서 미리 알려줄 수 있음</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 일반적으로 권장하는 패스워드 설정
1) 패스워드의 길이는 최소 8자 이상으로 설정
2) 영문(대문자, 소문자), 숫자, 특수문자를 혼합하여 패스워드 설정
3) 패스워드는 주기적으로 변경하고, 재사용 금지
4) 사전에 있는 단어나 누구나 유추 가능한 간단한 패스워드 사용 금지

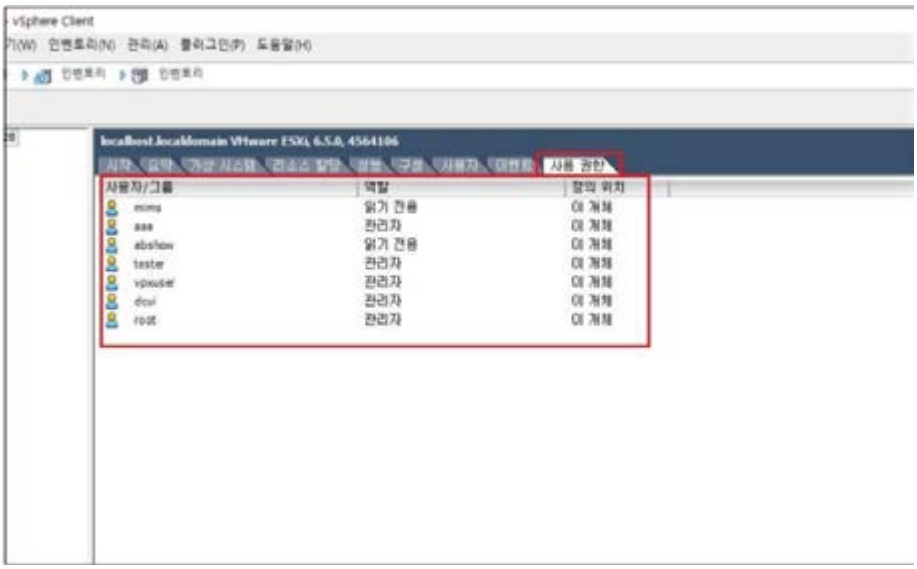
▪ ESXi 사용자 계정 패스워드 변경
1) 다른 사용자 계정 패스워드 변경(root 권한일 때)
passwd 변경할 ID
Enter new password : 변경할 Passwd
Re-type new passwd : 변경할 Passwd (위와 동일)
2) 접속 중인 자신의 계정 패스워드 변경
passwd
Enter new password : 변경할 Passwd
Re-type new passwd : 변경할 Passwd (위와 동일)

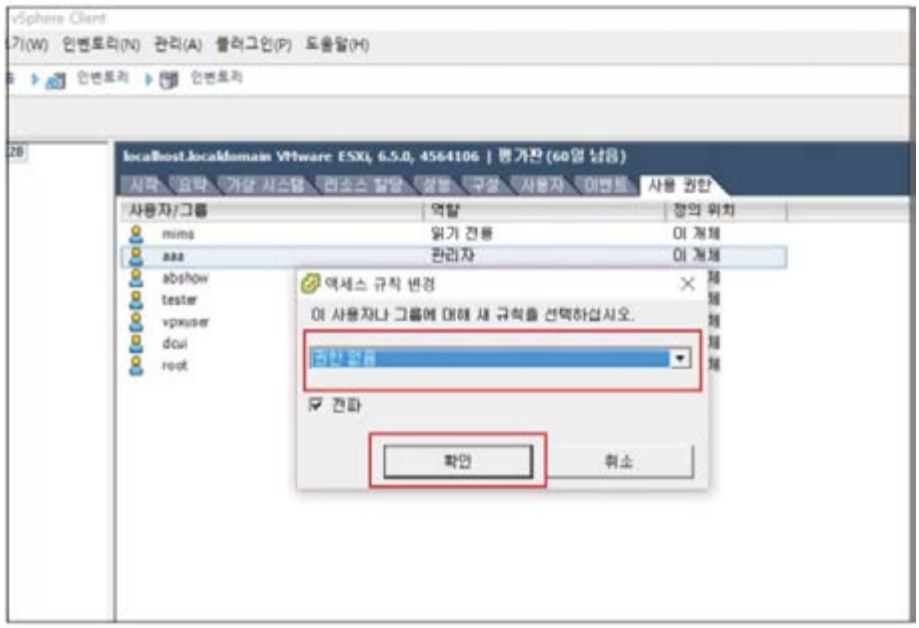
※ 다음과 같은 패스워드는 피해야 한다.
지역명, 부서명, 담당자, 성명, 대표, 업무명, “root”, “root123”, “admin”, “123admin” 등</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-03. 계정 잠금 임계값 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">침입자에 의한 패스워드 무작위 대입 공격(Bruce Force Attack)이나 패스워드 추측 공격(Password Guessing) 발생 시 암호입력 실패 횟수를 적정하게 제한함으로써 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄일 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 입력 횟수를 5 이하로 제한했을 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 입력 횟수를 5 초과로 제한했을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 패스워드 입력 횟수가 제한되어 있는지 해당 설정파일에서 설정 값 확인
<CLI>
cat /etc/pam.d/system-auth-tally
auth sufficient pam_tally2.so silent onerr=fail even_deny_root deny=3 unlock_time=100
..이하 생략..
account required pam_tally2.so silent
<vClient>
vClient 실행 > 해당 vSphereServer IP > 구성 > 고급설정 > security > security.AccountLockFailures 및 Security.Account.UnlockTime 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 해당 설정파일에 패스워드 입력 횟수를 제한하는 내용 추가 (예. 3회)
<CLI></td></tr>
</table>

	# vi /etc/pam.d/system-auth-tally  <vClient> vClient 실행 > 해당 vSphereServer IP > 구성 > 고급설정 > security > security.AccountLockFailures 및 Security.AccountUnlockTime 변경 * security.AccountLockFailures : 계정 잠금 임계값 * Security.AccountUnlockTime : 임계횟수만큼 실패 후 잠긴 기간(초)
비고	ESXi 6.0 아래 버전에서는 임계값 설정이 존재하지 않으므로 해당 사항 없음

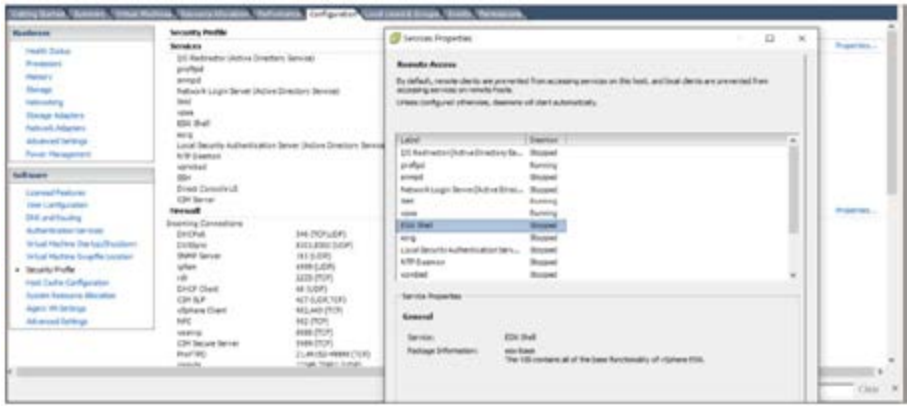
<table>
<tr><td>진단항목</td><td colspan="2">ES-04. 사용자 계정 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 모니터링 계정에 관리자 권한이 부여되어 있을 경우, 악의적인 사용자가 시스템을 조작 및 정보유출을 통해 서비스 장애 및 VM사용자의 정보가 악용될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 계정이 없거나 모니터링 계정에 최소한의 권한만 부여한 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 계정이 존재하거나 모니터링 계정과 관리자 계정을 구분하지 않고 사용한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 관리자 계정만 ssh 접속이 가능함

▪ 사용자 계정 권한 확인
<vClient>
vClient 실행 > 해당 vSphereServer IP > 사용 권한에서 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 사용자 계정 권한 설정
<vClient>
vClient 실행 > 해당 vSpereServer IP > 사용 권한 > 해당 계정 더블 클릭 > 최소한의 권한 부여</td></tr>
</table>

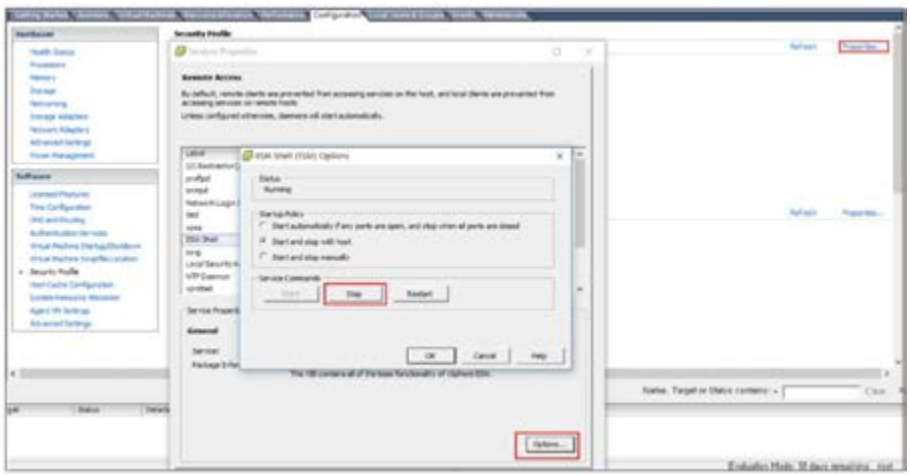
	 vSphere Client 기(W) 인벤토리(N) 관리(A) 플러그인(P) 도움말(H) 인벤토리 인벤토리 localhost.localdomain VMware ESXi, 6.5.0, 4564106 | 평가판 (60일 남음) 시작 요약 가상 시스템 리소스 할당 경보 구성 사용자 이벤트 사용 권한 사용자/그룹 역할 정의 위치 mms 읽기 전용 이 개체 aaa 관리자 이 개체 abshov tester vpxuser dcui root 액세스 규칙 변경 이 사용자나 그룹에 대해 새 규칙을 선택하십시오. 관리자 역할 전파 확인 취소
비고	

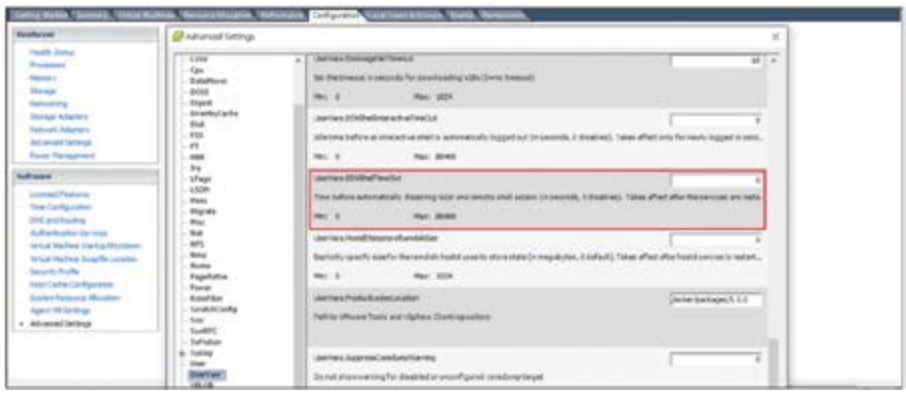
나. 보안 관리

<table>
<tr><td>진단항목</td><td colspan="2">ES-05. ESXi Shell 사용 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">ESXi Shell은 DCUI에서 local 또는 SSH를 통해 원격으로 사용 할 수 있는 대화형 명령줄 환경이다. ESXi Shell에서 수행되는 활동은 vCenter RBAC 및 감사 제어를 우회 하기 때문에 ESXi Shell은 필요한 때에만 사용을 해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">ESXi Shell이 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">ESXi Shell이 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ ESXi Shell 사용 여부 확인
<CLI>
/etc/init.d/ESXShell status 입력 후 ESXi Shell 활성화 여부 확인
 

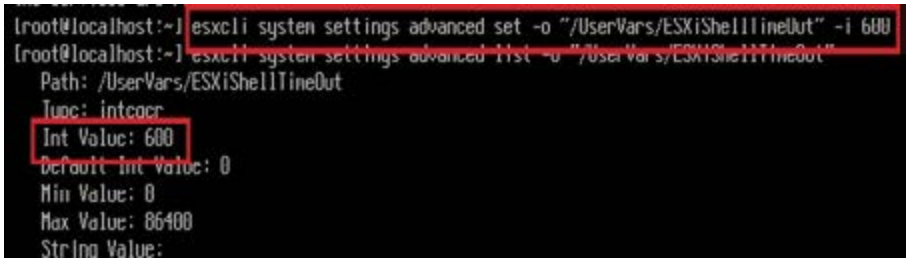
<vClient>
vClient 실행 > 설정 > 보안 프로파일 > 서비스 > 속성에서 ESXi SHELL 활성화 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ ESXi Shell 사용 제한 설정
<CLI>
/etc/init.d/ESXShell stop으로 ESXi Shell 비활성화
 

<vClient>
vClient 실행 > 설정 > 보안 프로파일 > 서비스 > 속성 > ESXi SHELL > 옵션에서 ESXi SHELL Stop 설정</td></tr>
</table>

	
비고	

<table>
<tr><td>진단항목</td><td colspan="2">ES-06. ESXi Shell 자동 종료</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">ESXi Shell은 기본적으로 사용하지 않도록 설정되어 있으나 작업 등의 이유로 Shell을 사용한 후 Shell을 닫는 것을 잊을 수 있다. 이때 ESXi Shell의 가용성 시간 초과를 설정하여 보안을 강화할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">ESXi Shell 시간 초과 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">ESXi Shell 시간 초과 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CLI>
■ ESXi Shell 시간 초과 설정 확인
esxcli system settings advanced list –o “/UserVars/ESXiShellTimeOut” 입력 후 Int Value 값 확인
 
<vClient>
■ ESXi Shell 사용 여부 확인
vClient 실행 > 설정 > 고급설정 > UserVars > UserVars.ESXiShellTimeOut에서 시간 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ ESXi Shell 시간 초과 설정
<CLI>
esxcli system settings advanced set –o “/UserVars/ESXiShellTimeOut” -i 600 (초 단위) 입력</td></tr>
</table>

<table>
<tr><td></td><td>

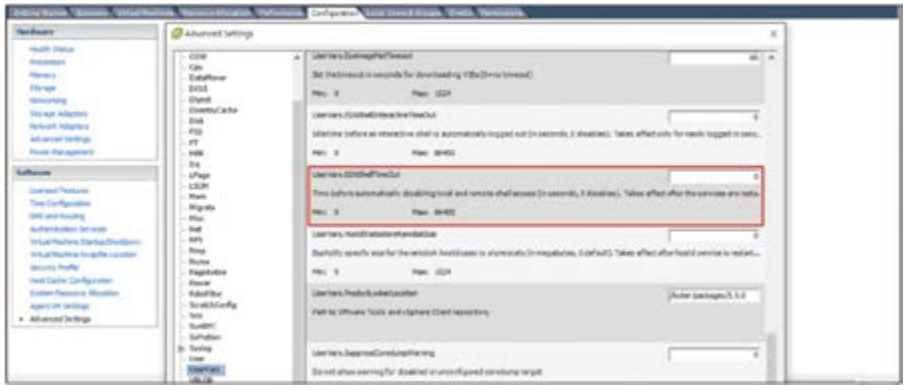


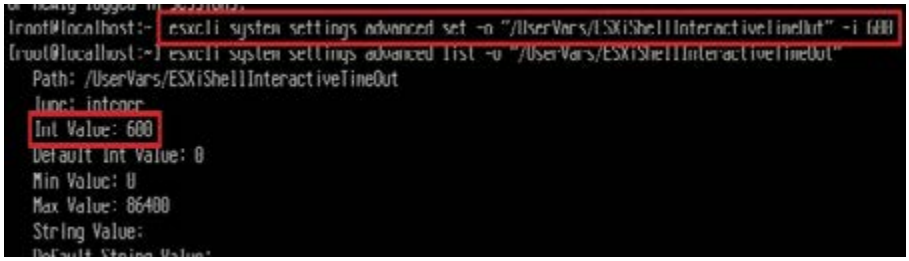
<vClient>

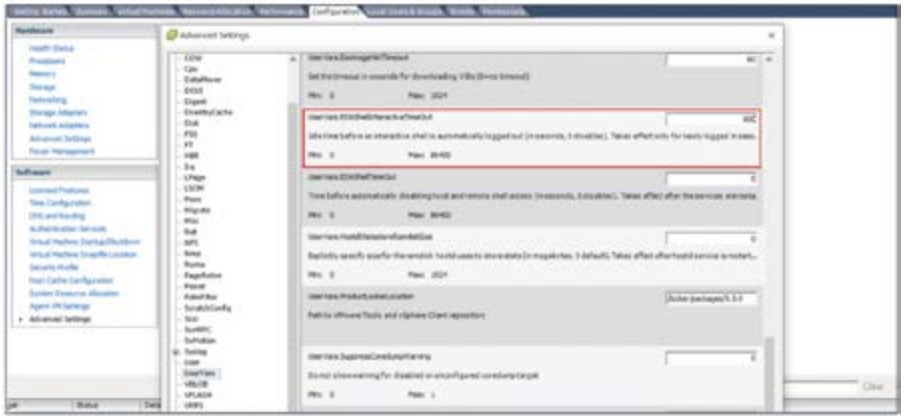
vClient 실행 > 설정 > 고급설정 > UserVars > UserVars.ESXiShellTimeOut에서 시간 설정 (초 단위)


</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

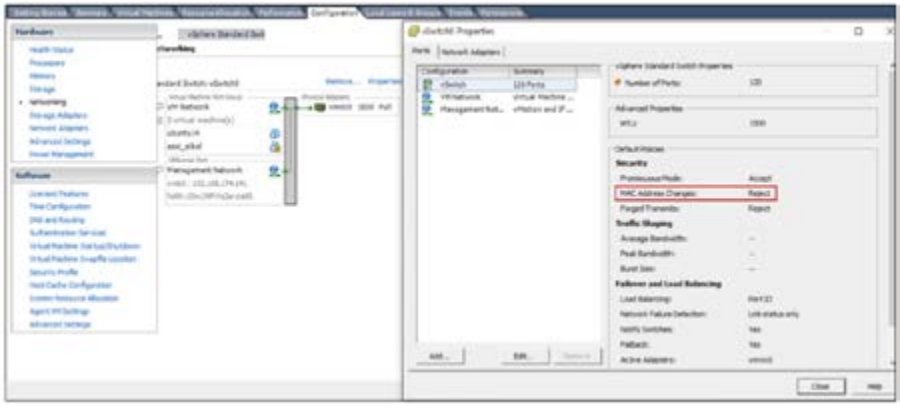
<table>
<tr><td>진단항목</td><td colspan="2">ES-07. ESXi Shell 및 SSH 세션 타임아웃 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자가 호스트에서 ESXi Shell 이나 SSH를 사용하고 로그아웃하는 것을 잊을 경우 유휴 세션이 무기한 연결 상태로 유지되며, 이 경우 열려 있는 연결에서 호스트에 대한 액세스 권한을 얻는 사용자가 늘어날 수 있다. 유휴 세션에 대한 시간 초과를 설정하여 이 문제를 방지할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">유휴 세션에 대한 시간 초과 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">유휴 세션에 대한 시간 초과 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 세션 타임아웃 설정 확인
<CLI>
esxcli system settings advanced list –o “/UserVars/ESXiShellInteractiveTimeOut” 입력 후 Int Value 값 확인
 

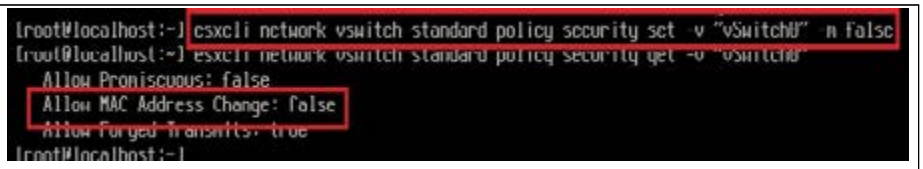
<vClient>
vClient 실행 > 설정 > 고급설정 > UserVars > UserVars.ESXiShellInteractiveTimeOut에서 시간 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 세션 타임아웃 설정
<CLI>
esxcli system settings advanced set –o “/UserVars/ESXiShellInteractiveTimeOut” -i 600 (초 단위) 입력</td></tr>
</table>

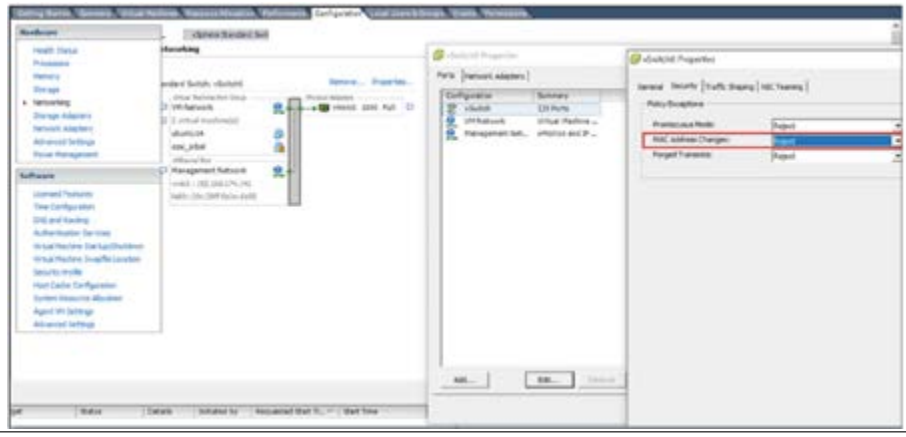
<table>
<tr><td></td><td>


■ ESXi Shell 시간 초과 설정
vClient 실행 > 설정 > 고급설정 > UserVars > UserVars.ESXiShellInteractiveTimeOut에서 시간 설정 (초 단위)

</td></tr>
<tr><td>비고</td><td>UserVars.ESXiShellTimeOut값이 0일 시 세션 무기한 연결</td></tr>
</table>

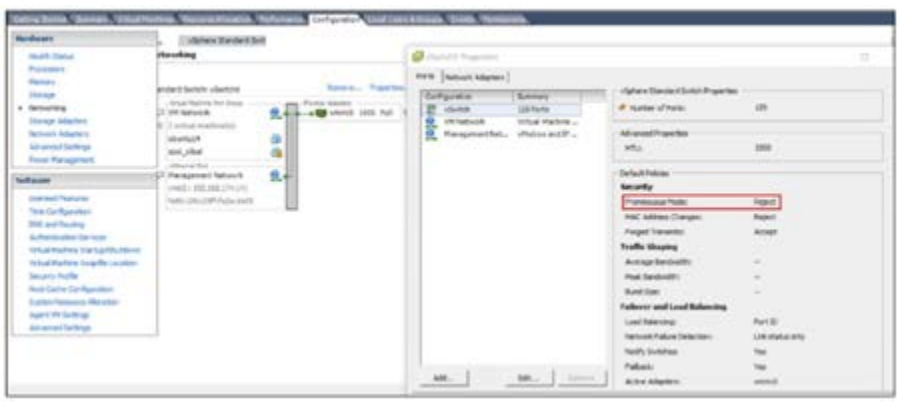
<table>
<tr><td>진단항목</td><td colspan="2">ES-08. 가상스위치 MAC 주소 변경정책 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">가상 시스템 운영체제에서 MAC 주소가 변경이 가능하면 인증 된 네트워크 어댑터를 가장하여 네트워크 장치에 악의적인 공격을 수행 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">가상스위치의 MAC 주소 변경 정책이 거부로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">가상스위치의 MAC 주소 변경 정책이 허용으로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 가상스위치 MAC 주소 변경 정책 확인
<CLI>
esxcli network vswitch standard policy security get –v “vSwitch0”(가상스위치 이름) 입력 후 MAC Address Change 값 확인
 

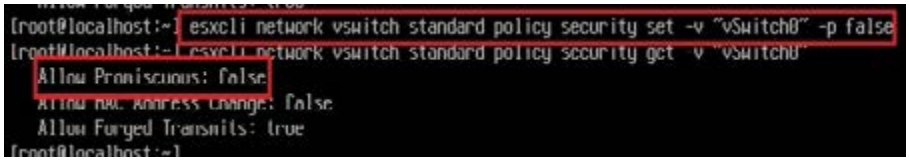
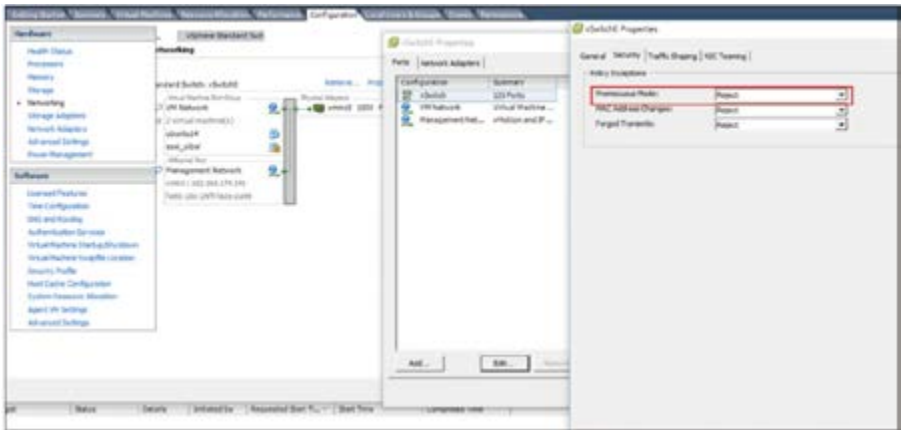
<vClient>
vClient 실행 > 설정 > 네트워크 > 속성 > vSwitch에서 MAC Address Changes 속성 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 가상스위치 MAC 주소 변경 정책 확인
<CLI>
esxcli network vswitch standard policy security set –v vSwitch0(가상스위치 이름) -m false 입력</td></tr>
</table>

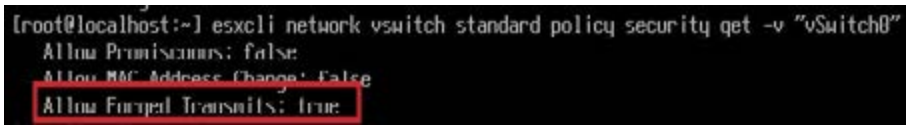
<table>
<tr><td></td><td>


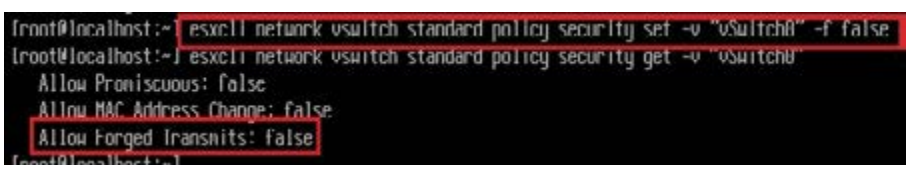
<vClient>
vClient 실행 > 설정 > 네트워크 > 속성 > vSwitch > edit > Security 탭에서 MAC Address Changes 속성을 reject로 변경

</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-09. 가상스위치 Promiscuous 모드 정책 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">가상스위치에서 Promiscuous 모드가 허용으로 설정이 되면 해당 네트워크를 통해 모든 패킷을 읽을 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">가상스위치의 Promiscuous 모드 정책이 거부로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">가상스위치의 Promiscuous 모드 정책이 허용으로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 가상스위치 Promiscuous 모드 정책 확인
<CLI>
esxcli network vswitch standard policy security get –v “vSwitch0(가상스위치 이름)” 입력 후 Promiscuous Mode 속성 확인
 

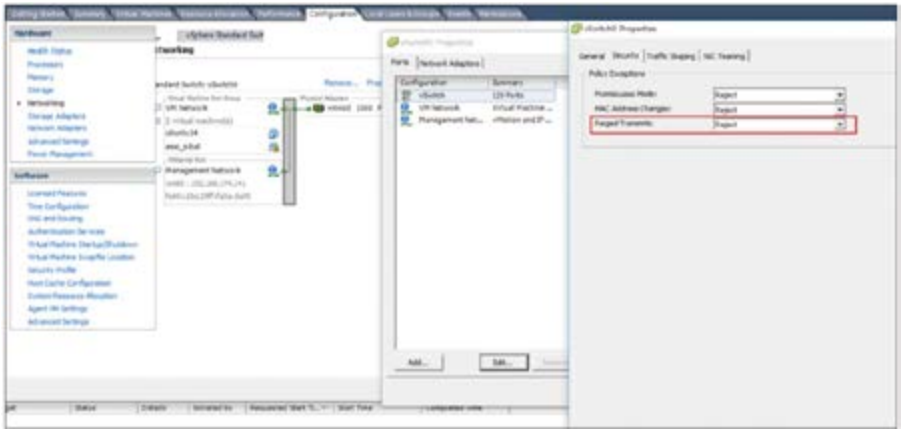
<vClient>
vClient 실행 > 설정 > 네트워크 > 속성 > vSwitch에서 Promiscuous Mode 속성 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 가상스위치 Promiscuous 모드 정책 변경
<CLI>
esxcli network vswitch standard policy security set –v “vSwitch0(가상스위치 이름)” -p false 입력</td></tr>
</table>

	 <vClient> vClient 실행 > 설정 > 네트워크 > 속성 > vSwitch에서 Promiscuous Mode 속성을 reject로 변경 
비고	

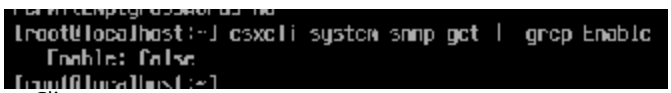
<table>
<tr><td>진단항목</td><td colspan="2">ES-10. 가상스위치 Forged Transmits 모드 정책 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">가상 시스템 운영체제에서 MAC 주소가 변경이 가능하면 인증된 네트워크 어댑터를 가장하여 네트워크 장치에 악의적인 공격을 수행 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">가상스위치 Forged Transmits 정책이 거부로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">가상스위치 Forged Transmits 정책이 허용으로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 가상스위치 Forged Transmits 모드 정책 확인
<CLI>
esxcli network vswitch standard policy security get –v “vSwitch0”(가상스위치 이름) 입력 후 Forged Transmits 값 확인
 

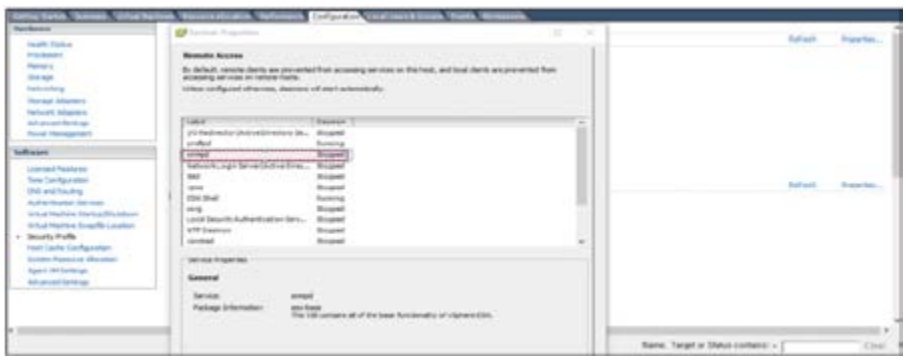
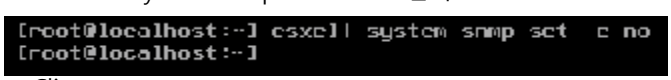
<vClient>
vClient 실행 > 설정 > 네트워크 > 속성 > Forged Transmits 속성 확인</td></tr>
<tr><td>조치방법</td><td colspan="4"><CLI>
■ 가상스위치 Promiscuous 모드 정책 변경
esxcli network vswitch standard policy security set –v “vSwitch0”(가상스위치 이름) -f false 입력
 

<vClient>
1. 가상스위치 MAC 주소 변경 정책 확인
vClient 실행 > 설정 > 네트워크 > 속성 > vSwitch > edit > Security 탭에서 Forged Transmits 속성을 reject로 변경</td></tr>
</table>

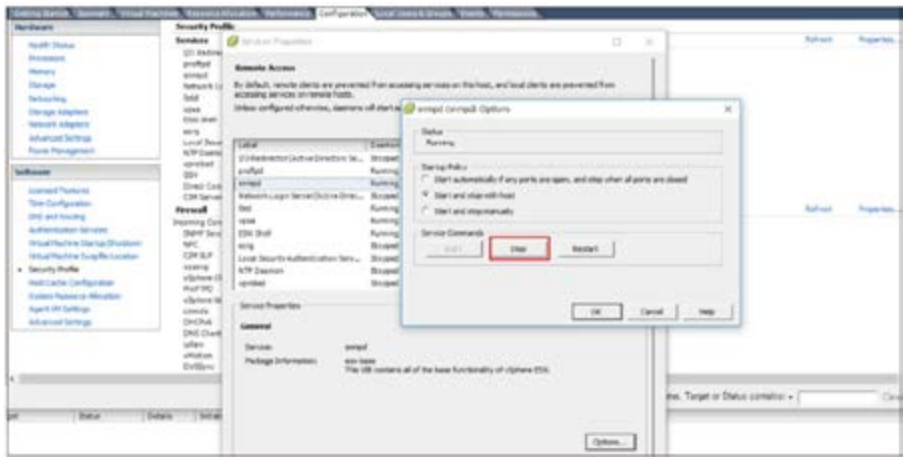
	
비고	

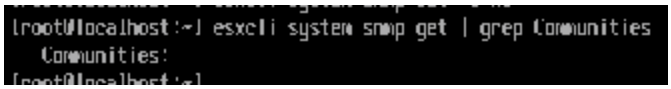
<table>
<tr><td>진단항목</td><td colspan="2">ES-11. SSH 데몬 빈암호 사용 인증 허용 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자 편의를 위해 SSH 설정에서 빈암호 사용 인증을 허용한 경우 공격자가 패스워드 인증 없이 시스템에 침투가 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/ssh/sshd_config 설정에 PermitEmptyPasswords 설정이 없거나 no 인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/ssh/sshd_config 설정에 PermitEmptyPasswords 설정이 yes인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ ssh 빈암호 인증 허용 사용 여부 확인
<CLI>
cat /etc/ssh/sshd_config | grep PermitEmptyPasswords 입력 후 PermitEmptyPasswords 값 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ ssh 빈암호 인증 허용 사용 제한 설정
<CLI>
1) vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후
vi /etc/ssh/sshd_config
2) 아래와 같이 설정 변경
PermitEmptyPasswords no</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

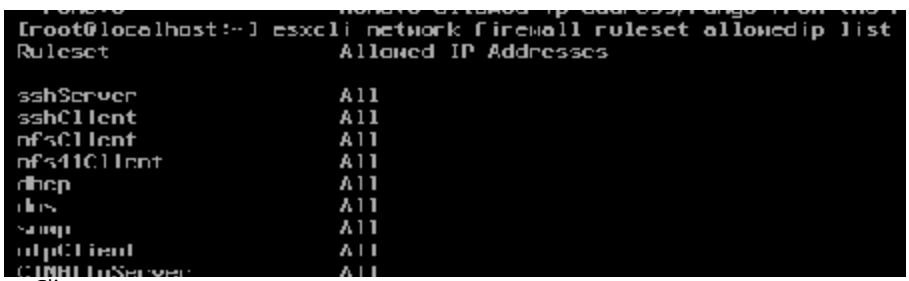
<table>
<tr><td>진단항목</td><td colspan="2">ES-12. SNMP 서비스 확인</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP를 사용할 경우 모니터링 정보를 악의적인 호스트로 보내고 해당 정보를 이용하여 공격을 계획 할 수 있으므로 불필요한 경우는 비활성화 시키는 것이 좋다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SNMP가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ SNMP 활성화 여부 확인
<CLI>
esxcli system snmp get | grep Enable 입력 후 Enable 값 확인
 

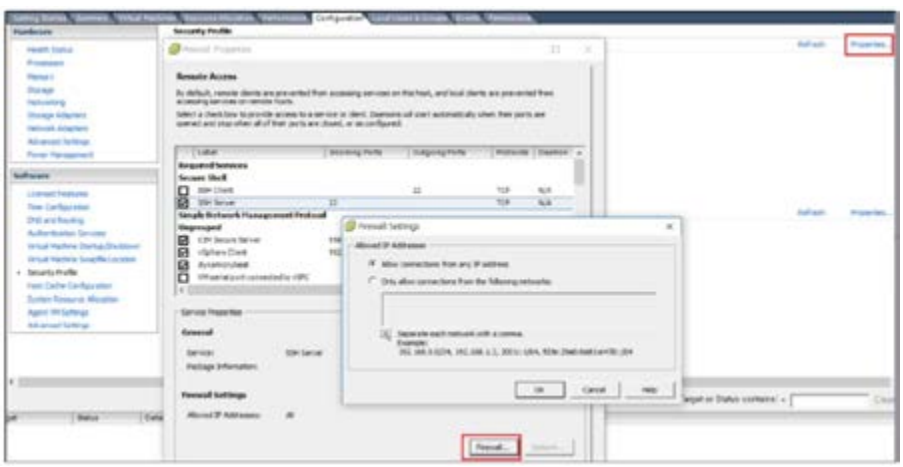
<vClient>
vClient 실행 > 설정 > 보안 프로파일 > 서비스 > 속성 > SNMP 활성화 여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ SNMP 비활성화 설정
<CLI>
esxcli system snmp set –e no 입력
 

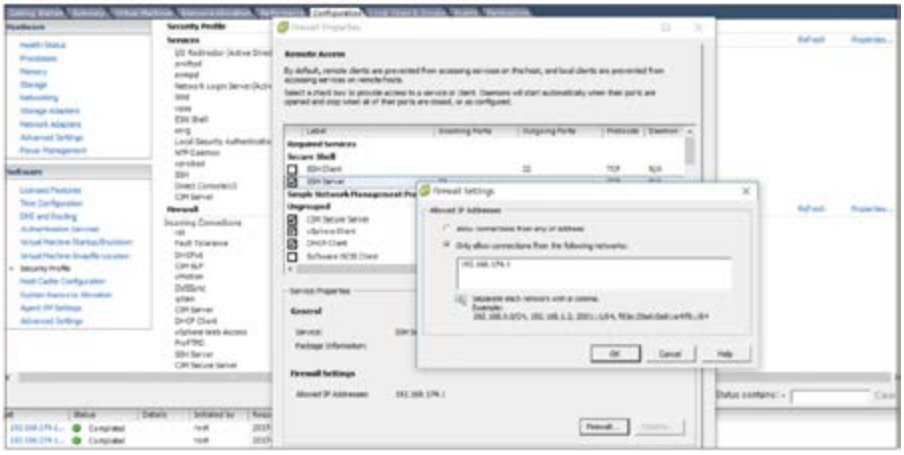
<vClient>
vClient 실행 > 설정 > 보안 프로파일 > 서비스 > 속성 > snmpd > 옵션에서 stop 클릭</td></tr>
</table>

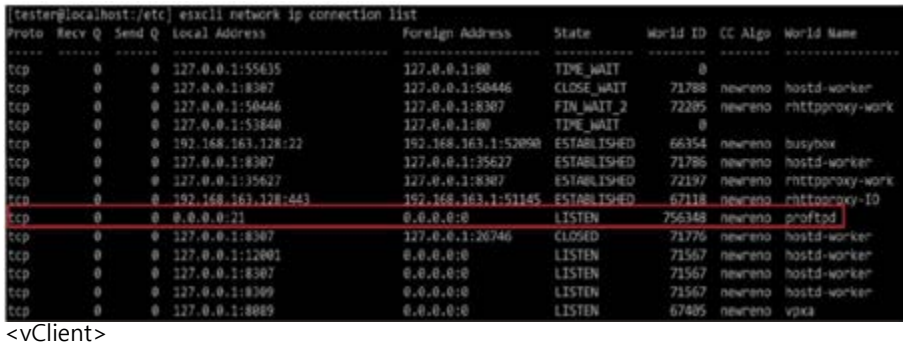
	
비고	

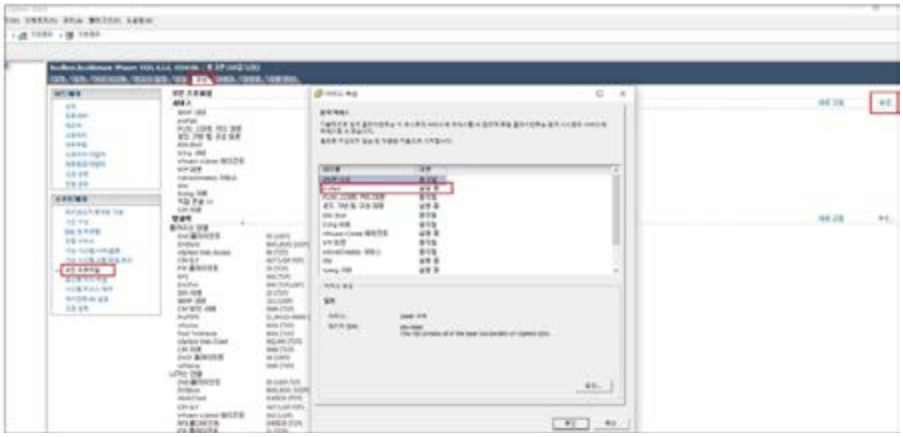
<table>
<tr><td>진단항목</td><td colspan="2">ES-13. SNMP Community String 복잡성 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP에서 community string은 SNMP(데몬)와 클라이언트가 데이터를 교환하기 전에 인증하는 일종의 패스워드로서 초깃값으로 설정되어 있는 Public, Private와 같은 SNMP default community string을 이용할 시에 해당 장비의 routing table, MAC address 등의 중요한 정보를 외부로 노출시킬 가능성이 많다. 이를 그대로 사용하는 것은 패스워드를 사용하지 않는 계정을 사용하는 것 이상 위험함에도 불구하고 대부분의 시스템, 네트워크 관리자들이 기본적인 문자열인 public을 그대로 사용하거나 다른 문자열로 변경을 해도 상호나 monitor, router mrtg 등 사회 공학적으로 추측할 수 있는 문자열을 사용하고 있어 문제가 되고 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP Community String에 추측 가능한 문자열을 사용하고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">SNMP Community String에 추측 가능한 문자열을 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Community String 값 확인
<CLI>
esxcli system snmp get | grep Communities 입력 후 Communities 값 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Community String 값 변경
esxcli system snmp set –c “수정할 Community String 값” 입력
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

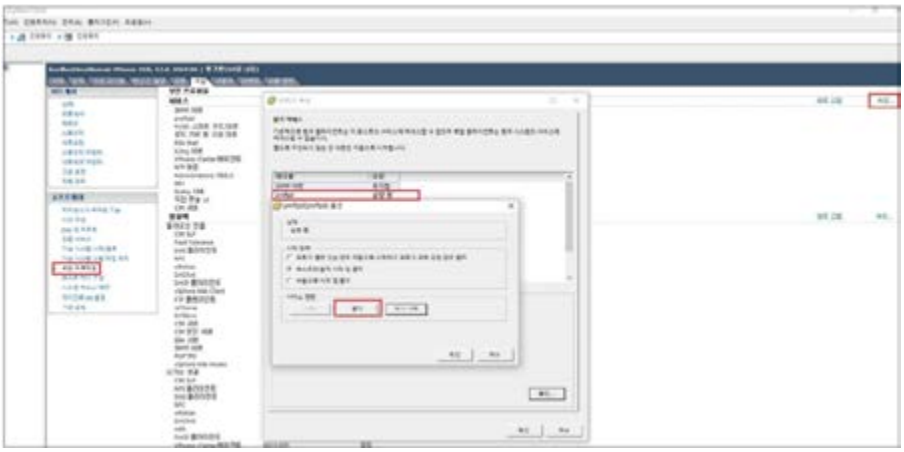
<table>
<tr><td>진단항목</td><td colspan="2">ES-14. 접속 IP 및 포트 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">ESXi 시스템이 제공하는 SSH, FTP 등 많은 네트워크 서비스를 통한 외부 비인가자의 불법적인 접근 및 시스템 침해사고를 방지하기 위하여 Firewall를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">원격 접속 가능한 서비스에 IP 제한 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">원격 접속 가능한 서비스에 IP 제한 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ firewall 설정 확인
<CLI>
esxcli network firewall ruleset allowedip list 입력 후 IP 제한 설정 확인
 

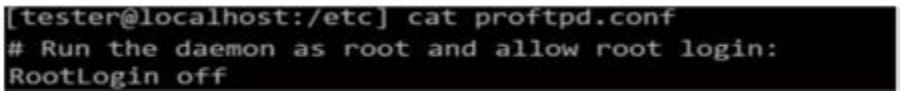
<vClient>
vClient 실행 > 설정 > 보안 프로파일 > Firewall > 속성에서 각 서비스별 IP 제한 설정 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 서비스별 허용할 IP 설정
<CLI>
1) 해당 서비스에서 모든 IP를 차단 한 후</td></tr>
</table>

	# esxcli network firewall ruleset set --ruleset-id sshServer --ip-address IP 주소 또는 대역 입력 [root@localhost:~] esxcli network firewall ruleset set --ruleset-id sshServer --allowed-all false [root@localhost:~] 2) 허용할 IP 설정 # esxcli network firewall ruleset allowdip add --ruleset-id sshServer --ip-address IP 주소 또는 대역 입력 [root@localhost:~] esxcli network firewall ruleset allowedip add --ruleset-id sshServer --ip-address 192.168.70.131 [root@localhost:~] <vClient> vClient 실행 > 설정 > 보안 프로파일 > Firewall > 속성에서 각 서비스별 IP 제한 설정 
비고	ESXi Shell에서 IP 제한 설정 시 설정할 서비스에서 모든 IP에 대해 deny 설정 후 허용할 IP 설정

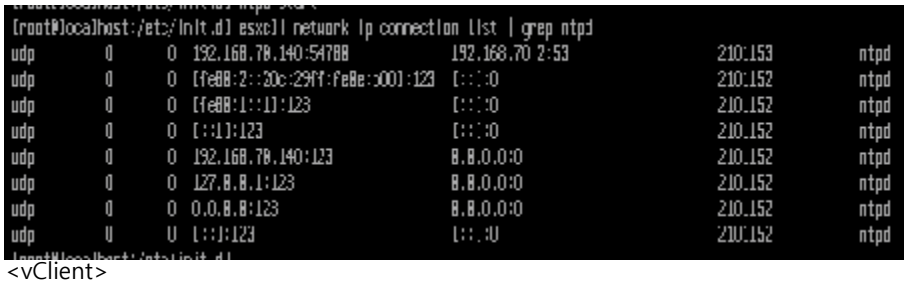
<table>
<tr><td>진단항목</td><td colspan="2">ES-15. FTP 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">불필요한 FTP가 활성화되어 있을 경우, 해당 서비스 포트가 외부에서 활성화되어 해커의 침입경로로 이용될 위험이 있다. 또한 해당 설정들을 관리하고 있지 않을 가능성이 높아 해당 서비스와 관련된 잘 알려진 취약점을 통해 서버를 공격할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">FTP가 설치되어 있지 않거나 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 FTP가 구동되고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ FTP 구동여부 확인
<CLI>
esxcli network ip connection list에서 21port의 proftpd 확인
 

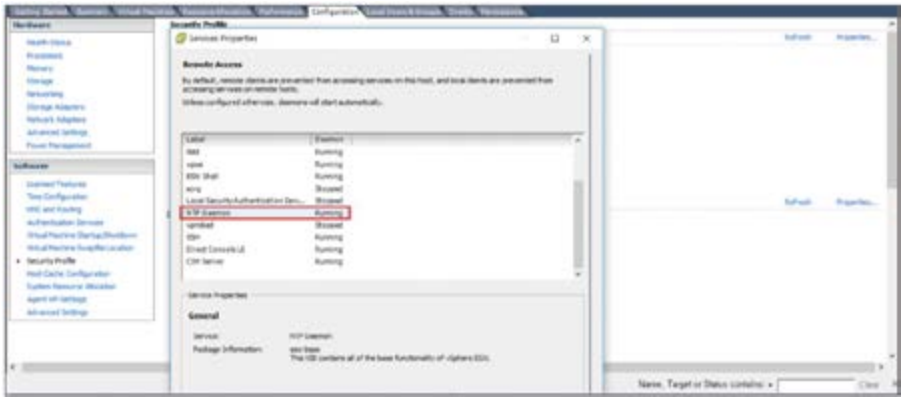
<vClient>
vClient 실행 > 해당 vSphereServer IP > 구성 > 보안 프로파일 > 보안프로파일(속성) > 서비스 속성(원격 액세스) 설정 확인
  </td></tr>
</table>

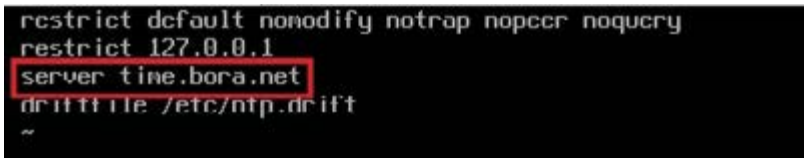
조치방법	<CLI> ▪ FTP 구동 중지 # /etc/init.d/proftpd stop [tester@localhost:/etc] /etc/init.d/proftpd stop Stopping proftpd <vClient> ▪ 서비스별 허용할 IP 설정 vClient 실행 > 해당 vSphereServer IP > 구성 > 보안 프로파일 > 보안프로파일(속성) > 서비스 속성(원격 액세스) > proftpd 선택 > 옵션 > 중지 
비고	

<table>
<tr><td>진단항목</td><td colspan="2">ES-16. FTP root 접속 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">FTP로 root로 접속이 가능할 경우, FTP의 root의 패스워드 무차별 대입공격으로 root 권한 획득 후, 시스템의 설정을 다운로드 받을 수 있는 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">root로 원격접속이 불가능할 경우</td></tr>
<tr><td>취약</td><td colspan="3">root로 원격접속이 가능할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ FTP root 접속 설정 확인
<CLI>
cat /etc/proftpd.com에서 RootLogin확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ FTP root 접속 제한 설정
1) vi 편집기를 이용하여 /etc/proftpd.conf 파일을 연 후
vi /etc/proftpd.conf
2) 아래와 같이 설정 변경
RootLogin off</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-17. FTP 기본 디렉터리 경로 확인</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">defaultRoot가 Root 최상위 디렉터리로 설정되어 있으므로 변경하여 사용하지 않을 경우, 악의적인 FTP 사용자가 시스템 설정에 접근하여 다운로드 후 2차 공격의 정보로 활용할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">defaultRoot 설정이 변경되어 있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">defaultRoot 설정이 최상위 Root 설정이거나 시스템 설정 디렉터리로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ FTP root 접속 설정 확인
<CLI>
cat /etc/proftpd.conf에서 DefaultRoot확인</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ FTP root 접속 제한 설정
1) vi 편집기를 이용하여 /etc/proftpd.conf 파일을 연 후
vi /etc/proftpd.conf
2) 아래와 같이 설정 변경
DefaultRoot /[지정할 디렉터리 경로]
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-18. NTP 시간 동기화 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">시간 설정이 되어 있지 않은 경우 로그 파일을 검사할 시 공격 시간대와 서버 시간대가 맞지 않아 감사가 부정확해 질 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">NTP 시간 동기화 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">NTP 시간 동기화 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ NTP 활성화 여부 확인
<CLI>
esxcli network ip connection list | grep ntpd 입력 후 ntp 목록 확인
 

<vClient>
vClient 실행 > 구성 > 보안 프로파일 > 서비스 > 속성 > ntpd 활성화 여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ NTP 활성화
<CLI>
1) vi 편집기를 이용하여 /etc/ntp.conf 파일에서 server time.bora.net(ntp 서버) 설정
vi /etc/ntp.conf</td></tr>
</table>

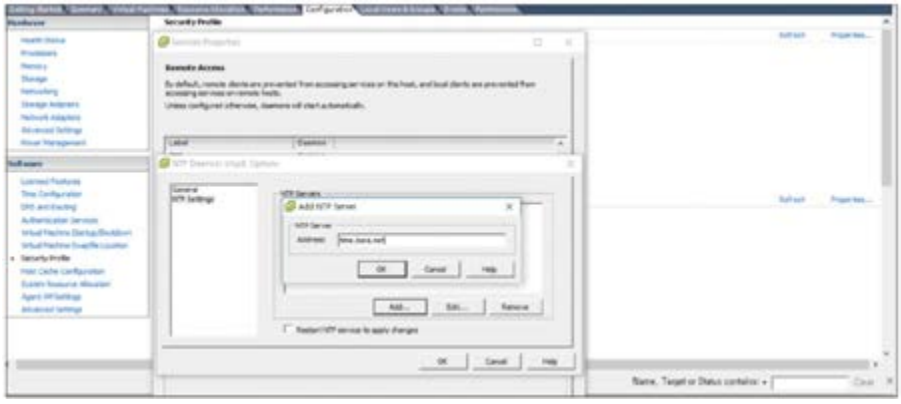


2) NTP 데몬 시작

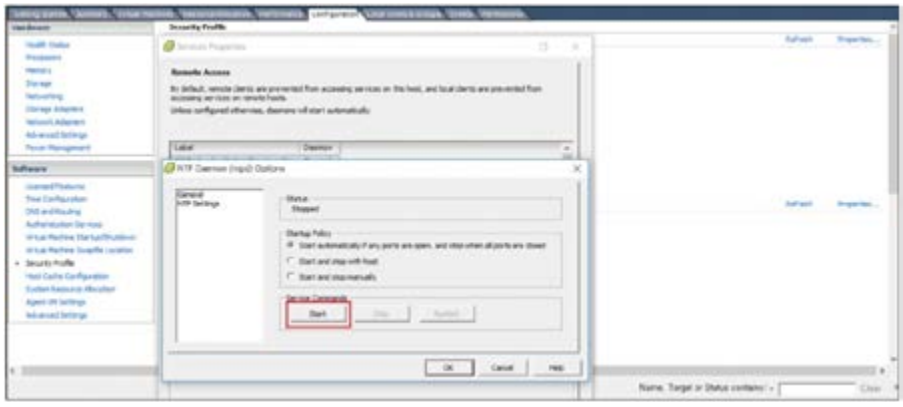
/etc/init.d/ntpd start

<vClient>

1) vClient 실행 > 구성 > 보안 프로파일 > 서비스 > 속성 > ntpd Daemon > 옵션 > NTP Setting > Add 클릭 후 /etc/ntp.conf에서 설정한 NTP 서버 입력

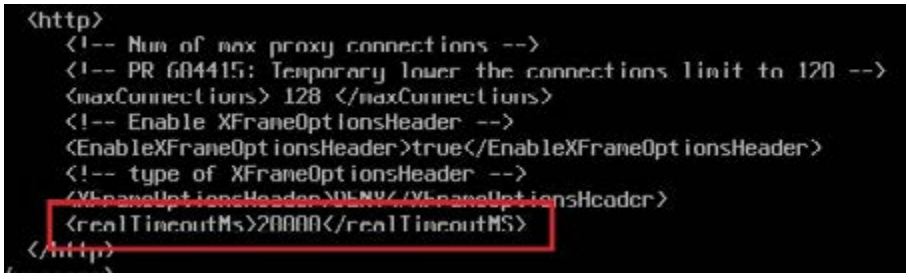
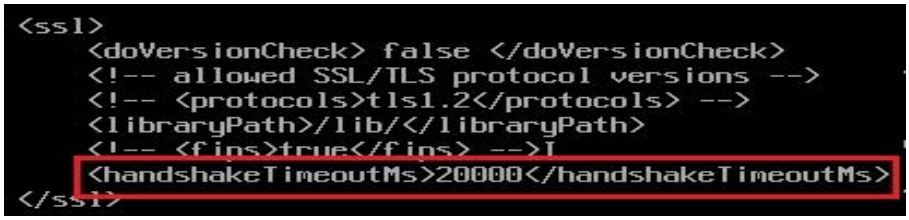


2) NTP 서버 입력 후 General 탭에서 NTP Deamon 활성화



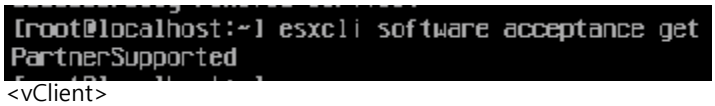
비고	

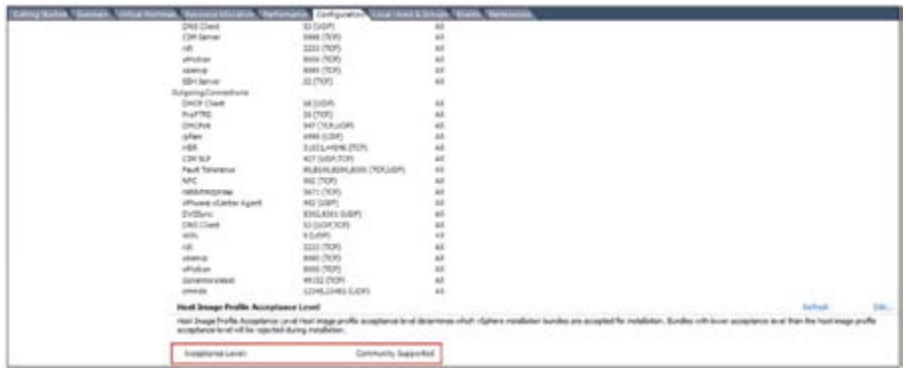
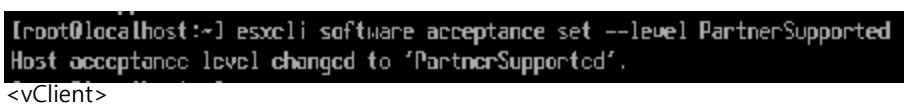
<table>
<tr><td>진단항목</td><td colspan="2">ES-19. SSL 시간 초과 구성 설정 확인</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">기본적으로 완전하게 SSL 연결은 시간제한이 없으므로, 악의적인 사용자가 많은 SSL 연결을 통해 서비스 거부 공격을 시행할 위험이 존재하므로 유휴 연결에 대하여 시간 초과 기간을 설정하여야 한다.

* 읽기 시간 초과 설정(readTimeoutMs) : ESXi의 포트 443에서 SSL 핸드셰이크 프로세스를 완료한 연결에 적용
핸드셰이크 시간 초과 설정(handshakeTimeoutMs) : ESXi의 포트 443에서 SSL</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SSL 유휴 연결에 대해 시간 초과 기간을 설정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">SSL 유휴 연결에 대해 시간 초과 기간을 설정하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ SSL 시간 초과 설정 확인
<CLI>
cat /etc/vmware/hostd/config.xml에서 readTimeoutMS, handshakeTimeoutMS 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">■ SSL 시간 초과 설정 확인
1) vi 편집기를 이용하여 /etc/vmware/hostd/config.xml 파일에서 readTimeoutMS, handShakeTimeoutMS설정
<vmacore>
...
 
...
  </td></tr>
</table>

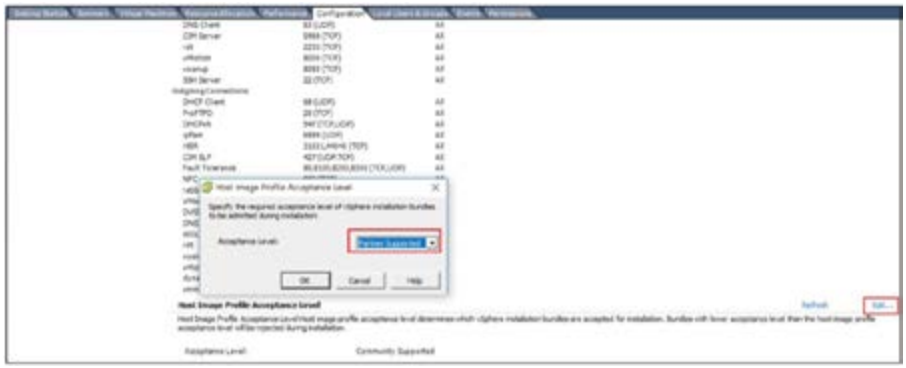
	... </vmacore> 2) hostd 재시작 # /etc/init.d/hostd restart
비고	

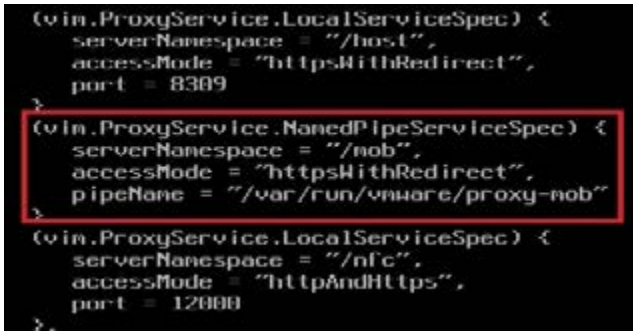
<table>
<tr><td>진단항목</td><td colspan="2">ES-20. 이미지 프로필 및 VIB 승인 레벨 확인</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">*VIB 승인 레벨은 4단계가 있으며 그중 Community Supported 승인 수준은 VM Ware 파트사와 관계없는 개인이나 회사에서 생성한 VIB를 설치 가능하게 해준다. Community Supported 수준에서는 디지털 서명이 존재하지 않으므로 기술지원 등을 받을 수 없다.

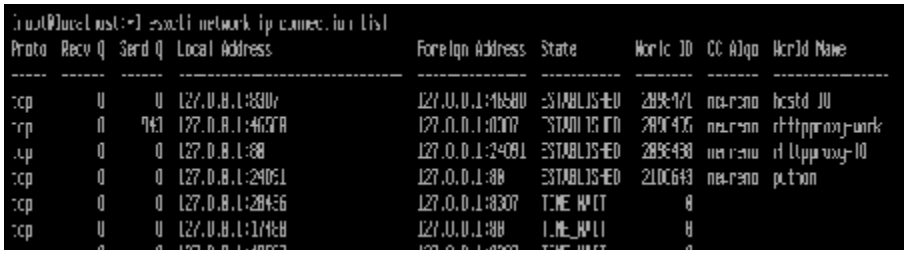
* VIB란 Vsphere Install Bundle로 VMware Update Manager이나 로컬 CLI를 통해 직접 설치하는 ESXi 소프트웨어 패키지</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">VIB 승인 레벨이 Partner Supported 이상인 경우</td></tr>
<tr><td>취약</td><td colspan="3">VIB 승인 레벨이 Community Supported 인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 승인 레벨 확인
<CLI>
esxcli software acceptance get 입력 후 승인 레벨 확인
 

<vClient>
vClient 실행 > 구성 > 보안 프로파일 > 호스트 이미지 프로파일 수락 수준에서 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 승인 레벨 변경
<CLI>
esxcli software acceptance set --level PartnerSupported 입력
 

<vClient></td></tr>
</table>

	vClient 실행 > 구성 > 보안 프로파일 > 호스트 이미지 프로파일 수락 수준 > Edit에서 변경 
비고	※ ESXi VIB 수락 수준 - VMwareCerfified: VMware 사에서 테스트 및 인증한 VIB만 설치 가능 - VMwareAccepted: 파트너사가 테스트하고 VMware사에서 결과를 확인한 VIB 설치 가능 - PartnerSupported: 신뢰하는 파트너사가 테스트 및 결과 확인을 한 VIB 설치 가능 - CommunitySupported: VMware사와 관계없는 개인 및 회사가 생성한 VIB 설치 가능

<table>
<tr><td>진단항목</td><td colspan="2">ES-21. MOB(Managed Object Browser) 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">MOB(Managed Object Browser)는 관리 대상 객체 브라우저로 호스트를 관리하는데 사용되는 객체 모델을 탐색하는 방법을 제공하지만 동시에 호스트의 설정 구성도 변경이 가능하므로 MOB를 비활성화 하는 것이 좋다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">MOB가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">MOB가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ MOB 활성화 여부 확인
<CLI>
vim-cmd proxysvc/service_list 입력 후 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ MOB 비활성화
<CLI>
vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect" 입력
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">ES-22. 불필요한 서비스 제거</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">서버에 불필요한 서비스의 Port들이 열려 있는 경우 주요 시스템 정보 노출 및 서비스 거부(DOS)를 야기시킬 수 있다. ESXi를 이용한 클라우드 컴퓨팅 서비스를 위해 서버관리용으로 SSH와 Vsphere Client를 제공하고 있으며, 클라우드 컴퓨팅 서비스에 불필요한 ftp 등을 사용 할 경우 각각의 프로토콜에 대한 취약점으로 인해 root권한 획득, Dos공격 등 다양한 공격의 대상이 될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 서비스가 활성화되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 서비스가 활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 오픈된 서비스 확인
esxcli network ip connection list
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 서비스 사용 여부 확인 후 비활성화 또는 최신 버전 패치
1) 서비스 필요 시
최신 버전 설치
2) 서비스 불필요 시
vClient 실행 > 구성 > 보안 프로파일 > 서비스 > 속성에서 불필요한 서비스 확인 후 중지</td></tr>
<tr><td>비고</td><td colspan="4"><table>
<tr><th colspan="4">ESXi 설치 시 기본적으로 열리는 포트</th></tr>
<tr><td>SSH Server(22)</td><td>DNS Client(53)</td><td>DHCP Client(68)</td><td>SNMP(161)</td></tr>
<tr><td>HTTP(80)</td><td>SLPv2(427)</td><td>SSL(443)</td><td>인증 및 원격 접속 프로토콜(902)</td></tr>
</table></td></tr>
</table>

다. 패치 및 로그관리

<table>
<tr><td>진단항목</td><td colspan="2">ES-23. 불필요한 서비스 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">ESXi Update는 ESXi 응용프로그램, 서비스, 실행 파일 등의 오류나 보안 취약점 등을 수정하여 적용한 Update 파일이다. Update Patch 발표 후 취약성을 이용한 공격 도구가 먼저 출현 할 수 있으므로, Update Patch는 발표 후 가능한 빨리 설치 할 것을 권장한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패치 적용 정책을 수립하지 않거나 주기적으로 패치를 관리하고 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 설정 기준 권고 (또는 정책기준)
1) 보안 취약점이 발표되면 시스템 영향도를 평가하고, 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응하는 것이 좋음
2) 패치를 수행할 시 시스템의 영향도에 따라 패치를 차등 수행하도록 해야 함
3) 시스템 운영에 영향을 주지 않는 범위 내에서 주기적으로 패치를 수행할 것을 권고함</td></tr>
<tr><td>비고</td><td colspan="4">※ ESXi Life Cycle (2020년 9월 1일 기준)
<table><tr><th>버전 정보</th><th>출시 날짜</th><th>일반 지원 종료 날짜</th><th>기술 지도 종료 날짜</th></tr><tr><td>ESXi 5.5</td><td>2013년 09월 19일</td><td>2018년 09월 19일</td><td>2020년 09월 19일</td></tr><tr><td>ESXi 6.0</td><td>2015년 03월 12일</td><td>2020년 03월 12일</td><td>2022년 03월 12일</td></tr><tr><td>ESXi 6.5</td><td>2016년 11월 15일</td><td>2021년 11월 15일</td><td>2023년 11월 15일</td></tr><tr><td>ESXi 6.7</td><td>2018년 04월 17일</td><td>2022년 10월 15일</td><td>2023년 11월 15일</td></tr><tr><td>ESXi 7.0</td><td>2020년 04월 02일</td><td>2025년 04월 02일</td><td>2027년 04월 02일</td></tr></table></td></tr>
</table>

진단항목	ES-24. 로그의 정기적 검토 및 보고	취약도	상
항목설명	로그 정보는 침해사고 발생 시 해킹의 흔적 및 공격기법을 확인할 수 있는 중요 자료로 정기적인 로그분석을 통하여 시스템 침입 흔적과 취약점을 확인할 수 있다.		
진단기준	양호	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지고 있는 경우	
	취약	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우	
진단방법	▪ 인터뷰를 통해 정기적인 로그 분석에 대한 결과물 확인		
조치방법	▪ 로그 파일에는 해킹의 흔적들이 남겨져 있을 수 있으므로, 다음과 같이 로그 파일의 백업에 대한 검토를 해야 함 1) 반복적인 로그인 실패에 관한 로그 2) 로그인 거부 메시지에 관한 로그 3) 기본적 log 파일의 위치는 /var/log		
비고			

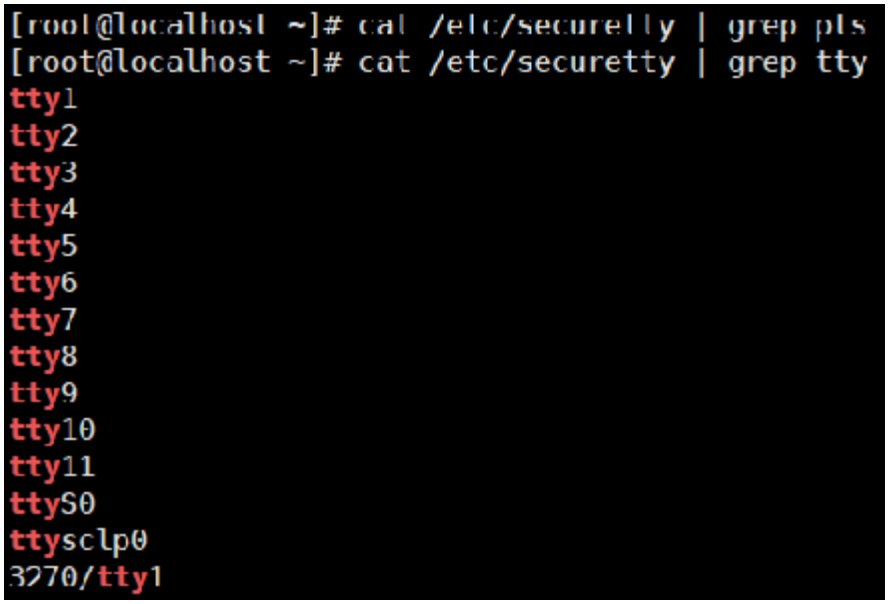
2.3. Linux

계정 관리(5개 항목), 파일 및 디렉토리 관리(14개 항목), 서비스 관리(15개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 36개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	U-01	root 계정 원격 접속 제한	상
	U-02	패스워드 복잡성 설정	상
	U-03	계정 잠금 임계값 설정	상
	U-04	패스워드 최대 사용 기간 설정	중
	U-05	패스워드 파일 보호	상
나. 파일 및 디렉토리 관리	U-06	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-07	파일 및 디렉터리 소유자 설정	상
	U-08	/etc/passwd 파일 소유자 및 권한 설정	상
	U-09	/etc/shadow 파일 소유자 및 권한 설정	상
	U-10	/etc/hosts 파일 소유자 및 권한 설정	상
	U-11	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-12	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	U-13	/etc/services 파일 소유자 및 권한 설정	상
	U-14	SUID, SGID, Sticky bit 설정 파일 점검	상
	U-15	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상
	U-16	world writable 파일 점검	상
	U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-18	접속 IP 및 포트 제한	상
	U-19	cron 파일 소유자 및 권한 설정	상
다. 서비스 관리	U-20	Finger 서비스 비활성화	상
	U-21	Anonymous FTP 비활성화	상
	U-22	r 계열 서비스 비활성화	상
	U-23	DoS 공격에 취약한 서비스 비활성화	상
	U-24	NFS 서비스 비활성화	상
	U-25	NFS 접근통제	상
	U-26	automountd 제거	상
	U-27	RPC 서비스 확인	상
	U-28	NIS, NIS+ 점검	상
	U-29	tftp, talk 서비스 비활성화	상
	U-30	Sendmail 버전 점검	상
	U-31	스팸 메일 릴레이 제한	상
	U-32	일반사용자의 Sendmail 실행 방지	상
	U-33	DNS 보안 버전 패치	상
	U-34	DNS ZoneTransfer 설정	상
라. 패치 및 로그관리	U-35	최신 보안패치 및 벤더 권고사항 적용	상
	U-36	로그의 정기적 검토 및 보고	상

[표 3] Linux서버 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">U-01. root 계정 원격 접속 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 root 원격 접속 차단이 적용되지 않은 시스템의 root 계정 정보를 비인가자가 획득할 경우 시스템 계정 정보 유출, 파일 및 디렉터리 변조 등의 행위 침해사고가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우</td></tr>
<tr><td>취약</td><td colspan="3">원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ Telnet
1) /etc/securetty 파일에 pts/0 ~ pts/x 관련 설정이 존재하는지 확인
cat /etc/securetty
 

※ tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함
※ pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함

■ SSH
1) /etc/ssh/sshd_config 파일에서 Root 로그인 설정 확인
cat /etc/ssh/sshd_config | grep PermitRootLogin</td></tr>
</table>

<table>
<tr><td></td><td>

```
[root@localhost ~]# cat /etc/ssh/sshd_config | grep PermitRo
otLogin
#PermitRootLogin yes
# the setting of "PermitRootLogin without-password".
```

</td></tr>
<tr><td>조치방법</td><td>

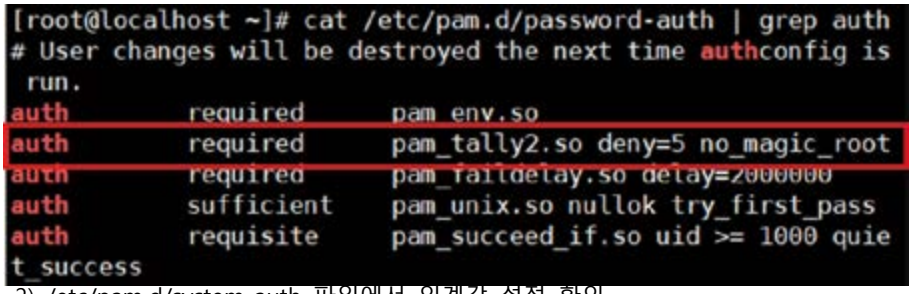
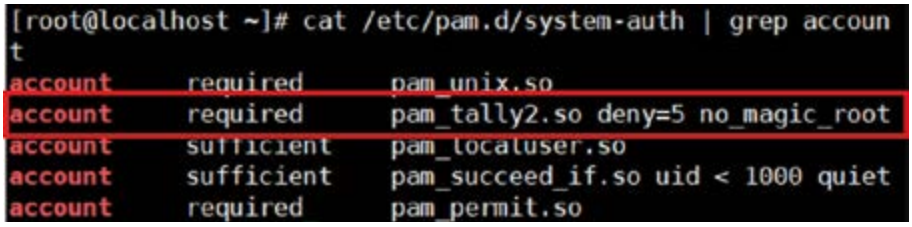
■ Telnet
1) "/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리
■ SSH
1) vi 편집기를 이용하여 /etc/ssh/sshd_config 파일을 연 후
vi /etc/ssh/sshd_config
2) 아래와 같이 설정 변경
PermitRootLogin no

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

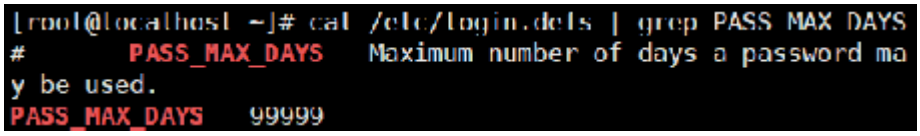
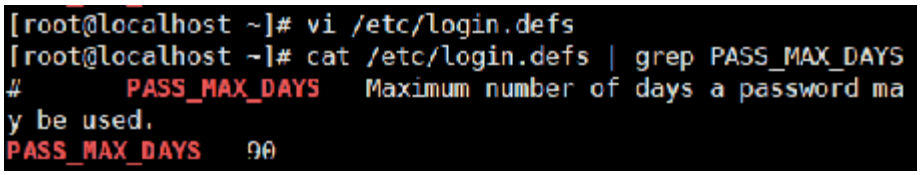
</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-02. 패스워드 복잡성 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드 복잡성 설정이 되어 있지 않은 사용자 계정 패스워드 존재 시 비인가자가 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 통해 취약한 패스워드가 설정된 사용자 계정의 패스워드를 획득하여 획득한 사용자 계정 정보를 통해 해당 사용자 계정의 시스템에 접근할 수 있는 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">영문, 숫자, 특수문자를 조합하여 2종류 조합 시 10자리 이상, 3종류 이상 조합 시 8자리 이상의 패스워드가 설정된 경우(공공기관 9자리 이상)</td></tr>
<tr><td>취약</td><td colspan="3">영문, 숫자, 특수문자를 조합하지 않거나 2종류 조합 시 10자리 미만, 3종류 이상 조합 시 8자리 미만의 패스워드가 설정된 경우(공공기관 9자리 미만)</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Debian 계열
1) /etc/pam.d/common-password 파일 또는
/etc/security/pwquality.conf 파일 설정 내용 확인
cat /etc/pam.d/common-password 또는
cat /etc/security/pwquality.conf
▪ RHEL 계열
1) /etc/pam.d/system-auth 파일 또는
/etc/security/pwquality.conf 파일 설정 내용 확인
cat /etc/pam.d/system-auth
cat /etc/security/pwquality.conf</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Debian 계열
1) /etc/pam.d/common-password 파일 또는
/etc/security/pwquality.conf 파일 편집
vi /etc/pam.d/common-password 또는
vi /etc/security/pwquality.conf
password requisite
pam_pwquality.so enforce_for_root
retry=3 minlen=8 dcredit=-1
ucredit=-1 lcredit=-1 ocredit=-1
▪ RHEL 계열
1) /etc/pam.d/system-auth 파일 또는
/etc/security/pwquality.conf 파일 편집
vi /etc/pam.d/system-auth 또는
vi /etc/security/pwquality.conf</td></tr>
</table>

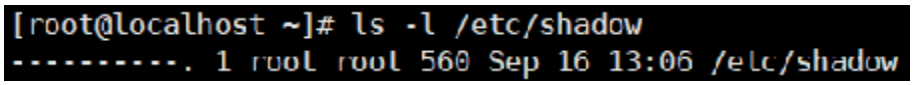
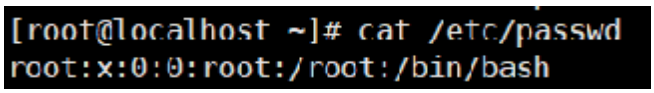
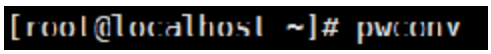
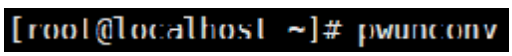
	password requisite pam_pwquality.so try_first_pass local_users_only enforce_for_root retry=3 authtok_type= minlen=8 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1
비고	lcredit=-1(최소 소문자 요구), ucredit=-1(최소 대문자 요구), dcredit=-1(최소 숫자 요구), ocredit=-1(최소 특수문자 요구), minlen=8(최소 8자리 이상) enforce_for_root(root 계정의 경우에도 정책 적용)

<table>
<tr><td>진단항목</td><td colspan="2">U-03. 계정 잠금 임계값 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">로그인 실패 임계값이 설정되어 있지 않을 경우 반복되는 로그인 시도에 대한 차단이 이루어지지 않아 각종 공격(무작위 대입 공격, 사전 대입 공격, 추측 공격 등)에 취약하여 비인가자에게 사용자 계정 패스워드를 유출 당할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ Debian 계열
1) /etc/pam.d/common-auth 파일에서 임계값 설정 확인
cat /etc/pam.d/common-auth
■ RHEL 계열
1) /etc/pam.d/password-auth 파일에서 임계값 설정 확인
cat /etc/pam.d/password-auth
 
2) /etc/pam.d/system-auth 파일에서 임계값 설정 확인
cat /etc/pam.d/system-auth
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ Debian 계열
1) /etc/pam.d/common-auth 파일 내 설정 값을 변경
vi /etc/pam.d/common-auth
auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄)
■ RHEL 계열
1) /etc/pam.d/system-auth 및 /etc/pam.d/password-auth 파일 내 설정 값</td></tr>
</table>

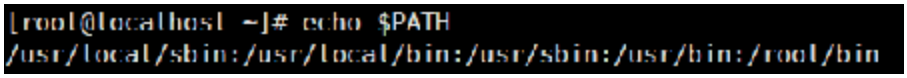
	변경 # vi /etc/pam.d/system-auth auth required pam_tally2.so deny=5 no_magic_root (첫 번째 단락 2번째 줄) # vi /etc/pam.d/password-auth account required pam_tally2.so deny=5 no_magic_root (두 번째 단락 2번째 줄)
비고	RHEL 계열의 경우, /etc/pam.d/system-auth 파일은 Console 접근, password-auth 파일은 SSH 접근 시 영향 받으므로 2가지 파일 모두 설정해야 함

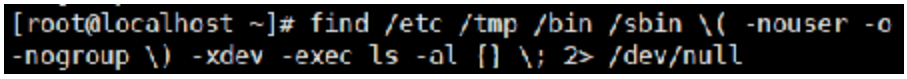
<table>
<tr><td>진단항목</td><td colspan="2">U-04. 패스워드 최대 사용 기간 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드 최대 사용기간을 설정하지 않은 경우 비인가자의 각종 공격(무작위 대입 공격, 사전 대입 공격 등)을 시도할 수 있는 기간 제한이 없으므로 공격자 입장에서는 장기적인 공격을 시행할 수 있어 시행한 기간에 비례하여 사용자 패스워드가 유출될 수 있는 확률이 증가한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드의 최대 사용기간이 90일 이내로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드의 최대 사용기간이 없거나, 90일 이내로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/login.defs 파일에서 패스워드 최대 사용 기간의 설정 값 확인
cat /etc/login.defs | grep PASS_MAX_DAYS
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ User 생성 시 적용
vi /etc/login.defs
PASS_MAX_DAYS 90
 

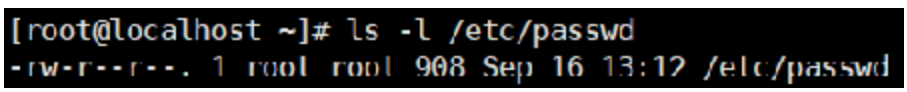
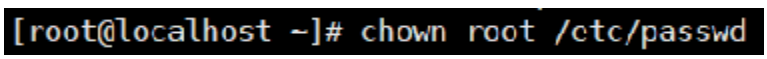
■ 현재 User의 최대 사용기간 적용
chage –M 90 <계정명></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

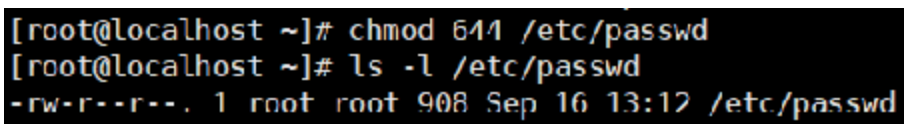
<table>
<tr><td>진단항목</td><td colspan="2">U-05. 패스워드 파일 보호</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">비인가자에 의해 사용자 계정 패스워드가 평문으로 저장된 파일이 유출될 경우 시스템 사용자 계정 패스워드가 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">쉐도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우</td></tr>
<tr><td>취약</td><td colspan="3">쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/shadow 파일 존재 확인
ls –l /etc/shadow
 
▪ /etc/passwd 파일 내 두 번째 필드가 “x”표시가 되어 있는지 확인
cat /etc/passwd
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 쉐도우 패스워드 정책 적용 방법
pwconv
 
▪ 일반 패스워드 정책 적용 방법
pwunconv
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

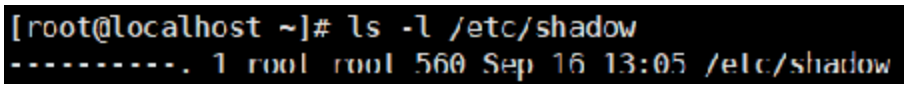
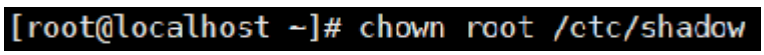
나. 파일 및 디렉토리 관리

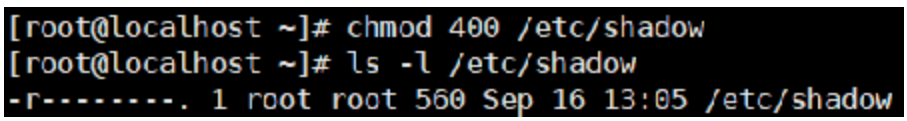
<table>
<tr><td>진단항목</td><td colspan="2">U-06. root 홈, 패스 디렉터리 권한 및 패스 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자가 명령어(예: ls, mv, cp등)를 수행했을 때 root 계정의 PATH 환경변수에 "." (현재 디렉터리 지칭)이 포함되어 있으면 현재 디렉터리에 명령어와 같은 이름의 악성파일이 실행되어 악의적인 행위가 일어날 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">PATH 환경변수에 “.”이 맨 앞이나 중간에 포함되지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">PATH 환경변수에 “.”이 맨 앞이나 중간에 포함된 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ echo $PATH 명령어로 현재 설정된 PATH 값 확인
echo $PATH
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ vi 편집기를 이용하여 root 계정의 설정파일(~/.profile 과 /etc/profile)을 연 후
vi /etc/profile
▪ 아래와 같이 수정
(수정 전) PATH=.:$PATH:$HOME/bin
(수정 후) PATH=$PATH:$HOME/bin</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

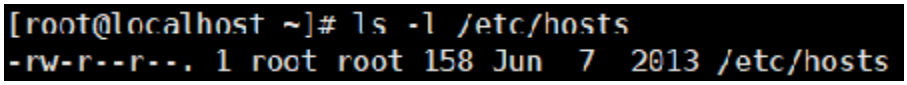
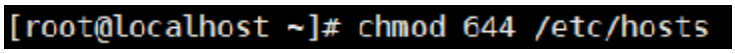
<table>
<tr><td>진단항목</td><td colspan="2">U-07. 파일 및 디렉터리 소유자 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">삭제된 소유자의 UID와 동일한 사용자가 해당 파일, 디렉터리에 접근 가능하여 사용자 정보 등 중요 정보가 노출될 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 시스템에서 소유자나 그룹이 존재하지 않는 파일 및 디렉터리를 검색
find / -nouser –o –nogroup 또는
find /etc /tmp /bin /sbin ₩(-nouser -o -nogroup ₩) -xdev -exec ls -al {} ₩; 2> /dev/null
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제
rm <file_name>
rm –rf <directory_name>
※ 삭제할 파일명 또는, 디렉터리 명 입력
▪ 필요한 경우 chown 명령으로 소유자 및 그룹 변경
chown <user_name> <file_name></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

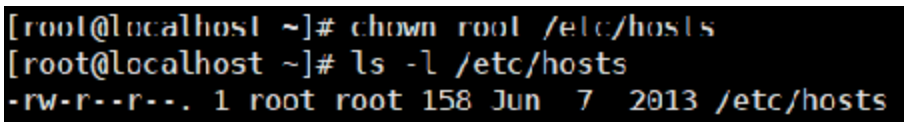
<table>
<tr><td>진단항목</td><td colspan="2">U-08. /etc/passwd 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자(root) 외 사용자가 "/etc/passwd" 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/passwd 파일의 소유자가 root이고, 권한이 644이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/passwd 파일의 퍼미션과 소유자를 확인
ls –l /etc/passwd
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/passwd 파일의 소유자 및 권한 변경(소유자 root, 권한 644)
chown root /etc/passwd
 

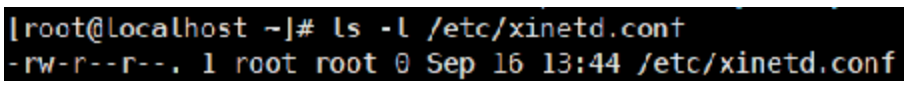
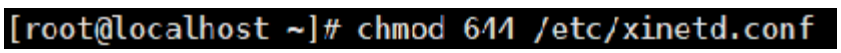
chmod 644 /etc/passwd
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

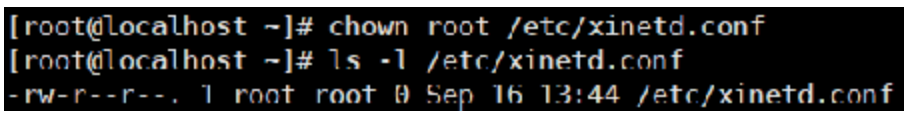
<table>
<tr><td>진단항목</td><td colspan="2">U-09. /etc/shadow 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/shadow 파일의 소유자가 root이고, 권한이 400이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/shadow 파일의 퍼미션과 소유자를 확인
ls –l /etc/shadow
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ "/etc/shadow" 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)
chown root /etc/shadow
 

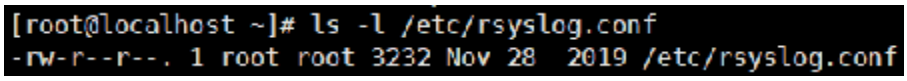
chmod 400 /etc/shadow
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

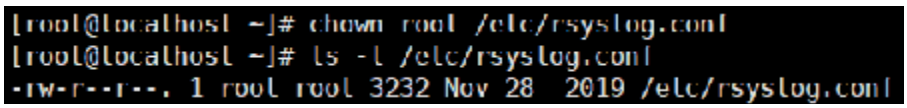
<table>
<tr><td>진단항목</td><td colspan="2">U-10. /etc/hosts 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/hosts 파일의 소유자가 root이고, 권한이 644 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/hosts 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/hosts 파일의 퍼미션과 소유자를 확인
ls –l /etc/hosts
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/hosts 파일의 퍼미션을 644로, 소유자를 root로 변경
chmod 644 /etc/hosts
 

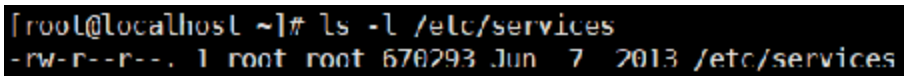
chown root /etc/hosts
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

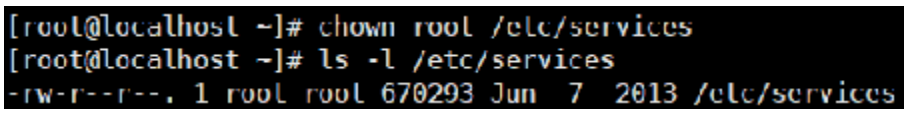
<table>
<tr><td>진단항목</td><td colspan="2">U-11. /etc/(x)inetd.conf 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">(x)inetd.conf 파일에 비인가자의 쓰기 권한이 부여되어 있을 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/(x)inetd.conf 파일의 소유자가 root이고, 권한이 644이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/(x)inetd.conf 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/(x)inetd.conf 파일의 퍼미션과 소유자를 확인
ls –l /etc/(x)inetd.conf
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/(x)inetd.conf 파일의 퍼미션을 644로, 소유자를 root로 변경
chmod 644 /etc/(x)inetd.conf
 

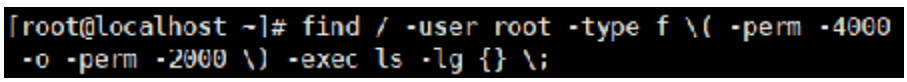
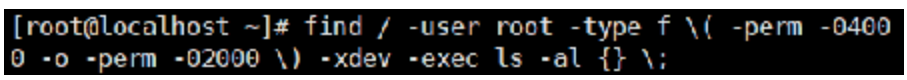
chown root /etc/(x)inetd.conf
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-12. /etc/(r)syslog.conf 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">(r)syslog.conf 파일의 접근권한이 적절하지 않을 경우, 임의적인 파일 변조로 인해 침입자의 흔적 또는, 시스템 오류 사항을 분석하기 위해 반드시 필요한 시스템 로그가 정상적으로 기록되지 않을 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/(r)syslog.conf 파일의 소유자가 root이고, 권한이 644이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/(r)syslog.conf 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/(r)syslog.conf 파일의 퍼미션과 소유자를 확인
ls –l /etc/(r)syslog.conf
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/(r)syslog.conf 파일의 퍼미션을 644로, 소유자를 root로 변경
chmod 644 /etc/(r)syslog.conf
 

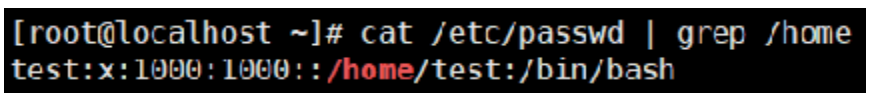
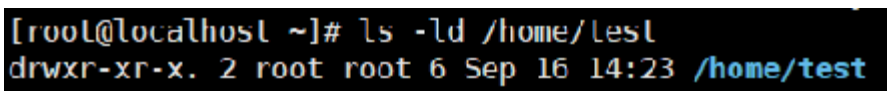
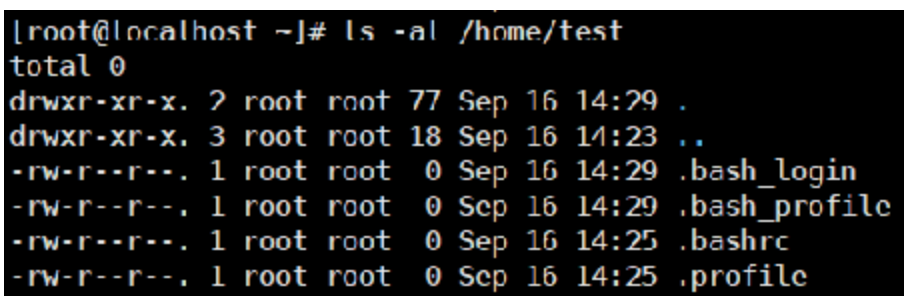
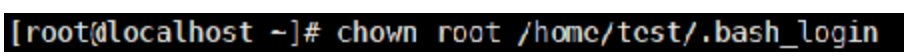
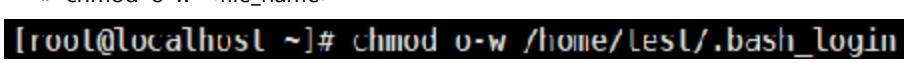
chown root /etc/(r)syslog.conf
 
</td></tr>
<tr><td>비고</td><td colspan="4">▪ root, bin, sys 등 시스템에서 사용하는 계정이 아닌 일반 계정에게 소유 권한이 부여되지 않도록 하여야 함</td></tr>
</table>

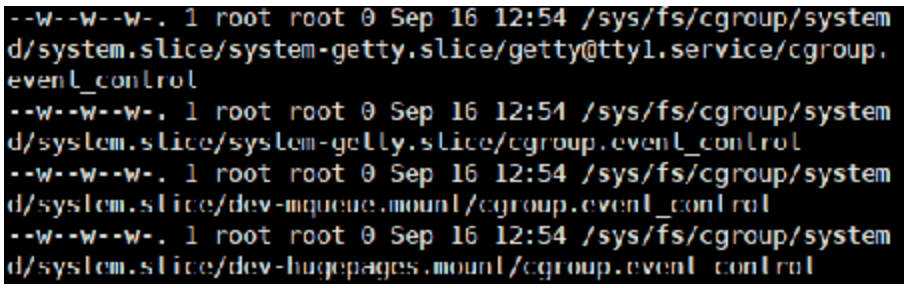
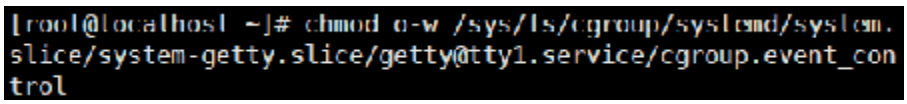
<table>
<tr><td>진단항목</td><td colspan="2">U-13. /etc/services 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">services 파일의 접근권한이 적절하지 않을 경우 비인가 사용자가 운영 포트 번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈하여 악성 서비스를 의도적으로 실행할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/services 파일의 소유자가 root이고, 권한이 644이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/services 파일의 소유자가 root가 아니거나, 권한이 644초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/services 파일의 퍼미션과 소유자를 확인
ls –l /etc/services
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/services 파일의 퍼미션을 644로, 소유자를 root로 변경
chmod 644 /etc/services
 

chown root /etc/services
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-14. SUID, SGID, Sticky bit 설정 파일 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상 서비스 장애를 발생시킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래와 같은 명령어를 통해 SUID와 SGID 파일을 검색하여 주요 파일의 권한을 확인
find / -user root -type f ₩(-perm -4000 -o -perm -2000 ₩) -exec ls -lg {} ₩;
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 제거 방법
chmod -s <file_name>
▪ 주기적인 감사 방법
find / -user root -type f ₩(-perm -04000 -o -perm -02000 ₩) -xdev -exec ls -al {} ₩;
 

▪ 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법(일반 사용자의 Setuid 사용을 제한함, 임의의 그룹만 가능)
/usr/bin/chgrp <group_name> <setuid_file_name>
/usr/bin/chmod 4750 <setuid_file_name></td></tr>
<tr><td>비고</td><td colspan="4">SUID 제거 시 OS 및 응용 프로그램 등 서비스 정상작동 유무 확인 필요</td></tr>
</table>

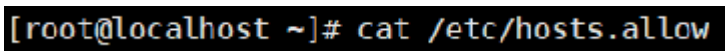
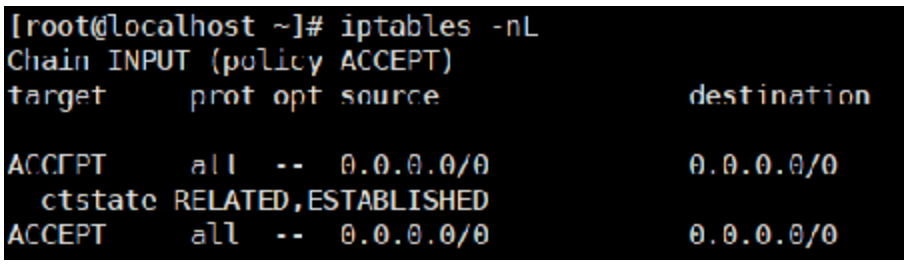
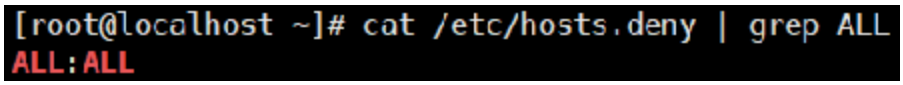
<table>
<tr><td>진단항목</td><td colspan="2">U-15. 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">홈 디렉터리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우 비인가자가 환경변수 파일을 변조하여 정상 사용중인 사용자의 서비스가 제한될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이고 권한이 644로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이 아니거나 권한이 644로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 사용자 홈 디렉터리 확인
cat /etc/passwd | grep /home
 
▪ 해당 홈 디렉터리 소유자 및 권한 확인
ls –ld <사용자 홈 디렉터리> (홈 디렉터리 소유자 및 권한 확인)
 
ls –al <사용자 홈 디렉터리> (홈 디렉터리 내 환경설정 파일 소유자 및 권한 확인)
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 소유자 변경 방법
chown <user_name> <file_name>
 
▪ 일반 사용자 쓰기 권한 제거 방법
chmod o-w <file_name>
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-16. world writable 파일 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 덧붙이거나 지울 수 있게 되어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ world writable 파일 존재 여부 확인
find / -type f -perm -2 -exec ls -l {} ₩;
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 일반 사용자 쓰기 권한 제거 방법
chmod o-w <file_name>
 

▪ 파일 삭제 방법
rm -rf <world-writable 파일명></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

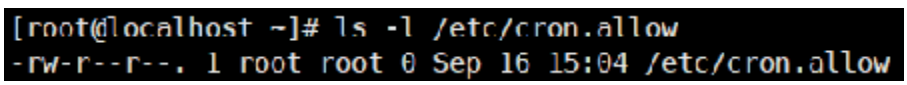
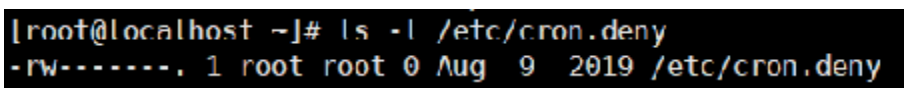
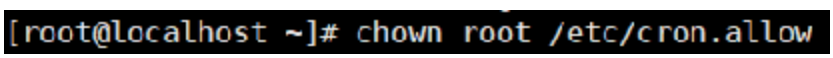
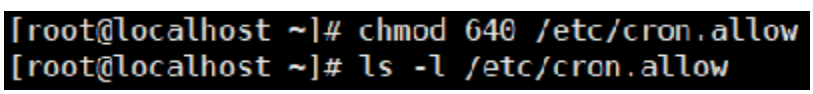
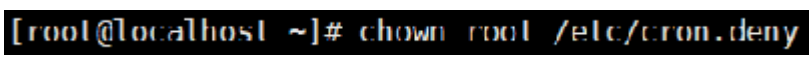
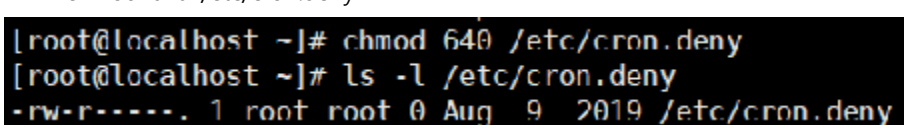
<table>
<tr><td>진단항목</td><td colspan="2">U-17. $HOME/.rhosts, hosts.equiv 사용 금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">rlogin, rsh 등과 같은 'r' command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템상의 임의의 명령을 수행시킬 수 있으며, 명령어 원격 실행을 통해 중요 정보 유출 및 시스템 장애를 유발시킬 수 있다. 또한 공격자 백도어 등으로도 활용될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600 이하인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우
- /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">login, shell, exec 서비스를 사용하거나, 사용 시 아래와 같은 설정이 적용되어 있지 않은 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600 이하인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에 '+' 설정이 없는 경우
- /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 파일 소유자 및 권한 확인
ls -al /etc/hosts.equiv
ls -al $HOME/.rhosts
■ 계정 별 '+' 부여 적절성 확인
cat /etc/hosts.equiv
cat $HOME/.rhosts</td></tr>
<tr><td>조치방법</td><td colspan="4">■ .rhosts, hosts.equiv 파일 미사용 시
1) .rhosts, hosts.equiv 파일 삭제
rm -f [삭제 할 파일 및 디렉터리 경로]
rm -f $HOME/.rhosts 또는 or /etc/ hosts.equiv
■ .rhosts, hosts.equiv 파일 사용 시
1) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 소유자를 root 또는, 해당 계정으로 변경
chown root /etc/hosts.equiv
chown [계정 명] $HOME/.rhosts
2) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일의 퍼미션을 600 이하로 변경
chmod 600 /etc/hosts.equiv
chmod 600 $HOME/.rhosts</td></tr>
</table>

	3) "/etc/hosts.equiv" 및 "$HOME/.rhosts" 파일에서 "+"를 제거하고 허용 호스트 및 계정 등록 # vi /etc/hosts.equiv (or $HOME/.rhosts)
비고	

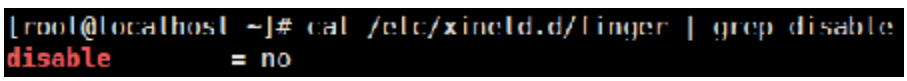
<table>
<tr><td>진단항목</td><td colspan="2">U-18. 접속 IP 및 포트 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ All deny 적용 확인 및 접근 허용 IP 적절성 확인 또는 iptables에서 서버로 접속 하는 IP 설정 확인
- /etc/hosts.deny, allow 설정 확인
cat /etc/hosts.deny
 
cat /etc/hosts.allow
 
- iptables 설정 확인
iptables –nL
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ vi 편집기를 이용하여 “/etc/hosts.deny” 파일을 연 후
vi /etc/hosts.deny
 
▪ 아래와 같이 수정 또는 추가 (ALL Deny 설정)
ALL:ALL
 

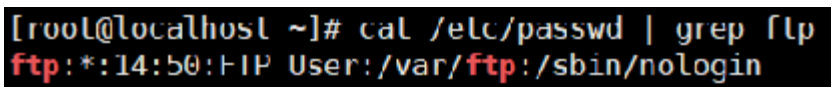
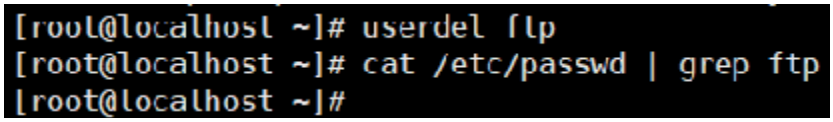
▪ vi 편집기를 이용하여 “/etc/hosts.allow” 파일을 연 후
vi /etc/hosts.allow</td></tr>
</table>

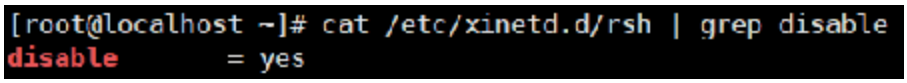
	[root@localhost ~]# vi /etc/hosts.allow ▪ 아래와 같이 접속 허용 서비스 및 IP 설정 sshd : 192.168.0.148, 192.168.0.6 (다른 서비스도 동일한 방식으로 설정) [root@localhost ~]# cat /etc/hosts.allow | grep sshd sshd : 192.168.88.128 ※ TCP Wrapper 접근제어 가능 서비스 SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH
비고	허용되지 않는 IP는 서비스 사용이 불가함

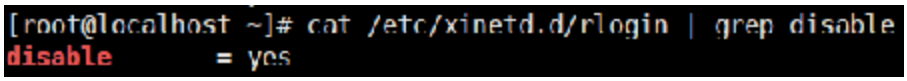
<table>
<tr><td>진단항목</td><td colspan="2">U-19. cron 파일 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">root 외 일반사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/crontab 파일의 소유자가 root이고, 권한이 640이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/crontab 파일의 소유자가 root가 아니거나, 권한이 640초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ “/etc/cron.allow” 및 “/etc/cron.deny” 파일의 소유자 및 권한 확인
ls –l /etc/cron.allow
 
ls –l /etc/cron.deny
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ “/etc/cron.allow” 및 “/etc/cron.deny” 파일의 소유자 및 권한 변경
chown root /etc/cron.allow
 
chmod 640 /etc/cron.allow
 
chown root /etc/cron.deny
 
chmod 640 /etc/cron.deny
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

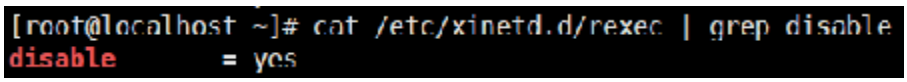
다. 서비스 관리

<table>
<tr><td>진단항목</td><td colspan="2">U-20. Finger 서비스 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">비인가자에게 사용자 정보가 조회되어 패스워드 공격을 통한 시스템 권한 탈취 가능성이 있으므로 사용하지 않는다면 해당 서비스를 중지하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">finger 서비스가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">finger 서비스가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ xinetd인 경우 /etc/xinetd.d/finger 파일에서 서비스 비활성화 여부 확인
cat /etc/xinetd.d/finger | grep disable
 
▪ inetd인 경우 /etc/inetd.conf 파일에서 finger 서비스 라인 #처리(주석처리) 또는 삭제 되어 있는지 확인
cat /etc/inetd.conf | grep finger</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/xinetd.d/finger 파일에서 서비스 비활성화 설정
vi /etc/xinetd.d/finger
disable = no</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-21. Anonymous FTP 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Anonymous FTP (익명 ftp) 접속을 차단한 경우</td></tr>
<tr><td>취약</td><td colspan="3">Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Default FTP를 사용하는 경우 /etc/passwd 파일에 ftp 계정 존재 여부 확인
cat /etc/passwd | grep ftp
 
▪ ProFTP를 사용하는 경우 proftpd.conf 파일에서 <Anonymous ~ ftp> 부분 확인
※ UserAlias 항목이 주석처리 되어있거나, 없으면 양호
cat etc/proftpd/proftpd.conf
UserAlias anonymous ftp
▪ vsFTP를 사용하는 경우 vsftpd.conf 파일에서 anonymous_enable 값이 No로 설정되어 있는지 확인
cat /etc/vsftpd/vsftpd.conf
anonymous_enable = Yes</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 일반 FTP - Anonymous FTP 접속 제한 설정 방법 "/etc/passwd" 파일에서 ftp 또는, anonymous 계정 삭제
userdel ftp
 
▪ ProFTP - Anonymous FTP 접속 제한 설정 방법
"/etc/passwd" 파일에서 ftp 계정 삭제
userdel ftp
▪ vsFTP - Anonymous FTP 접속 제한 설정 방법
vsFTP 설정파일("/etc/vsftpd/vsftpd.conf" 또는, "/etc/vsftpd.conf")에서 anonymous_enable=NO 설정</td></tr>
<tr><td>비고</td><td colspan="4">Anonymous FTP를 사용하지 않을 경우 영향 없음</td></tr>
</table>

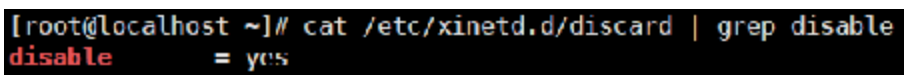
<table>
<tr><td>진단항목</td><td colspan="2">U-22. r 계열 서비스 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">서비스 포트가 열려있을 경우, 비인가자에 의한 중요 정보 유출 및 시스템 장애 발생 등 침해사고의 원인이 될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">r 계열 서비스(rlogin, rsh, rexec)가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">r 계열 서비스(rlogin, rsh, rexec)가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ xinetd인 경우 rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인
cat /etc/xinetd.d/rsh | grep disable
 

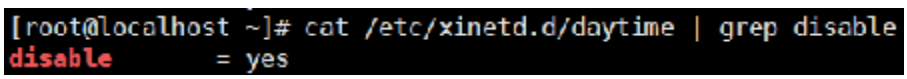
cat /etc/xinetd.d/rlogin | grep disable
 

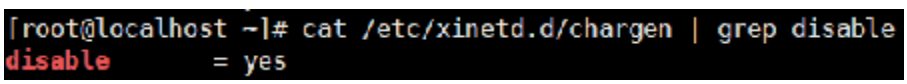
cat /etc/xinetd.d/rexec | grep disable
 

▪ inetd인 경우 rsh, rlogin, rexec (shell, login, exec) 서비스 비활성화 여부 확인
cat /etc/inetd.conf | egrep "rsh|rlogin|rexec" (주석 처리 되어 있으면 비활성화)</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 rlogin, rsh, rexec 파일을 연 후
▪ 아래와 같이 설정 (disable = yes 설정)
- /etc/xinetd.d/rlogin 파일
- /etc/xinetd.d/rsh 파일
- /etc/xinetd.d/rexec 파일
service rlogin
{
...
disable = yes
}</td></tr>
<tr><td>비고</td><td colspan="4">▪ rlogin, rshell, rexec 서비스는 backup 등의 용도로 종종 사용되며 /etc/hosts.equiv 또는, 각 홈 디렉터리 밑에 있는. rhosts 파일에 설정 유무를 확인하여 해당 파일이 존재하지 않거나 해당파일 내에 설정이 없다면 사용하지 않는 것으로 파악</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-23. DoS 공격에 취약한 서비스 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS(서비스 거부 공격)의 대상이 될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 된 경우</td></tr>
<tr><td>취약</td><td colspan="3">Dos 공격에 취약한 echo, discard, daytime, chargen 서비스가 활성화 된 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 서비스 비활성화 여부 확인
cat /etc/xinetd.d/echo | grep disable
 

cat /etc/xinetd.d/discard | grep disable
 

cat /etc/xinetd.d/daytime | grep disable
 

cat /etc/xinetd.d/chargen | grep disable
 

▪ inetd인 경우 /etc/inetd.conf 파일에서 echo, discard, daytime, chargen 서비스 비활성화 여부 확인
cat /etc/inetd.conf | egrep “echo|discard|daytime|chargen” (주석 처리 되어 있으면 비활성화)</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ vi 편집기를 이용하여 "/etc/xinetd.d/" 디렉터리 내 echo, discard, daytime, chargen 파일 열기
▪ 아래와 같이 설정 (Disable = yes 설정)
/etc/xinetd.d/echo 파일(echo-dgram, echo-stream)
/etc/xinetd.d/discard 파일(discard-dgram, discard-stream)
/etc/xinetd.d/daytime 파일(daytime-dgram, daytime-stream)
/etc/xinetd.d/chargen 파일(chargen-dgram, chargen-stream)
service echo</td></tr>
</table>

	{ disable = yes id = echo-stream type = internal wait = no socket—type = stream } ■ xinetd 서비스 재시작 # service xinetd restart
비고	

진단항목	U-24. NFS 서비스 비활성화	취약도	상
항목설명	비인가자가 NFS 서비스로 인가되지 않은 시스템이 NFS 시스템 마운트하여 비인가된 시스템 접근 및 파일변조 등의 침해 행위 가능성이 존재한다.		
진단기준	양호	NFS 서비스 관련 데몬이 비활성화 되어 있는 경우	
	취약	NFS 서비스 관련 데몬이 활성화 되어 있는 경우	
진단방법	▪ NFS 데몬 구동 여부 확인 # ps -ef | grep nfsd		
조치방법	▪ NFS 데몬(nfsd)을 중지 # kill –9 [PID]		
비고	▪ showmount, share, exportfs 등의 명령어를 사용하여 로컬 서버에 마운트 되어 있는 디렉터리 확인 및 NFS 설정파일에 공유디렉터리 설정 여부 확인 후 해당 디렉터리가 존재하지 않을 경우 서비스 중지 가능		

진단항목	U-25. NFS 접근통제	취약도	상
항목설명	접근제한 설정이 적절하지 않을 경우 인증절차 없이 비인가자의 디렉터리나 파일의 접근이 가능하며, 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있다.		
진단기준	**양호**	NFS 서비스 사용 시 everyone 공유를 제한한 경우	
	취약	NFS 서비스 사용 시 everyone 공유를 제한하지 않은 경우	
진단방법	▪ everyone으로 시스템이 마운트 되어 있는지 확인 # showmount -e hostname ▪ /etc/exports 파일에서 접근 통제 설정 여부 확인 # cat /etc/exports - 취약한 설정 예 : /var/www/img *(ro,all_squash) - 양호한 설정 예 : /data 172.27.0.0/16(rw,no_root_squash)		
조치방법	▪ everyone 마운트 제거 # umount "파일시스템 이름" ▪ /etc/exports 파일에서 접근 통제 설정 # vi /etc/exports (예) /data 172.27.0.0/16(rw,no_root_squash)		
비고	▪ showmount, share, exportfs 등의 명령어를 사용하여 로컬 서버에 마운트 되어 있는 디렉터리 확인 및 NFS 설정파일에 공유디렉터리 설정 여부 확인 후 해당 디렉터리가 존재하지 않을 경우 서비스 중지 가능		

진단항목	U-26. automountd 제거	취약도	상
항목설명	파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 automountd 프로세스 권한으로 임의의 명령을 실행할 수 있다.		
진단기준	양호	automount 서비스가 비활성화 되어 있는 경우	
	취약	automount 서비스가 활성화 되어 있지 않은 경우	
진단방법	▪ automountd 서비스 데몬 확인 # ps -ef | grep auto		
조치방법	▪ automountd서비스 데몬 실행 중지 # kill –9 [PID] ▪ 시스템 재시작 시 automount 가 시작되지 않도록 설정 <방법1> 부팅스크립트에서 automountd 제거 # chkconfig --level 0123456 autofs off <방법2> 아래와 같이 파일경로 확인 후 파일명 변경 # mv /etc/rc2.d/S28autofs /etc/rc2.d/S28autofs.orig		
비고	▪ NFS 및 삼바(Samba) 서비스에서 사용 시 automountd 사용 여부 확인이 필요하며, 적용 시 CDROM의 자동 마운트는 이뤄지지 않음 (/etc/auto.*, /etc/auto_* 파일을 확인하여 필요 여부 확인) ※ 삼바(Samba) : 서로 다른 운영체제(OS) 간의 자원 공유를 위해 이용하는 서버로 같은 네트워크 내 연결된 PC는 서로 운영체제가 달라도 네트워크로 파일을 주고받을 수 있고 자원을 공유할 수 있음		

<table>
<tr><td>진단항목</td><td colspan="2">U-27. RPC 서비스 확인</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">버퍼 오버플로우(Buffer Overflow), Dos, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 RPC 서비스가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 RPC 서비스가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 RPC 서비스 파일에서 비활성화 여부 확인
cat /etc/xinetd.d/rstatd
▪ inetd인 경우 /etc/inetd.conf 파일에서 불필요한 RPC 서비스 비활성화 여부 확인
cat /etc/inetd.conf | grep rpc.cmsd</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내의 불필요한 RPC 서비스 파일을 연 후
▪ 아래와 같이 설정 (disable = yes 설정)
service rstatd
{
disable = yes
... 이하 생략 ...
}</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	U-28. NIS, NIS+ 점검	취약도	상
항목설명	보안상 취약한 서비스인 NIS를 사용하는 경우 비인가자가 타시스템의 root 권한 획득이 가능하므로 사용하지 않는 것이 가장 바람직하나 만약 NIS를 사용해야 하는 경우 사용자 정보보안에 많은 문제점을 내포하고 있는 NIS보다 NIS+를 사용하는 것을 권장한다.		
진단기준	양호	NIS, NIS+ 서비스가 구동 중이지 않을 경우	
	취약	NIS, NIS+ 서비스가 구동 중일 경우	
진단방법	▪ NIS, NIS+ 서비스 구동 확인 # ps -ef | egrep "ypserv|ypbind|ypxfrd|rpc.yppasswdd|rpc.ypupdated" | grep -v "grep"		
조치방법	▪ NFS 서비스 데몬 중지 # kill -9 [PID]		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">U-29. tftp, talk 서비스 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격자의 공격 시도가 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">tftp, talk 서비스가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">tftp, talk 서비스가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ xinetd인 경우 "/etc/xinetd.d/" 디렉터리 내 tftp, talk, ntalk서비스 파일에서 비활성화 여부 확인
cat /etc/xinetd.d/tftp
■ inetd인 경우 /etc/inetd.conf 파일에서 tftp, talk, ntalk 서비스 비활성화 여부 확인
cat /etc/inetd.conf | egrep “tftp|talk|”</td></tr>
<tr><td>조치방법</td><td colspan="4">■ vi 편집기를 이용하여 “/etc/xinetd.d/” 디렉터리 내 tftp, talk, ntalk 파일을 연 후
■ 아래와 같이 설정 (disable = yes 설정)
- /etc/xinetd.d/tftp 파일
- /etc/xinetd.d/talk 파일
- /etc/xinetd.d/ntalk 파일
service tftp
{
... 생략 ...
disable = yes
}</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-30. Sendmail 버전 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 유출 가능성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Sendmail 버전을 정기적으로 점검하고, 최신 버전 패치를 했을 경우</td></tr>
<tr><td>취약</td><td colspan="3">Sendmail 버전을 정기적으로 점검하지 않거나, 최신 버전 패치가 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Sendmail 프로세스 확인
ps -ef | grep sendmail
 
▪ Sendmail 버전 확인
cat /etc/mail/sendmail.cf | grep DZ</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Sendmail 서비스 실행 여부 및 버전 점검 후, http://www.sendmail.org/ 또는, 각 OS 벤더사의 보안 패치 설치</td></tr>
<tr><td>비고</td><td colspan="4">패치를 적용할 경우 시스템 및 서비스의 영향 정도를 충분히 고려하여야 함</td></tr>
</table>

진단항목	U-31. 스팸 메일 릴레이 제한		취약도	상
항목설명	SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸메일 서버로 사용하거나 Dos공격의 대상이 될 수 있다.			
진단기준	양호	SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우		
	취약	SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우		
진단방법	▪ SMTP 서비스 사용 여부 및 릴레이 제한 옵션 확인 # ps -ef | grep sendmail | grep -v "grep" # cat /etc/mail/sendmail.cf | grep "R$ ₩*" | grep "Relaying denied"			
조치방법	▪ vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후 ▪ 아래와 같이 주석 제거 (수정 전) #R$* $#error $@ 5.7.1 $: "550 Relaying denied" (수정 후) R$* $#error $@ 5.7.1 $: "550 Relaying denied" ▪ 특정 IP, domain, Email Address 및 네트워크에 대한 sendmail 접근 제한 확인 # vi /etc/mail/access			
비고	릴레이를 허용할 대상에 대한 정보를 입력한다면 영향 없음			

진단항목	U-32. 일반사용자의 Sendmail 실행 방지	취약도	상
항목설명	일반 사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있다.		
진단기준	양호	SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우	
	취약	SMTP 서비스 사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정되지 않은 경우	
진단방법	▪ sendmail.cf 파일에서 restrictqrun 옵션 설정 여부 확인 # cat /etc/mail/sendmail.cf | grep PrivacyOptions O PrivacyOptions=authwarnings, novrfy, noexpn		
조치방법	▪ vi 편집기를 이용하여 sendmail.cf 설정파일을 연 후 # vi /etc/mail/sendmail.cf ▪ O PrivacyOptions= 설정 부분에 restrictqrun 옵션 추가 (수정 전) O PrivacyOptions=authwarnings, novrfy, noexpn (수정 후) O PrivacyOptions=authwarnings, novrfy, noexpn, restrictqrun		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">U-33. DNS 보안 버전 패치</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신버전 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DNS 서비스를 사용하며, 주기적으로 패치를 관리하고 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ DNS 서비스 사용 및 BIND 버전 확인
ps -ef | grep named
named -v</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ [DNS 서비스를 사용할 경우]
1) “DNS” 서비스 사용 시 BIND 버전 확인 후 최신 버전으로 업데이트
▪ [DNS 서비스를 사용하지 않는 경우]
1) 서비스 중지
kill –9 [PID]</td></tr>
<tr><td>비고</td><td colspan="4">패치를 적용 시 시스템 및 서비스 영향 정도를 충분히 고려하여야 함</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">U-34. DNS ZoneTransfer 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우</td></tr>
<tr><td>취약</td><td colspan="3">DNS 서비스를 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 설정 파일에서 zone transfer 설정 확인
cat /etc/named.conf
<pre>Options {
allow-transfer{10.10.10.10;};
};</pre></td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 특정 서버의 Zone Transfer 지정
vi /etc/named.conf
<pre>Options {
allow-transfer{10.10.10.111; 10.10.10.112;};
};</pre>▪ 특정 도메인의 Zone에 대해서 제한할 경우에는 다음과 같이 설정
vi /etc/named.conf
<pre>zone "xxx.co.kr" {
Type master ;
File "db.xxx.co.kr";
allow-transfer{10.10.10.111; 10.10.10.112;};
}</pre></td></tr>
<tr><td>비고</td><td colspan="4">Zone 파일 전송을 허용할 대상을 정상적으로 등록할 경우 일반적으로 영향 없음</td></tr>
</table>

라. 패치 및 로그관리

진단항목	U-35. 최신 보안패치 및 벤더 권고사항 적용	취약도	상
항목설명	최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재한다.		
진단기준	양호	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있는 경우	
	취약	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않은 경우	
진단방법	▪ 패치 적용 정책 수립 여부 및 정책에 따른 패치 적용 여부 확인		
조치방법	▪ LINUX는 서버에 설치된 패치 리스트의 관리가 불가능하므로 rpm 패키지별 버그가 Fix된 최신 버전 설치가 필요함 ▪ LINUX는 오픈되고, 커스터마이징 된 OS이므로 LINUX를 구입한 벤더에 따라 rpm 패키지가 다를 수 있으며, 아래의 사이트는 RedHat LINUX에 대한 버그 Fix 관련 사이트임 <Red Hat 일 경우> 1) 다음의 사이트에서 해당 버전을 찾음 http://www.redhat.com/security/updates/ http://www.redhat.com/security/updates/eol/ (Red Hat LINUX 9 이하 버전) 2) 발표된 Update 중 현재 사용 중인 보안 관련 Update 찾아 해당 Update Download 3) Update 설치 # rpm -Uvh <pakage-name>		
비고			

진단항목	U-36. 로그의 정기적 검토 및 보고	취약도	상
항목설명	로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어렵다.		
진단기준	양호	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지고 있는 경우	
	취약	로그 기록의 검토, 분석, 리포트 작성 및 보고 등이 정기적으로 이루어지지 않는 경우	
진단방법	■ 로그 정책 수립 여부 및 정책에 따른 로그 검토 여부 확인		
조치방법	■ 다음과 같이 로그 파일의 백업에 대한 검토를 해야 함 1) su 시도에 관한 로그 2). 반복적인 로그인 실패에 관한 로그 3) 로그인 거부 메세지에 관한 로그 4) 기본적 log 파일의 위치는 /var/adm, /var/log ※ 커널과 시스템에 관련된 로그 메시지들은 syslogd와 klogd 두개의 데몬에 의해서 /var/log/messages에 기록하게 됨. 이 파일을 분석함으로써 시스템을 항상 점검 관리해야 함		
비고			

2.4. Windows Server

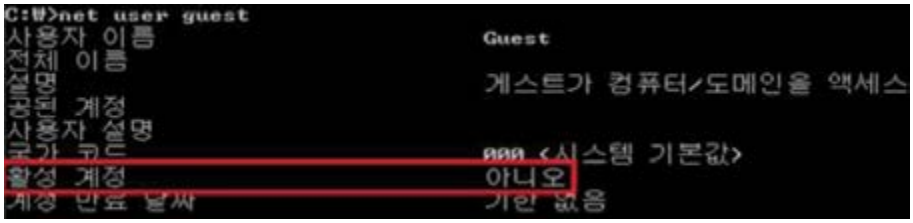
계정 관리(8개 항목), 서비스 관리(10개 항목), 패치 및 로그관리(5개 항목), 보안 관리(9개 항목), 총 4개 영역에서 32개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	W-01	Administrator 계정 이름 바꾸기	상
	W-02	GUEST 계정 상태	상
	W-03	불필요한 계정 제거	상
	W-04	계정 잠금 임계값 설정	상
	W-05	패스워드 최대 사용 기간 설정	중
	W-06	암호 사용 기간 제한 없음 제거	증
	W-07	해독 가능한 암호화를 사용하여 암호 저장	상
	W-08	관리자 그룹에 최소한의 사용자 포함	상
나. 서비스 관리	W-09	공유 권한 및 사용자 그룹 설정	상
	W-10	하드디스크 기본 공유 제거	상
	W-11	불필요한 서비스 제거	상
	W-12	NetBIOS 바인딩 서비스 구동 점검	상
	W-13	FTP 서비스 구동 점검	상
	W-14	FTP 디렉토리 접근권한 설정	상
	W-15	Anonymous FTP 금지	상
	W-16	FTP 접근 제어 설정	상
	W-17	DNS Zone Transfer 설정	상
	W-18	RDS(RemoteDataServices)제거	상
다. 패치 및 로그관리	W-19	최신 서비스 팩 적용	상
	W-20	최신 HOT FIX 적용	상
	W-21	백신 프로그램 업데이트	상
	W-22	로그의 정기적 검토 및 보고	상
	W-23	원격으로 엑세스할 수 있는 레지스트리 경로	상
라. 보안 관리	W-24	백신 프로그램 설치	상
	W-25	SAM 파일 접근 통제 설정	상
	W-26	화면보호기 설정	상
	W-27	로그온하지 않고 시스템 종료 허용	상
	W-28	원격 시스템에서 강제로 시스템 종료	상
	W-29	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상
	W-30	SAM 계정과 공유의 익명 열거 허용 안함	상
	W-31	Autologon기능 제어	상
	W-32	이동식 미디어 포맷 및 꺼내기 허용	상

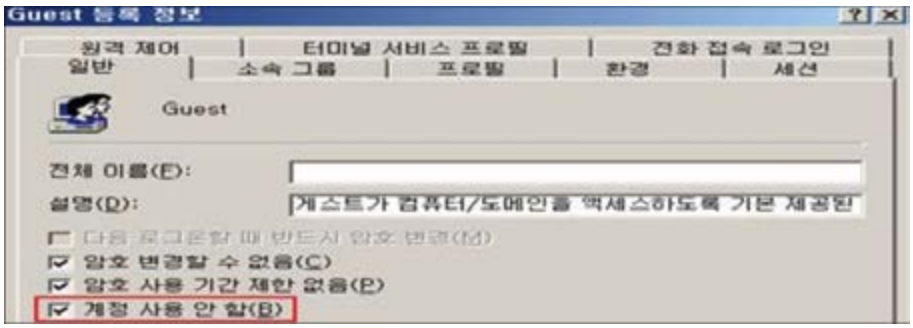
[표 4] Windows서버 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">W-01. Administrator 계정 이름 바꾸기</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일반적으로 관리자 계정으로 잘 알려진 Administrator를 변경하지 않은 경우 악의적인 사용자의 패스워드 추측 공격을 통해 사용 권한 상승의 위험이 있으며, 관리자를 유인하여 침입자의 액세스를 허용하는 악성코드를 실행할 우려가 있다. 윈도우즈 최상위 관리자 계정인 Administrator는 기본적으로 삭제하거나 잠글 수 없어 악의적인 사용자의 목표가 된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Administrator Default 계정 이름을 변경한 경우</td></tr>
<tr><td>취약</td><td colspan="3">Administrator Default 계정 이름을 변경하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net user 명령어 실행 후 Administrator 계정명 존재 유무 확인
 
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > "계정: Administrator 계정 이름 바꾸기"의 값을 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd> wmic UserAccount where Name="administrator" call Rename Name="변경할 계정명" 명령어 입력
[GUI]
■ 시작> 프로그램> 제어판> 관리도구> 로컬 보안 정책> 로컬 정책> 보안옵션
■ "계정: Administrator 계정 이름 바꾸기"를 유추하기 어려운 계정 이름으로 변경</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

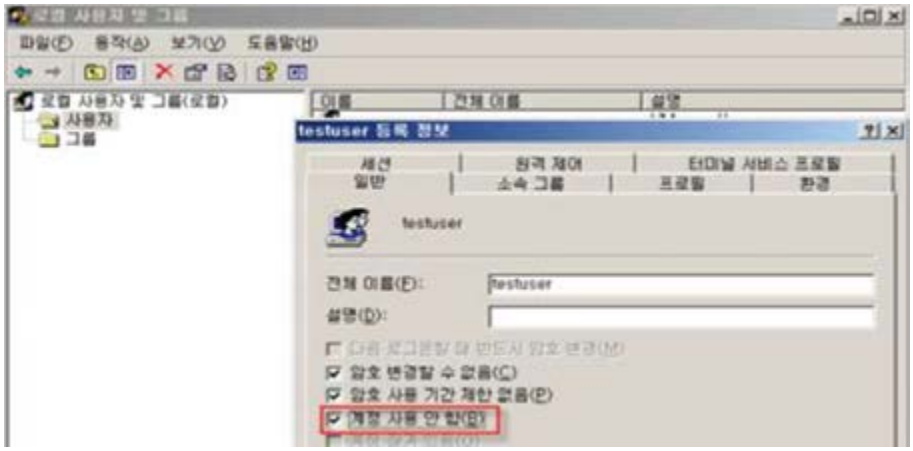
<table>
<tr><td>진단항목</td><td colspan="2">W-02. GUEST 계정 상태</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Guest 계정은 시스템에 임시로 액세스해야 하는 사용자용 계정으로, 이 계정을 사용하여 권한 없는 사용자가 시스템에 익명으로 액세스할 수 있으므로 비인가자 접근, 정보 유출 등 보안 위험이 따를 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Guest 계정이 비활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Guest 계정이 활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net user guest 명령어 실행 후 Guest 계정 활성 상태 확인
 

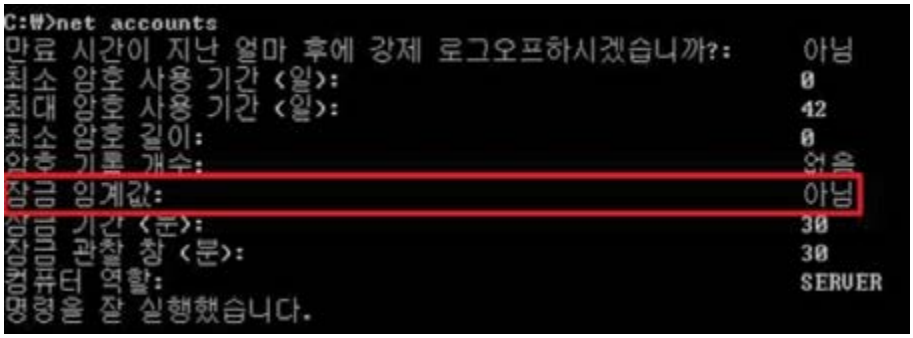
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > Guest 속성 > "계정 사용 안 함" 체크 유무 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd> net user guest /active:no 명령어 실행
[GUI]
■ 시작> 실행> LUSRMGR.MSC> 사용자> GUEST> 속성
■ "계정 사용 안 함" 체크</td></tr>
</table>

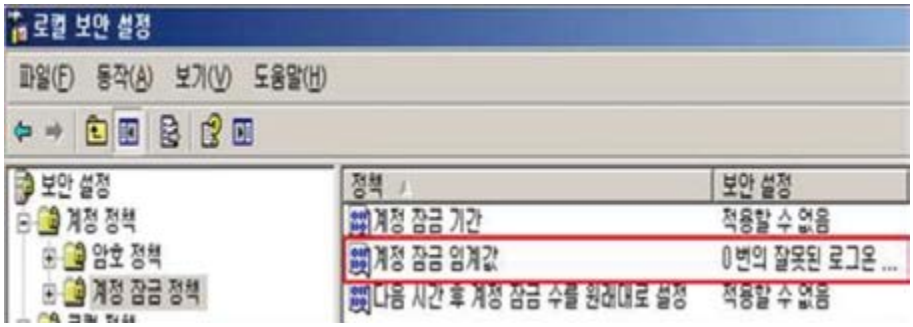
	 Guest 등록 정보 원격 제어 터미널 서비스 프로필 전화 접속 로그인 일반 소속 그룹 프로필 환경 세션 Guest 전체 이름(F): 설명(D): 게스트가 컴퓨터/도메인을 액세스하도록 기본 제공된 다음 로그온할 때 반드시 암호 변경(M) 암호 변경할 수 없음(C) 암호 사용 기간 제한 없음(P) 계정 사용 안 함(B)
비고	

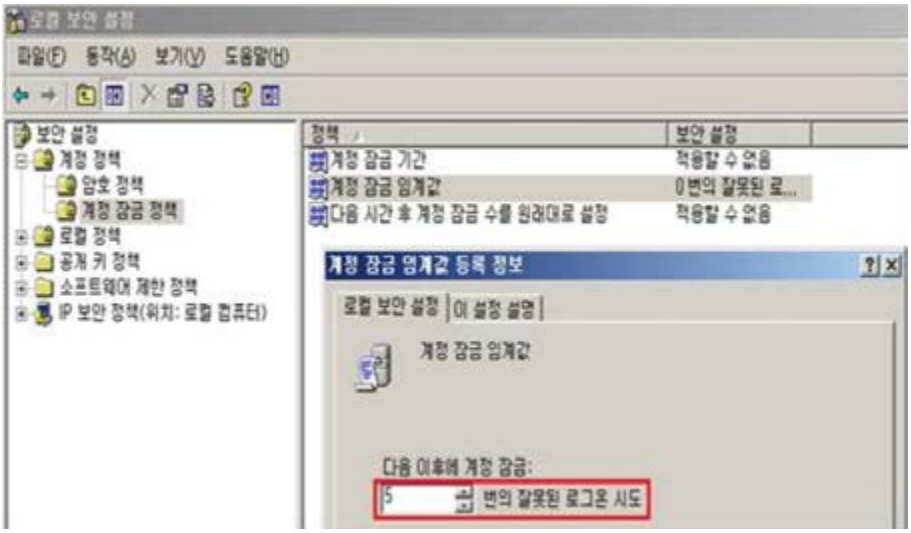
<table>
<tr><td>진단항목</td><td colspan="2">W-03. 불필요한 계정 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격 (Password Guessing Attack)의 가능성이 존재하며, 또한 이런 공격에 의해 계정 정보가 유출되어도 유출 사실을 인지하기 어렵다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 계정이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 계정이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net user 명령어 실행 후 사용자 계정 점검
 

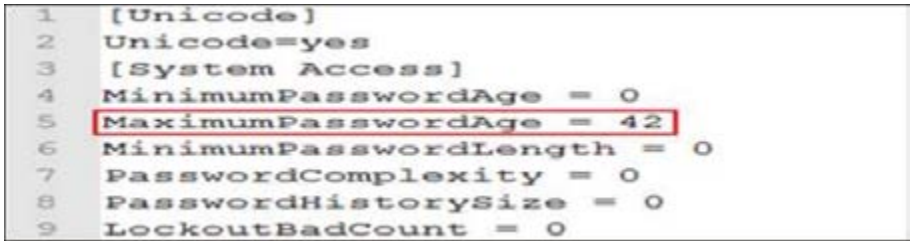
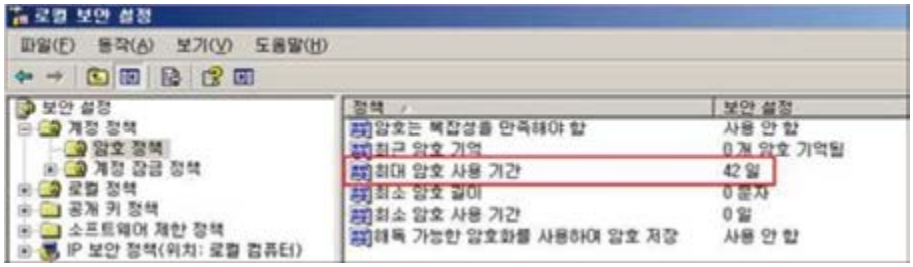
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > 속성 > "계정 사용 안함" 체크 유무 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd> net user “제거할 계정명” /delete를 입력하여 삭제
[GUI]
■ 시작> 실행> LUSRMGR.MSC> 사용자
■ 등록된 계정 중 불필요한 사용자 선택> 속성> "계정 사용 안 함"에 체크하거나 계정 삭제</td></tr>
</table>

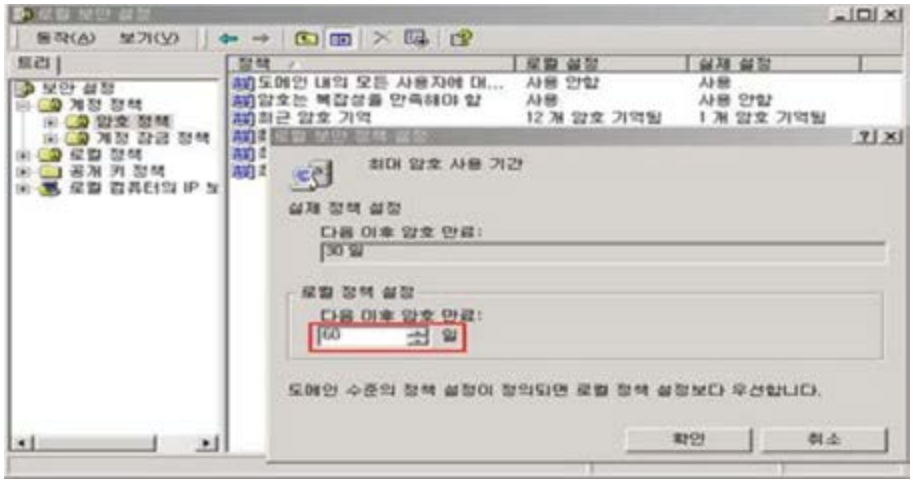
	
비고	▪ 명확하게 파악되지 않은 계정을 삭제하는 경우 해당 계정과 관련한 업무에 장애 발생 가능성이 존재함

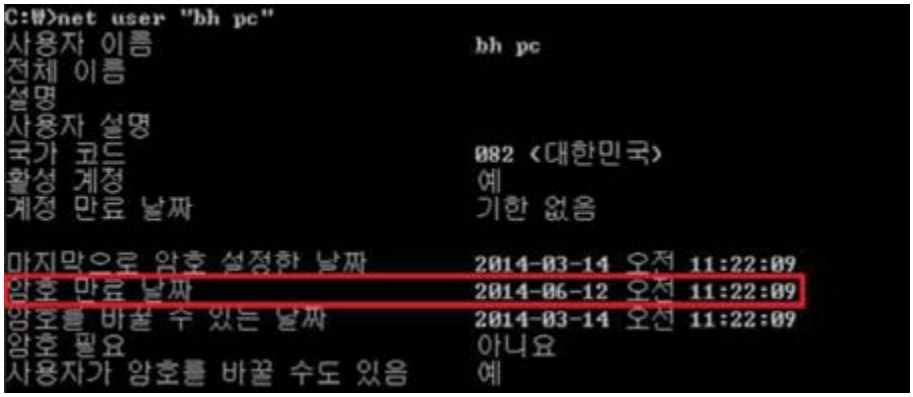
<table>
<tr><td>진단항목</td><td colspan="2">W-04. 계정 잠금 임계값 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">공격자는 시스템의 계정 잠금 임계값이 설정되지 않은 경우 자동화된 방법을 이용하여 모든 사용자 계정에 대해 암호조합 공격을 자유롭게 시도할 수 있으므로 사용자 계정 정보의 노출 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">계정 잠금 임계값이 6 이상의 값으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net accounts 명령어 실행 후 계정 잠금 임계값 설정 확인
 

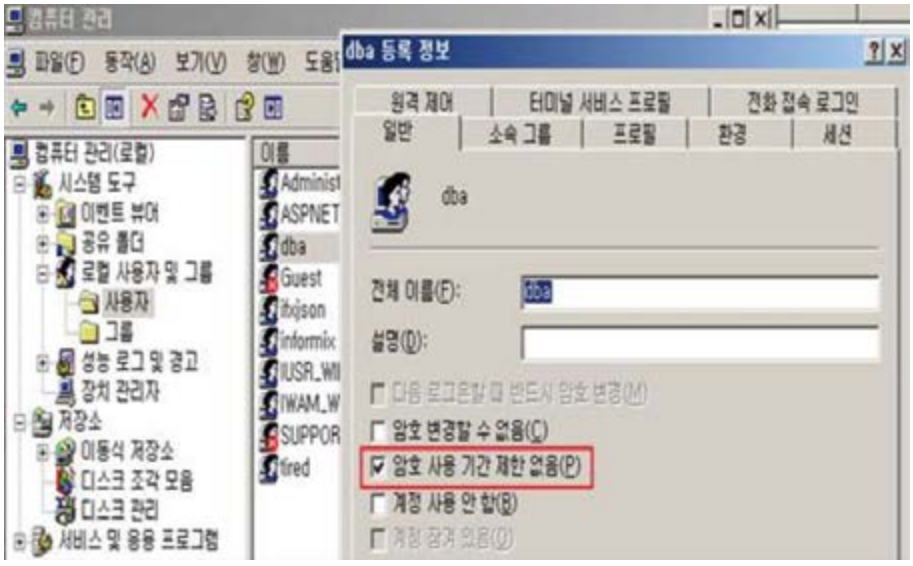
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 계정 정책 > 계정 잠금 정책 > "계정 잠금 임계값" 설정 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd> net accounts /lockoutthreshold:5 명령어 실행
[GUI]
■ 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책
■ "계정 잠금 임계값"을 "5" 이하의 값으로 설정</td></tr>
</table>

	
비고	▪ Administrator 계정은 잠기지 않으며, 일반 계정의 경우 5번 패스워드 입력 실패 시 잠김

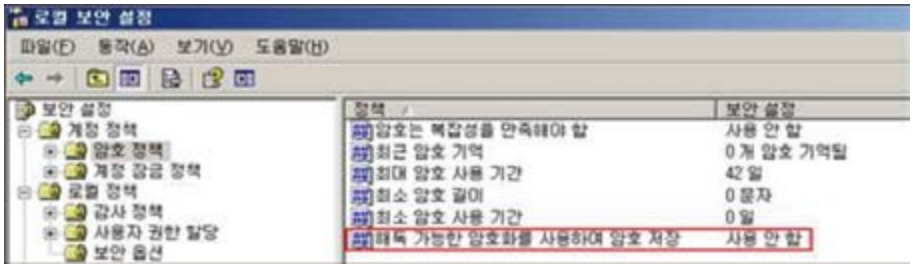
<table>
<tr><td>진단항목</td><td colspan="2">W-05. 패스워드 최대 사용 기간 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">오랫동안 변경하지 않은 패스워드를 지속적으로 사용하는 경우 암호 추측 공격에 의해 유출될 수 있으므로 사용자가 암호를 자주 바꾸도록 하면 유효한 암호가 공격당하는 위험을 줄일 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 최대 사용 기간이 90일 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 최대 사용 기간이 설정되어 있지 않거나 90일 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
- 시작 > 실행 > cmd > secedit /export /cfg /c:₩cfg.txt 명령어 실행
- 탐색기 > c:₩cfg.txt 파일을 열어서 MaximumPasswordAge 설정 값이 90일 이하로 설정되어 있는지 확인
 
1 [Unicode]
2 Unicode=yes
3 [System Access]
4 MinimumPasswordAge = 0
5 MaximumPasswordAge = 42
6 MinimumPasswordLength = 0
7 PasswordComplexity = 0
8 PasswordHistorySize = 0
9 LockoutBadCount = 0
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 계정 정책 > 암호 정책 > "최대 암호 사용 기간" 정책이 90일 이하로 설정되어 있는지 확인
 
로컬 보안 설정
파일(F) 동작(A) 보기(V) 도움말(H)
보안 설정
계정 정책
암호 정책
계정 잠금 정책
로컬 정책
공개 키 정책
소프트웨어 제한 정책
IP 보안 정책(위치: 로컬 컴퓨터)
정책 / 보안 설정
암호는 복잡성을 만족해야 함 사용 안 함
최근 암호 기억 0 개 암호 기억됨
최대 암호 사용 기간 42 일
최소 암호 길이 0 문자
최소 암호 사용 기간 0 일
해독 가능한 암호화를 사용하여 암호 저장 사용 안 함</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd> net accounts /MAXPWAGE:90 명령어 실행
[GUI]
■ 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책
■ "최대 암호 사용 기간"의 다음 이후 암호 만료 기간을 "90일"로 설정</td></tr>
</table>

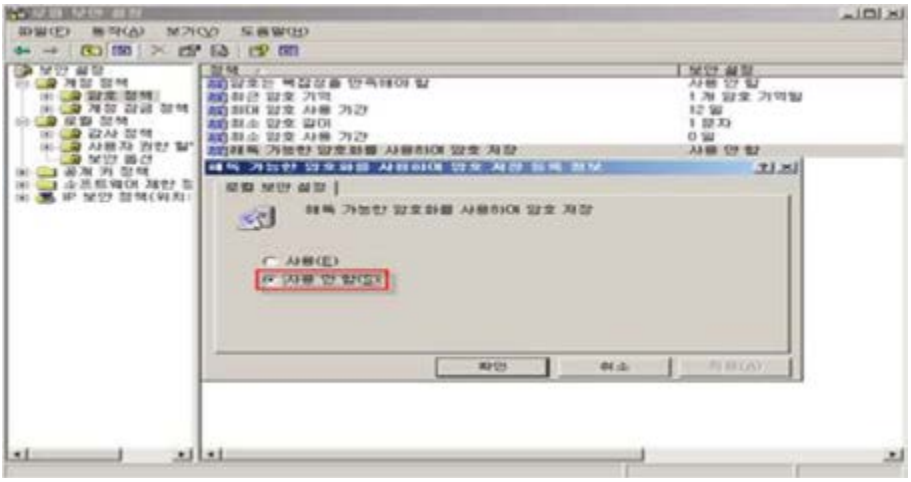
	
비고	■ 암호 사용기간이 90일로 설정되며 90일 주기로 패스워드를 변경하여야 함 ■ 패스워드 사용기간 만료 전 패스워드 변경을 위한 경고 메시지 제공을 권고함

<table>
<tr><td>진단항목</td><td colspan="2">W-06. 암호 사용 기간 제한 없음 제거</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">암호 사용 기간의 제한이 없다면 암호 추측 공격 등의 방법에 의해 유출될 수 있으므로 암호 사용 기간의 제한 없음을 제거해야한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">계정마다 암호 사용 기간 제한 없음 설정이 비활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">계정마다 암호 사용 기간 제한 없음 설정이 활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net user "계정명" 명령어를 입력하여 "암호 만료 날짜" 설정 확인
 

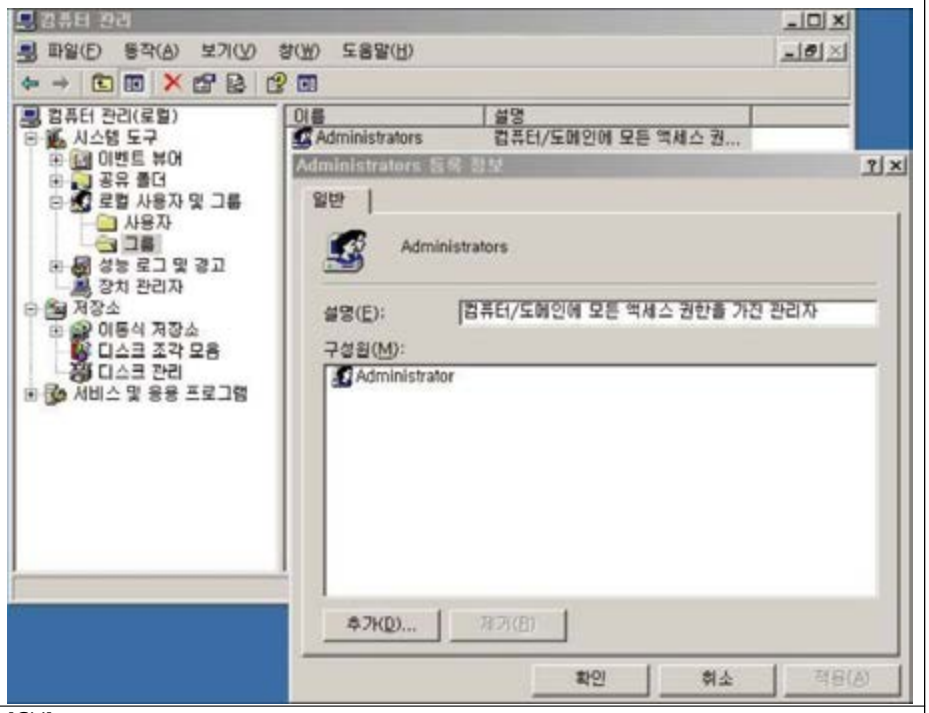
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > 설정할 계정 선택 > 속성에서 "암호 사용 기간 제한 없음"
 
</td></tr>
</table>

조치방법	[CLI] ■ 시작> 실행> cmd> wmic useraccount where name="계정명" set passwordexpires=true 명령어 입력 [GUI] ■ 시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > 설정할 계정 선택 > 속성에서 "암호 사용 기간 제한 없음" 해제 조치
비고	

<table>
<tr><td>진단항목</td><td colspan="2">W-07. 해독 가능한 암호화를 사용하여 암호 저장</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">위 정책이 설정된 경우 OS에서 사용자 ID, PW를 입력받아 인증을 진행하는 응용 프로그램 프로토콜 지원 시 OS는 사용자의 PW를 해독 가능한 방식으로 암호를 저장하기 때문에, 노출된 계정에 대해 공격자가 암호 복호화 공격으로 PW를 획득하여 네트워크 리소스에 접근할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용 안 함"으로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용함"으로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
- 시작 > 실행 > cmd > secedit /export /cfg c:₩cfg.txt 명령어 실행
- 탐색기 > cfg.txt 파일을 열어서 ClearTextPassword 설정 값이 1로 되어 있는지 확인 (0일 경우 양호, 1일 경우 취약)
 
■ 로컬 보안 정책에서 확인방법
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 계정 정책 > 암호 정책 > "해독 가능한 암호화를 사용하여 암호 저장" 설정 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ 시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > 설정할 계정 선택 > 속성에서 "암호 사용 기간 제한 없음" 해제 조치</td></tr>
</table>

	■ 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책 ■ "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정 
비고	

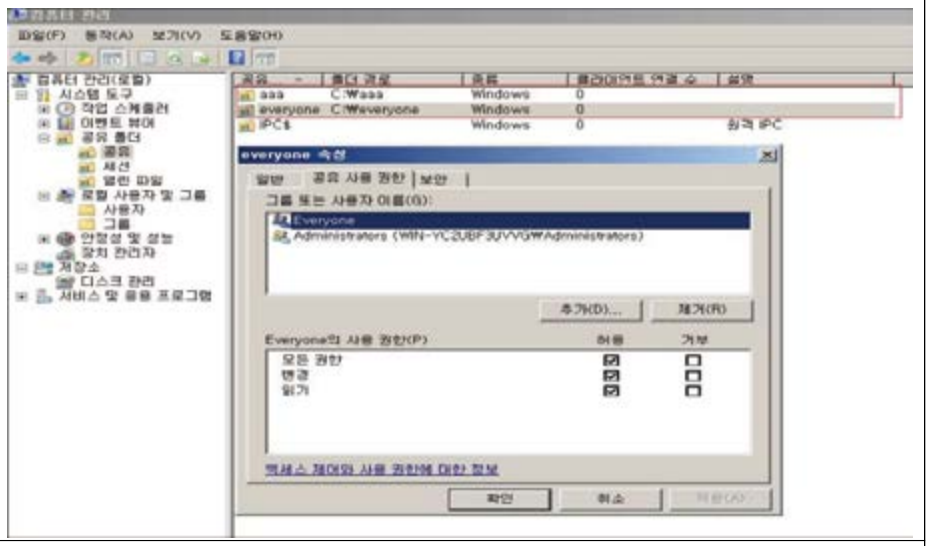
<table>
<tr><td>진단항목</td><td colspan="2">W-08. 관리자 그룹에 최소한의 사용자 포함</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Administrators와 같은 관리자 그룹에 속한 구성원은 컴퓨터 시스템에 대한 완전하고 제한 없는 액세스 권한을 가지므로, 사용자를 관리자 그룹에 포함 시킬 경우 비인가 사용자에 대한 과한 관리 권한이 부여될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Administrators 그룹의 구성원을 1명 이하로 유지하거나, 불필요한 관리자 계정이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Administrators 그룹의 구성원에 불필요한 관리자 계정이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령 프롬프트에서 확인방법
시작> 실행> cmd> net localgroup administrators 명령어 실행

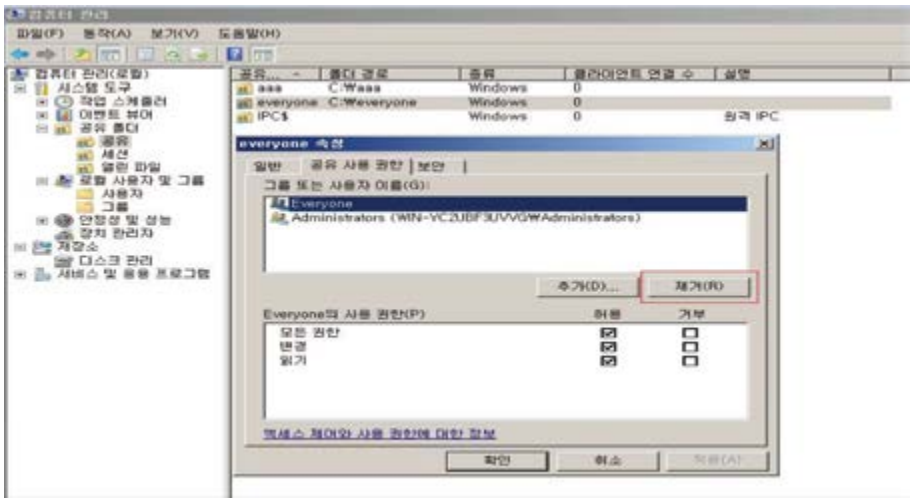
▪ 컴퓨터 관리에서 확인
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 그룹 > Administrators 선택 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
▪ 시작> 실행> cmd> net localgroup administrators 삭제할 계정명 /del 명령어 입력

[GUI]
▪ 시작> 실행> LUSRMGR.MSC> 그룹> Administrators> 속성
▪ Administrators 그룹에서 불필요한 계정 제거 후 그룹 변경</td></tr>
</table>

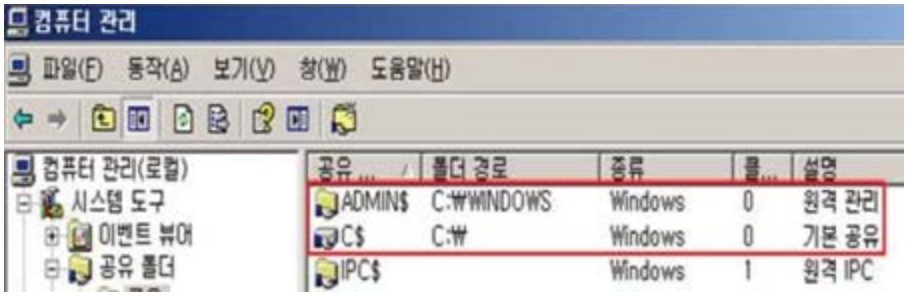
비고	▪ Administrator 그룹에 있는 계정을 잘못 삭제하는 경우 해당 업무에 장애 발생 가능성이 있음

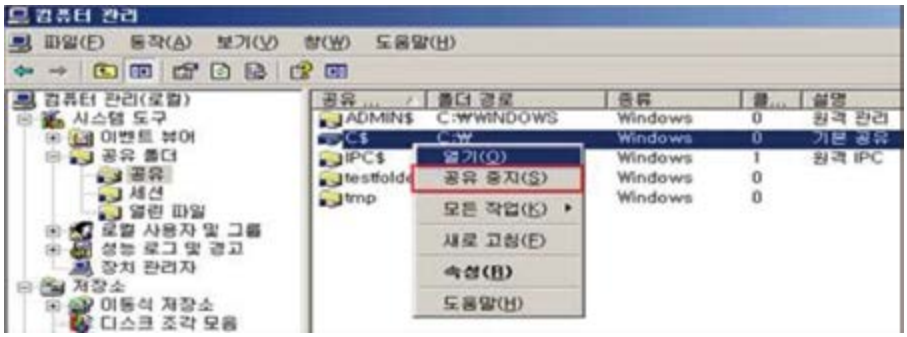
나. 서비스 관리

<table>
<tr><td>진단항목</td><td colspan="2">W-09. 공유 권한 및 사용자 그룹 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Everyone이 공유계정에 포함되어 있으면 익명 사용자의 접근이 가능하여 내부 정보 유출 및 악성코드의 감염 우려가 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">일반 공유 디렉토리가 없거나 공유 디렉토리 접근 권한에 Everyone 권한이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">일반 공유 디렉토리의 접근 권한에 Everyone 권한이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령 프롬프트에서 확인
시작> 실행> cmd> net share 명령어 입력 (C$, D$, Admin$, IPXC$ 등을 제외한 일반 공유폴더가 존재하지 않으면 양호)
▪ 컴퓨터 관리에서 확인
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 공유 폴더 > 공유에서 일반 공유폴더가 존재하는지 확인 (C$, D$, Admin$, IPC$ 등을 제외한 일반 공유폴더가 존재하지 않으면 양호)
위 항목에서 C$, D$, Admin$, IPC$ 등을 제외한 일반 공유폴더가 존재하는 경우, 일반 공유폴더 > 속성 > 보안 탭에서 Everyone으로 된 공유가 존재하는지 확인 (Everyone 공유가 존재하지 않으면 양호)
  </td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
▪ 시작> 실행> FSMGMT.MSC> 공유
▪ 사용 권한에서 Everyone으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가</td></tr>
</table>

	
비고	▪ 애플리케이션이나 Backup 용도로 Everyone 공유를 사용하는 경우 해당 작업에 영향 가능

<table>
<tr><td>진단항목</td><td colspan="2">W-10. 하드디스크 기본 공유 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Windows는 프로그램 및 서비스를 네트워크나 컴퓨터 환경에서 관리하기 위해 시스템 기본 공유 항목을 자동으로 생성한다. 이를 제거하지 않으면 비인가자가 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있으며 이러한 공유 기능의 경로를 이용하여 바이러스가 침투될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">레지스트리의 AutoShareServer(WinNT: AutoShareWks)가 0이며 기본 공유가 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">레지스트리의 AutoShareServer(WinNT: AutoShareWks)가 1이거나 기본 공유가 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net share 명령어 실행 후 기본 공유가 존재하는지 확인
 

■ 컴퓨터 관리에서 확인
시작 > 프로그램 > 관리도구 > 컴퓨터 관리 > 공유 폴더 > 공유에서 기본 공유 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
■ 시작> 실행> cmd > net share 삭제할 공유 이름 /del 명령어 실행
[GUI]
■ 시작> 실행> FSMGMT.MSC> 공유> 기본 공유 선택> 우 클릭> 공유 중지</td></tr>
</table>

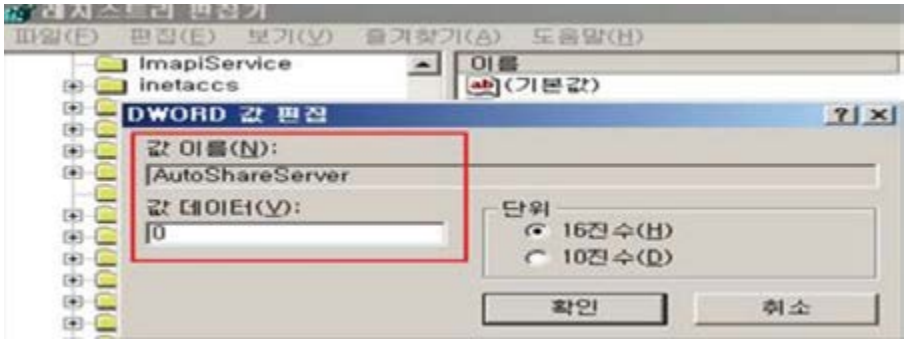


[레지스트리]

■ 시작> 실행> REGEDIT

아래 레지스트리 값을 0으로 수정함 (키 값이 없을 경우 새로 생성함)

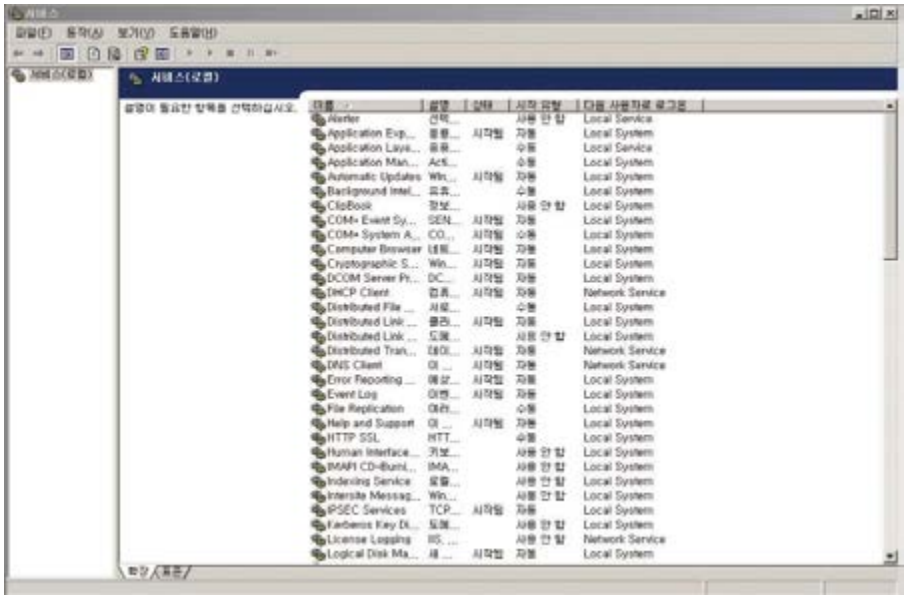
"HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩LanmanServer₩Parameters₩AutoShareServer"(Windows NT일 경우: AutoShareWks)

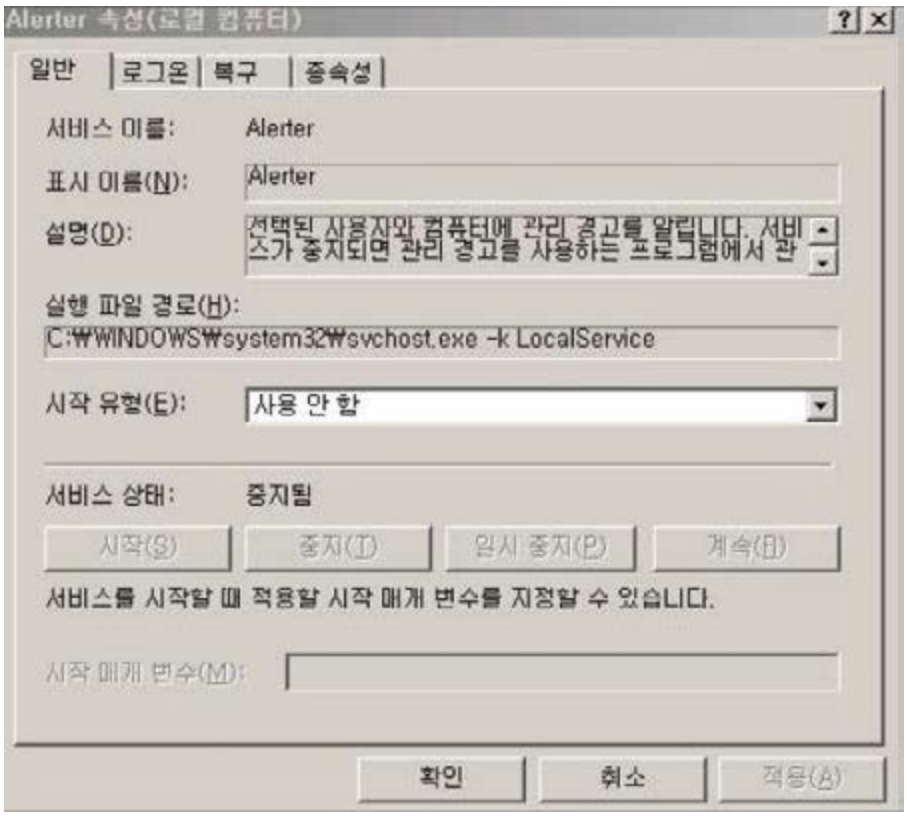


비고

■ Active Directory, Clustered system에서는 적용 시 영향 있음

※ Active Directory: 중앙 집중화된 자원 관리를 위한 계층적 디렉토리 서비스
※ Clustered system: 여러 개의 시스템을 결합하여 사용함

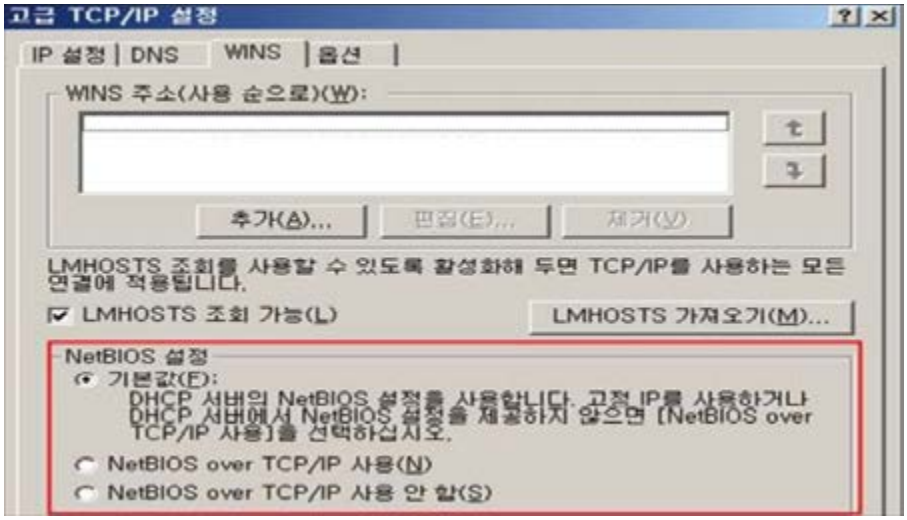
<table>
<tr><td>진단항목</td><td colspan="2">W-11. 불필요한 서비스 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템에 기본적으로 설치되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침입의 가능성이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">일반적으로 불필요한 서비스(아래 목록 참조)가 중지되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 아래 서비스가 중지되어 있는 경우
- Alerter(서버에서 클라이언트로 경고 메시지를 보냄)
- Clipbook(서버 내 Clipbook을 다른 클라이언트와 공유)
- Messenger(net send 명령어를 이용하여 클라이언트에 메시지 보냄)
- Simple TCP/IP Services(Echo, Discard, Character Generator, Daytime, Quote of the Day)
■ 시작 > 관리도구 > 서비스에서 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ 시작> 실행> SERVICES.MSC> "해당 서비스" 선택> 속성
■ 시작 유형 -> 사용 안 함</td></tr>
</table>

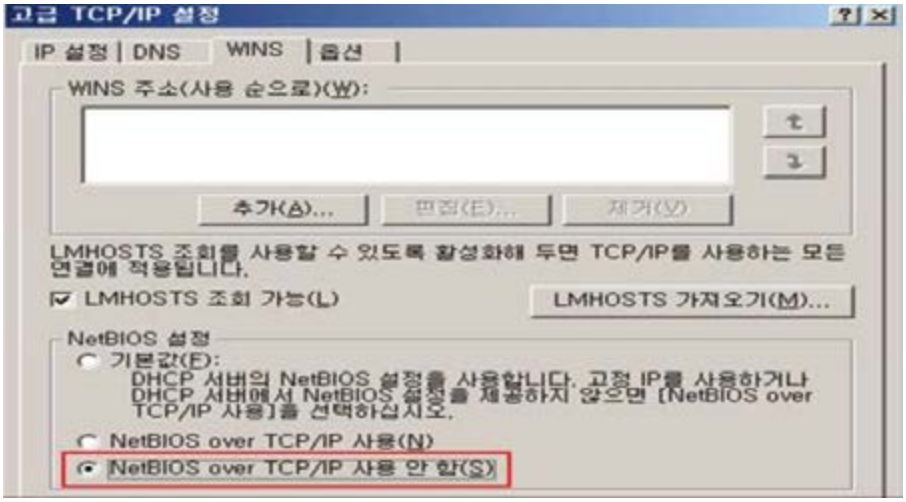


■ 서비스 상태 -> 중지 설정

비고	조치 시 일반적으로 영향 없음

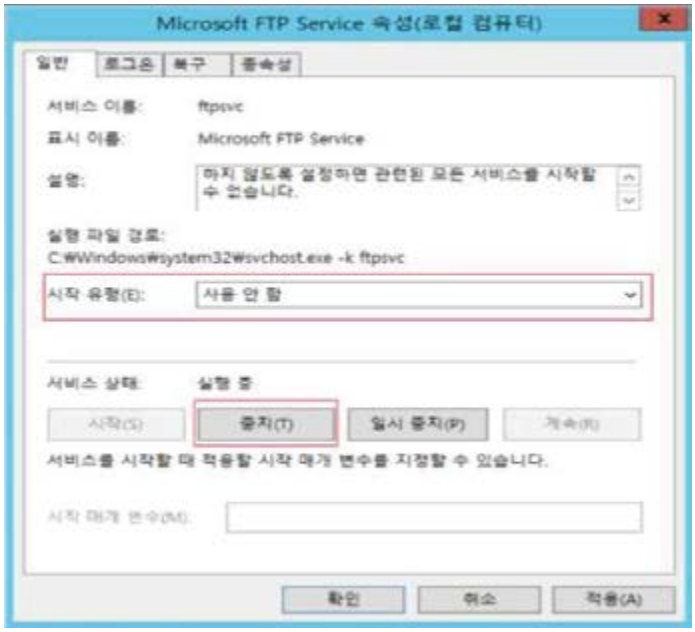
<table>
<tr><td>진단항목</td><td colspan="2">W-12. NetBIOS 바인딩 서비스 구동 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인터넷에 직접 연결되어 있는 윈도우 시스템에서 NetBIOS TCP/IP 바인딩이 활성화되어 있을 경우 공격자가 네트워크 공유자원을 사용할 우려가 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">TCP/IP와 NetBIOS 간의 바인딩이 제거되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">TCP/IP와 NetBIOS 간의 바인딩이 제거되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 레지스트리에서 확인
- 시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩NetBT₩Parameters₩Interfaces
- Interfaces 폴더 마우스 우 클릭 > 찾기 > NetbiosOptions 를 검색하여 해당 데이터 값이 2로 설정되어 있는지 확인 (데이터 값이 2로 설정되어 있을 경우 양호)
 

▪ 네트워크 연결에서 확인
시작 > 실행 > ncpa.cpl > 로컬 영역 연결 > 속성 > TCP/IP > 속성 > 일반 탭 > 고급 > WINS 탭 > NetBIOS 설정에서 NetBIOS를 사용하고 있는지 확인 (설정이 "NetBIOS over TCP/IP 사용 안 함"으로 설정되어 있을 경우 양호)
 
</td></tr>
</table>

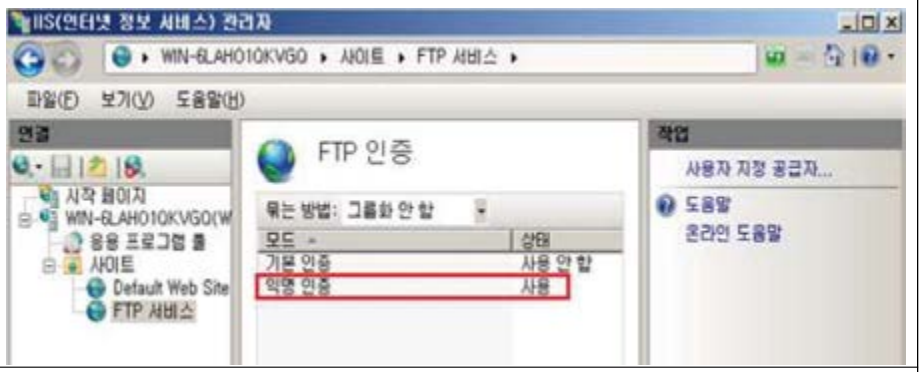
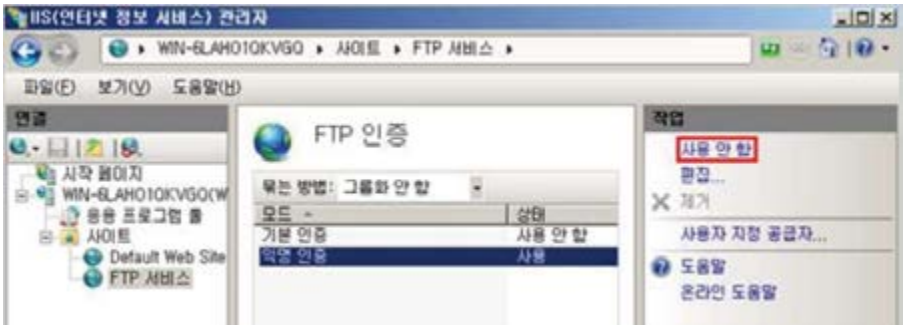
조치방법	[GUI] ■ 시작> 실행> ncpa.cpl> 로컬 영역 연결> 속성> TCP/IP> [일반] 탭에서 [고급] 클릭> [WINS] 탭에서 TCP/IP에서 "NetBIOS 사용 안 함" 또는, "NetBIOS over TCP/IP 사용 안 함" 선택  [레지스트리] ■ 시작> 실행 > regedit >HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet services NetBT Parameters Interfaces에서 NetbiosOptions 데이터 값을 2로 변경 
비고	■ TCP/IP을 거지게 되는 파일 공유 서비스가 제공되지 않음. 인터넷에서의 공유 자원에 대한 접근시도가 불가능함 (라우터를 거치지 않은 내부 네트워크에서는 가능함)

<table>
<tr><td>진단항목</td><td colspan="2">W-13. FTP 서비스 구동 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">OS에서 제공하는 기본적인 FTP 서비스를 사용할 경우 계정과 패스워드가 암호화되지 않은 채로 전송되어 Sniffer에 의한 계정 정보의 노출 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">FTP 서비스가 구동중이지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">FTP 서비스가 구동중일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net start 명령어를 통해 FTP 서비스 구동 확인
 

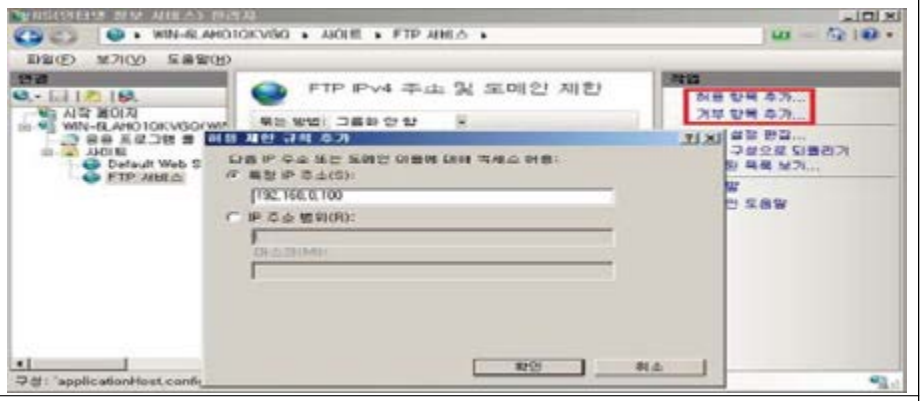
■ 서비스에서 확인
시작 > 프로그램 > 관리도구 > 서비스에서 FTP 서비스 구동 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ 시작> 실행> SERVICES.MSC> FTP Publishing Service> 속성> [일반] 탭에서 " 시작 유형"을 "사용 안 함"으로 설정한 후, FTP 서비스 중지</td></tr>
</table>

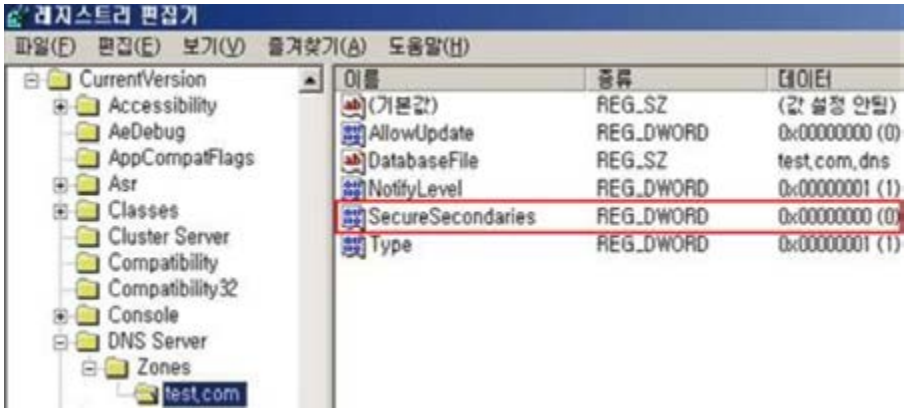
	 Microsoft FTP Service 속성(로컬 컴퓨터) 일반 로그온 복구 종속성 서비스 이름: ftpsvc 표시 이름: Microsoft FTP Service 설명: 실행 파일 경로: C:₩Windows₩system32₩svchost.exe -k ftpsvc 시작 유형(E): 사용 안 함 서비스 상태: 실행 중 시작(S) 중지(T) 일시 중지(P) 계속(R) 서비스를 시작할 때 적용할 시작 매개 변수를 지정할 수 있습니다. 시작 매개 변수(M): 확인 취소 적용(A)
비고	

진단항목	W-14. FTP 디렉토리 접근권한 설정	취약도	상
항목설명	FTP 홈 디렉토리에 과도한 권한(예. Everyone Full Control)이 부여된 경우 임의의 사용자가 쓰기, 수정이 가능하여 정보유출, 파일 위·변조 등의 위험이 존재한다.		
진단기준	양호	FTP 홈 디렉터리에 Everyone 권한이 없는 경우	
	취약	FTP 홈 디렉터리에 Everyone 권한이 있는 경우	
진단방법	■ 인터넷 정보 서비스(IIS) 관리에서 확인 - 시작 > 프로그램 > 관리도구 > 인터넷 정보 서비스(IIS) 관리 > FTP 사이트> 해당 FTP 사이트> 속성> [홈 디렉터리] 탭에서 FTP 홈 디렉터리 확인 - 탐색기> 홈 디렉터리> 속성> [보안] 탭에서 Everyone 권한 확인		
조치방법	■ Windows 2012(IIS 8.0), 2016, 2019 - 시작> 프로그램> 관리도구> 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 해당 FTP 사이트> 기본 설정에서 FTP 홈 디렉터리 확인 - 탐색기> 홈 디렉터리> 속성> [보안] 탭에서 Everyone 권한 제거 ※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)		
비고			

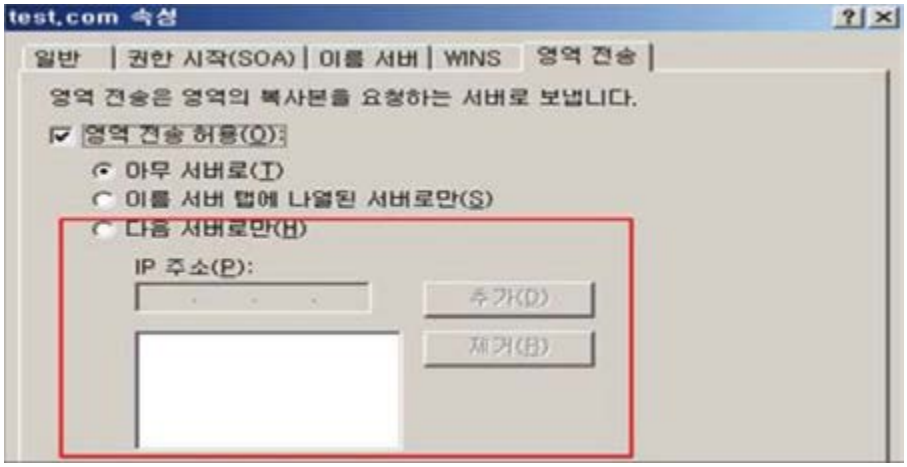
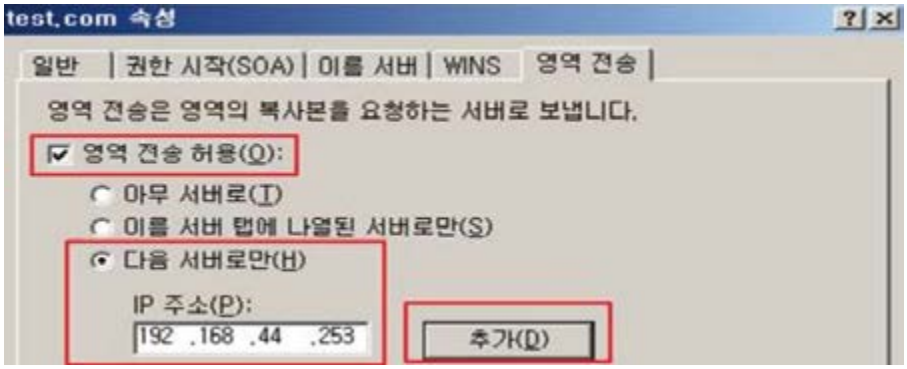
<table>
<tr><td>진단항목</td><td colspan="2">W-15. Anonymous FTP 금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">FTP 익명 접속이 허용된 경우 핵심 기밀 자료나 내부 정보의 불법 유출 가능성이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">FTP를 사용하지 않거나 "익명 연결 허용"이 체크되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">FTP를 사용하면서 "익명 연결 허용"이 체크되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 인터넷 정보 서비스(IIS) 관리에서 확인
시작 > 프로그램 > 관리도구 > IIS(인터넷 정보 서비스) 관리자 > 사용 중인 FTP 서비스 > FTP 인증에서 "익명 인증"이 "사용 안 함"으로 되어있는지 확인 (익명 인증이 "사용 안 함"으로 되어 있으면 양호)
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
▪ Windows 2012(IIS 8.0), 2016(IIS 10.0), 2019(IIS 10.0)
- 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 마우스 우클릭> FTP 게시 추가
- 이후 진행 과정에서 인증 화면의 익명 체크 박스 해제
 

※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)</td></tr>
<tr><td>비고</td><td colspan="4">▪ 애플리케이션에서 익명 연결을 사용할 경우를 제외하고, 조치 시 일반적으로 영향 없음</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">W-16. FTP 접근 제어 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">FTP 프로토콜은 로그온에 지정된 자격 증명이나 데이터 자제가 암호화되지 않고 모든 자격 증명을 일반 텍스트로 네트워크를 통해 전송되는 특성상 서버 클라이언트 간 트래픽 스니핑을 통해 인증정보가 쉽게 노출되므로 접속 허용된 사용자 IP를 지정하여 접속자를 제한할 것을 권고한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">FTP 서비스에 접근 가능한 IP 제한 설정을 적용한 경우</td></tr>
<tr><td>취약</td><td colspan="3">FTP 서비스에 접근 가능한 IP 제한 설정을 적용하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 인터넷 정보 서비스(IIS) 관리에서 확인
시작 > 프로그램 > 관리도구 > IIS(인터넷 정보 서비스) 관리자 > 사용중인 FTP 사이트 > FTP IPv4 주소 및 도메인 제한에서 허용 및 거부 IP 설정 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Windows 2012(IIS 8.0), 2016(IIS 10.0), 2019(IIS 10.0)
- 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> FTP IPv4 주소 및 도메인 제한
- [작업]의 허용 항목 추가에서 FTP 접속을 허용할 IP 입력
- [작업]의 기능 설정 편집에서 지정되지 않은 클라이언트에 대한 액세스를 거부 선택
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">W-17. DNS Zone Transfer 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">DNS Zone Transfer 차단 설정이 적용되지 않은 경우 DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS 서버가 아닌 외부로 유출 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DNS 서비스를 사용하지 않거나, Zone Transfer(영역 전송) 허용을 하지 않거나, 특정 서버로만 허용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DNS 서비스를 사용하거나, Zone Transfer(영역 전송) 허용을 하거나, 특정 서버로만 허용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩ SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩DNS Server₩Zones₩ 운영중인 DNS 영역에서 SecureSecondaries 값이 2로 설정되어 있는지 확인 (해당 값이 2일 경우 양호)
 

■ DNS 관리자에서 확인
시작 > 프로그램 > 관리도구 > DNS > 정방향 조회 영역 > 사용 중인 DNS > 속성 > 영역 전송에서 특정 서버로만 영역 전송이 이루어지도록 되어있는지 확인 ("영역 전송 허용" 설정이 제한되어 있거나, 허용 시, "다음 서버로만"으로 설정되어 있을 경우 양호)</td></tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>조치방법</td><td>[GUI]
■ Windows 2012(IIS 8.0), 2016(IIS 10.0), 2019(IIS 10.0)
- 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 영역 전송
- "다음 서버로만" 선택 후 전송할 서버 IP 추가
- 불필요 시 해당 서비스 제거
시작> 실행> SERVICES.MSC> DNS 서버> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, DNS 서비스 중지
 
</td></tr>
<tr><td>비고</td><td>■ 영역 전송할 경우 서버를 지정해 주면 조치 시 영향 없음</td></tr>
</table>

진단항목	W-18. RDS(RemoteDataServices) 제거	취약도	상
항목설명	DNS Zone Transfer 차단 설정이 적용되지 않은 경우 DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS 서버가 아닌 외부로 유출 위험이 존재한다.		
진단기준	양호	다음 중 한 가지라도 해당되는 경우(2008 이상 양호) - IIS를 사용하지 않는 경우 - Windows 2000 서비스 팩 4, Windows 2003 서비스 팩 2 이상 설치되어 있는 경우 - 디폴트 웹 사이트에 MSADC 가상 디렉터리가 존재하지 않는 경우 - 해당 레지스트리 값이 존재하지 않는 경우	
	취약	양호 기준에 한 가지라도 해당되지 않는 경우	
진단방법	■ Windows 2008 이후는 해당 항목에 대해 패치가 적용되어 있으므로 양호함		
조치방법	■ Windows NT, 2000, 2003 < RDS 제거 방법 > 1) 웹 사이트로부터 "/msadc" 가상 디렉토리 제거 시작> 실행> INETMGR> 웹 사이트 선택 후 오른쪽 디렉토리에서 msadc 제거 2) 다음의 레지스트리 키/디렉토리 제거 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVCWParameters₩ADCLaunch₩RDSServer.DataFactory HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVCWParameters₩ADCLaunch₩AdvancedDataFactory HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVCWParameters₩ADCLaunch₩VbBusObJ.VbBusObJCls		
비고	■ WAS와 연동될 경우 일부 RDS를 사용하는 경우가 있으며 사용할 경우 레지스트리 키 값 제거		

다. 패치 및 로그관리

<table>
<tr><td>진단항목</td><td colspan="2">W-19. 최신 서비스 팩 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">보안 업데이트를 적용하지 않은 경우 시스템 및 응용프로그램의 취약성으로 인해 권한 상승, 원격 코드 실행, 보안 기능 우회 등의 문제를 일으킬 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 서비스 팩이 설치되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 서비스 팩이 설치되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ winver명령어를 통해서 확인
시작 > 실행 > winver 명령어를 실행하여 버전 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 시작> 실행> Winver
▪ 서비스 팩 버전 확인 후 최신 버전이 아닌 경우 아래 사이트에서 최신 서비스 팩 다운로드 후 설치 또는 자동업데이트 활용
https://docs.microsoft.com/ko-kr/windows-server/
※ 인터넷 웜(Worm)이 Windows의 취약점을 이용하여 공격하기 때문에 서비스 팩 설치 시에는 네트워크와 분리된 상태에서 설치할 것을 권장</td></tr>
<tr><td>비고</td><td colspan="4">▪ 설치 후 시스템 재시작이 필요하며 설치에 따른 영향 정도를 확인해야 함</td></tr>
</table>

진단항목	W-20. 최신 HOT FIX 적용		취약도	상
항목설명	최신 Hot Fix가 즉시 적용되지 않은 경우 알려진 취약성으로 인한 시스템 공격 가능성이 존재한다.			
진단기준	양호	최신(1개월 이내) Hot Fix가 설치되어 있을 경우		
	취약	최신(1개월 이내) Hot Fix가 설치되어 있지 않을 경우		
진단방법	▪ 프로그램 추가/제거에서 확인 시작 > 설정 > 제어판 > 프로그램 추가/제거 > 업데이트 표시 > 보안 패치 업데이트 날짜 확인			
조치방법	▪ < 수동 HOT FIX 적용 > 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치함 https://technet.microsoft.com/ko-kr/security/ ▪ < 자동 HOT FIX 적용 > Windows 자동 업데이트 기능을 이용한 설치 제어판> windows update ▪ < PMS(Patch Management System) > Agent를 설치하여 자동으로 업데이트 되도록 설정함 ※ 주의: 보안 패치 및 Hot Fix 경우 적용 후 시스템 재시작을 요하는 경우가 대부분이므로 관리자는 서비스에 지장이 없는 시간대에 적용할 것을 권장함. 일부 Hot Fix는 수행되고 있는 OS 프로그램이나 개발용 Application 프로그램에 영향을 줄 수 있으므로 패치 적용 전 Application 프로그램을 구분하고, 필요하다면 OS 벤더 또는, Application 엔지니어에게 확인 작업을 거친 후 패치를 수행하여야 함.			
비고	▪ 설치 후 시스템 재시작이 필요한 경우가 존재하며 설치에 따른 영향도가 필요함			

<table>
<tr><td>진단항목</td><td colspan="2">W-21. 백신 프로그램 업데이트</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">백신이 지속적, 주기적으로 업데이트되지 않은 경우 계속되는 신종 바이러스의 출현으로 인한 시스템 공격의 우려가 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립된 경우</td></tr>
<tr><td>취약</td><td colspan="3">바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립되지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 백신 엔진에서 확인
바이러스 백신 프로그램의 최신 엔진 업데이트 설치 유무를 수동으로 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 긴급한 경우 수시로 업데이트 진행
(백신 종류마다 다소 차이는 있으나 매주 업데이트가 진행됨)
▪ 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신 사에서 발표하는 경보 주시
▪ 백신 프로그램의 자동 업데이트 기능을 이용하면 온라인을 통해 변동 사항을 자동으로 업데이트하여 알 수 있음

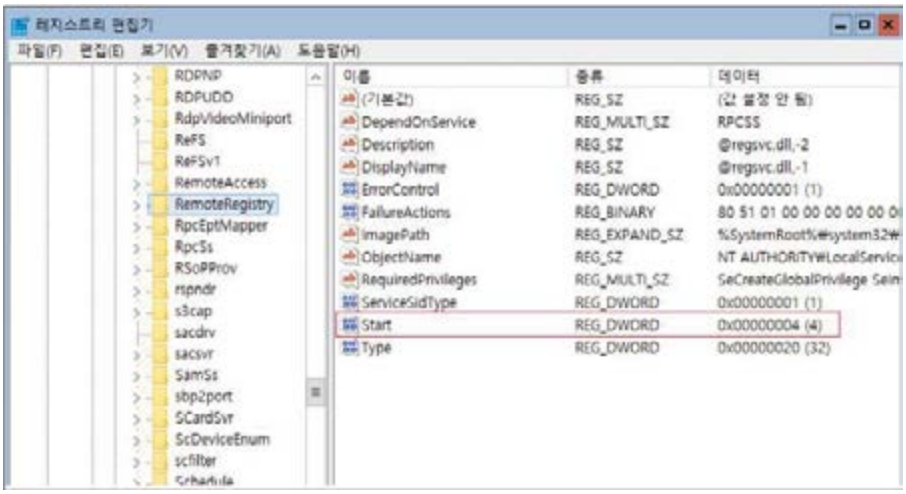
※ 기타 기관에서 사용중인 백신의 환경설정에서 업데이트 기능 활성화 여부 확인</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	W-22. 로그의 정기적 검토 및 보고	취약도	상
항목설명	로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어렵다.		
진단기준	양호	로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우	
	취약	로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지지 않는 경우	
진단방법	▪ 담당자와의 인터뷰 및 증적을 통해서 확인 로그 기록에 대한 정기적 검토 및 분석 증적, 보고서 확인		
조치방법	▪ 로그 기록에 대한 정기적 검토 및 분석 실시 1) 시작> 제어판> 관리 도구> 이벤트 뷰어 2) 응용 프로그램 로그, 보안 로그, 시스템 로그 분석 ※ OS 구성에 따라 디렉토리 서비스 로그, 파일 복제 서비스 로그, DNS 서버 로그 등 분석 ▪ 로그 분석 결과에 대한 일일, 월간 보고서 작성 및 보고		
비고	▪ 로컬 보안 정책 감사 설정의 기본 값		

정책	서버 버전 기본 값	데스크탑 버전 기본 값
개체 액세스 감사	감사 안함	감사 안함
계정 관리 감사	사용자 계정 관리 : 성공 컴퓨터 계정 관리 : 성공 보안 그룹 관리 : 성공	사용자 계정 관리 : 성공 보안 그룹 관리 : 성공
계정 로그온 이벤트 감사	Kerberos 서비스 티켓 작업 : 성공 Kerberos 인증 서비스 : 성공	감사 안함
권한 사용 감사	감사 안함	감사 안함
디렉터리 서비스 액세스 감사	디렉터리 서비스 액세스 : 성공 로그온 : 성공, 실패 로그오프 : 성공	로그온 : 성공 로그오프 : 성공
로그온 이벤트 감사	계정 잠금 : 성공 특수 로그온 : 성공 네트워크 정책 서버 : 성공, 실패 보안 상태 변경 : 성공	계정 잠금 : 성공 특수 로그온 : 성공 네트워크 정책 서버 : 성공, 실패 보안 상태 변경 : 성공
시스템 이벤트 감사	시스템 무결성 : 성공, 실패 기타 시스템 이벤트 : 성공, 실패	시스템 무결성 :성공, 실패 기타 시스템 이벤트 : 성공, 실패
정책 변경 감사	감사 정책 변경 : 성공 인증 정책 변경 : 성공	감사 정책 변경 : 성공 인증 정책 변경 : 성공
프로세스 추적 감사	감사 안함	감사 안함

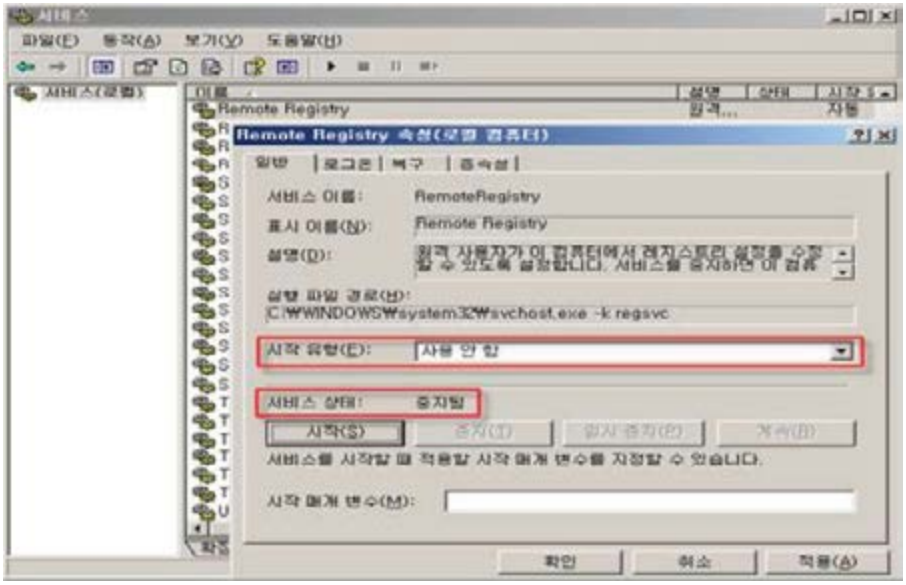
<table>
<tr><td>진단항목</td><td colspan="2">W-23. 원격으로 엑세스할 수 있는 레지스트리 경로</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Windows에 의해 사용되는 모든 초기화와 환경설정 정보는 레지스트리에 저장되므로 레지스트리에 대한 철저한 보안이 요구된다. 레지스트리 편집기는 원격접속으로도 그 키를 바꿀 수 있는데 이는 대단히 위험한 것으로 네트워크를 통한 레지스트리 접속을 차단해야 한다. 원격에서 레지스트리로 접근을 위해서는 관리자의 권한 또는 원격에서 접근을 위한 특별한 계정이 필요하다. 윈도우에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는데 이 서비스를 중지시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Remote Registry Service가 중지되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Remote Registry Service가 사용 중인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령 프롬프트에서 확인방법
시작 > 실행 > cmd > net start 명령어를 실행하여 원격 레지스트리 서비스가 구동 중인지 확인
 

▪ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩RemoteRegistry 에서 Start 값이 4로 되어 있는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 레지스트리에서 변경
시작> 실행> SERVICES.MSC> Remote Registry> 속성
시작 유형을 사용 안 함으로 설정하고 서비스를 중지</td></tr>
</table>



■ 서비스에서 변경

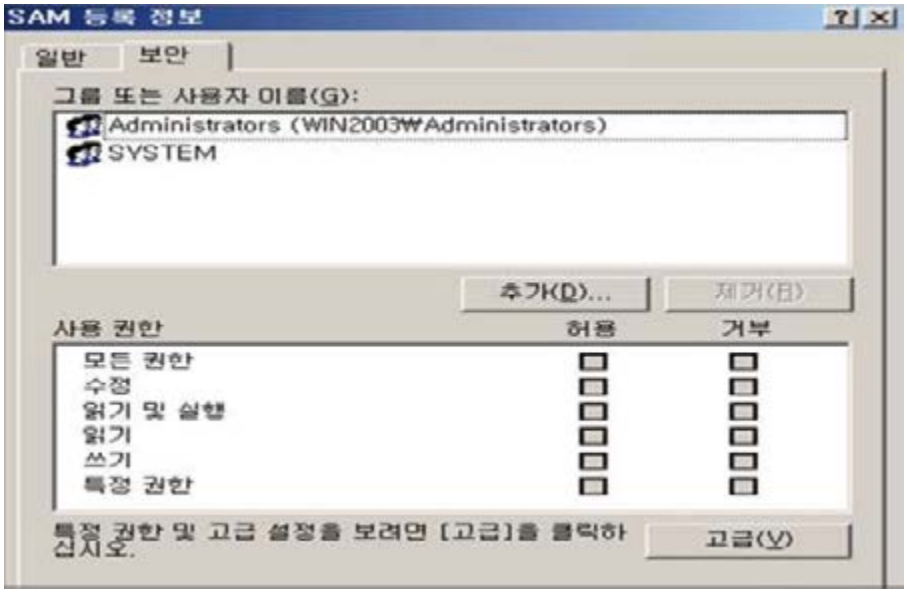
시작 > 프로그램 > 관리도구 > 서비스 > Remote Registry > 속성에서 시작 유형을 "사용 안 함"으로 설정하고, 서비스를 중지

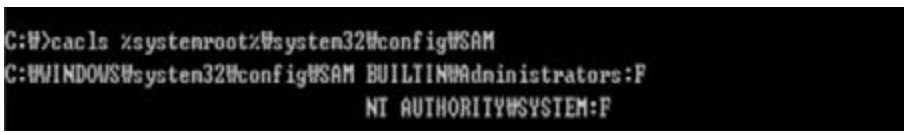


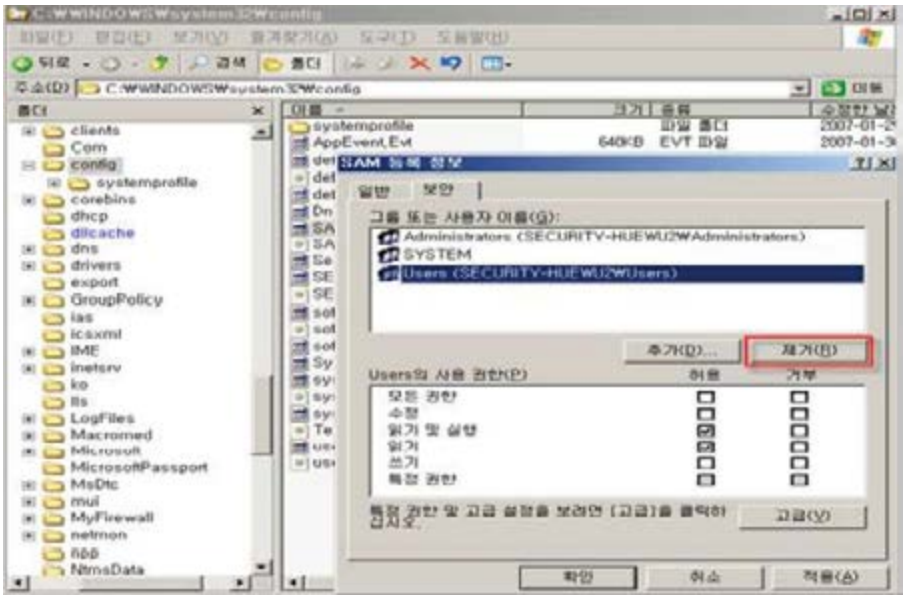
비고	■ Remote Registry Service를 사용하는지 확인 필요 (서비스> Remote Registry Service> 등록 정보> 종속성 참고)

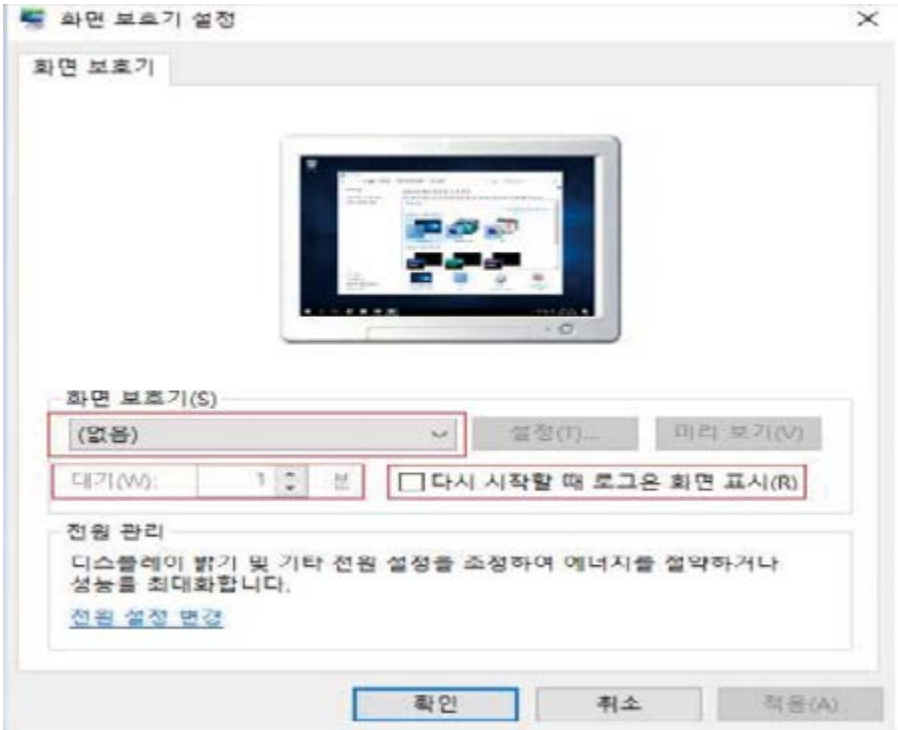
라. 보안 관리

진단항목	W-24. 백신 프로그램 설치		취약도	상
항목설명	백신 프로그램이 설치되지 않은 경우 웜, 트로이목마 등의 악성 바이러스로 인한 시스템 피해 위험이 있다.			
진단기준	양호	바이러스 백신 프로그램이 설치되어 있는 경우		
	취약	바이러스 백신 프로그램이 설치되어 있지 않은 경우		
진단방법	■ 백신엔진을 통해서 확인 - 바이러스 백신 프로그램 설치 여부 - 실시간 감시 기능 설정 여부 - 최신 Update 여부			
조치방법	■ 백신 설치			
비고				

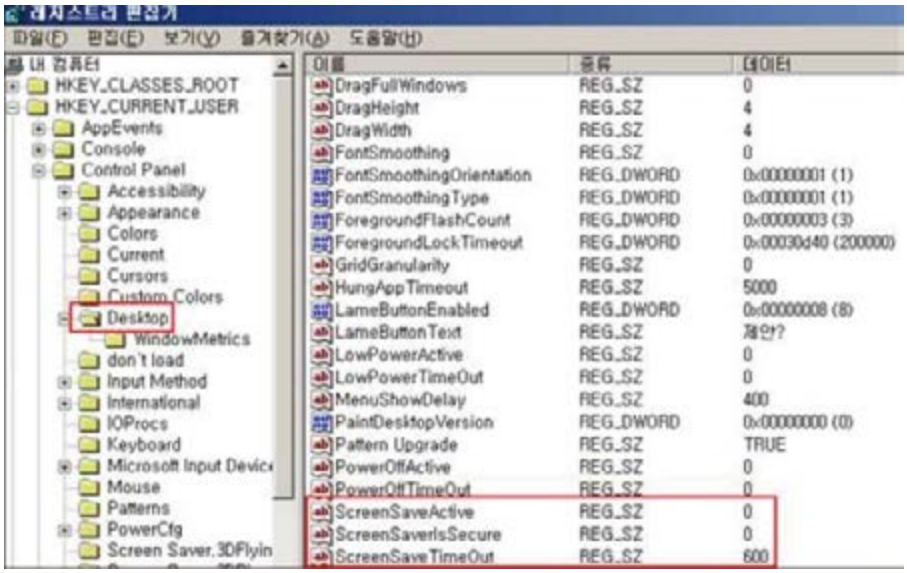
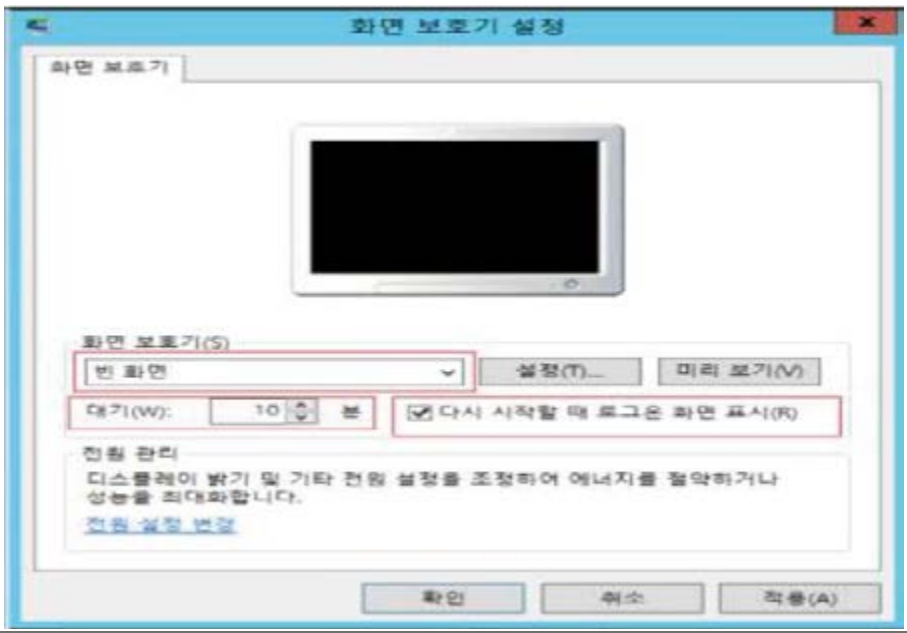
<table>
<tr><td>진단항목</td><td colspan="2">W-25. SAM 파일 접근 통제 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SAM 파일이 노출될 경우 패스워드 공격 시도로 인해 계정 및 패스워드 데이터베이스 정보가 탈취될 우려가 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SAM 파일 접근권한에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 탐색기에서 확인
탐색기 > C:₩Windows₩system32₩config₩SAM > 속성 > 보안 탭에서 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인
 

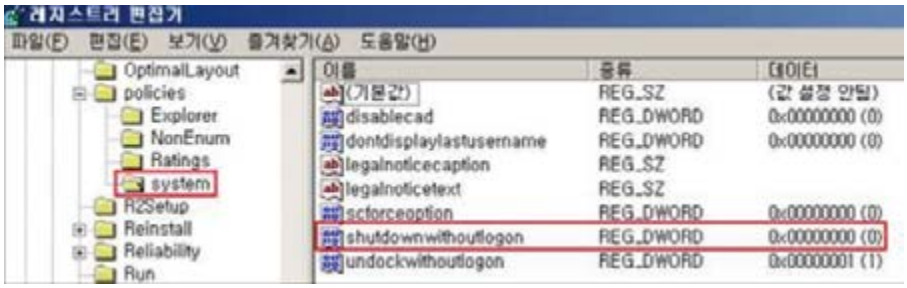
▪ 명령 프롬프트에서 확인
시작 > 실행 > cmd > cacls %systemroot%₩system32₩config₩SAM 명령어를 통해 SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 등록되어 있는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[CLI]
▪ [Win2012, Win2016, Win2019]
- 시작> 실행> cmd> cals %systemroot%₩system32₩config₩SAM> 속성> 보안</td></tr>
</table>

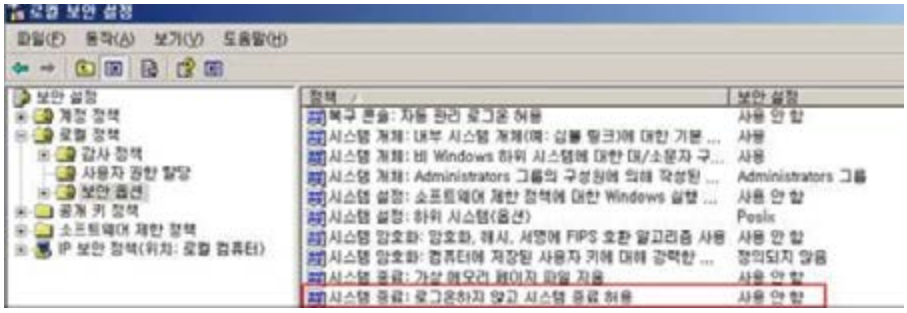
	▪ Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거 [GUI] 
비고	

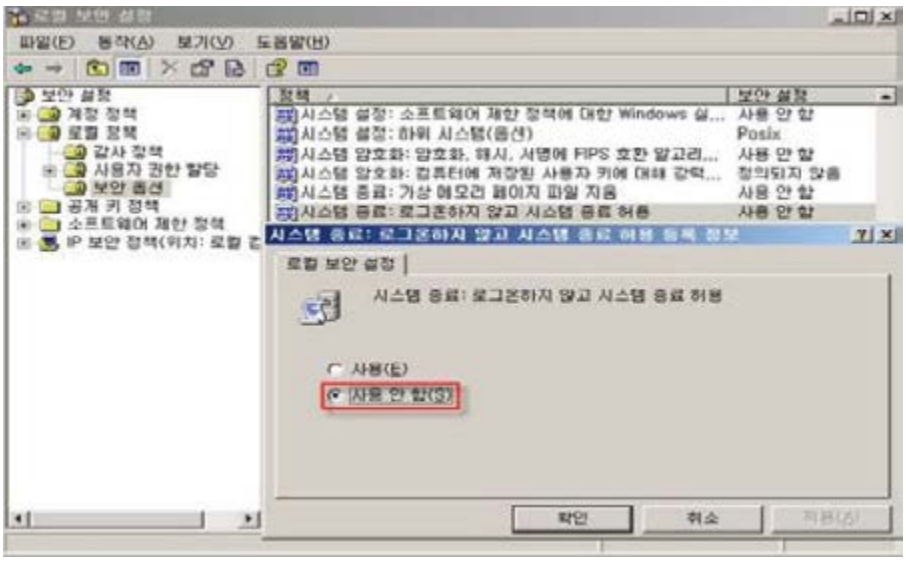
<table>
<tr><td>진단항목</td><td colspan="2">W-26. 화면보호기 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">화면보호기 설정을 하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">화면 보호기를 설정하고 대기 시간이 10분 이하의 값으로 설정되어 있으며, 화면 보호기 해제를 위한 암호를 사용하는 경우</td></tr>
<tr><td>취약</td><td colspan="3">화면 보호기가 설정되지 않았거나 암호를 사용하지 않은 경우 또는, 화면 보호기 대기 시간이 10분을 초과 한 값으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 디스플레이에서 확인
시작 > 제어판 > 디스플레이 > 화면보호기 탭에서 아래 항목의 설정 여부 확인
- 화면 보호기 : 없음 이외의 값으로 설정되어 있을 경우 양호
- 대기 시간 : 10분
- 다시 시작할 때 암호로 보호 기능 사용 체크 여부
 

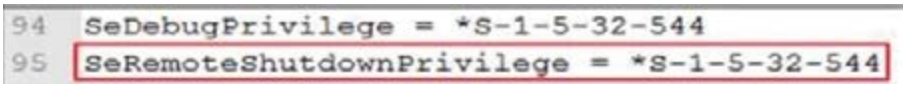
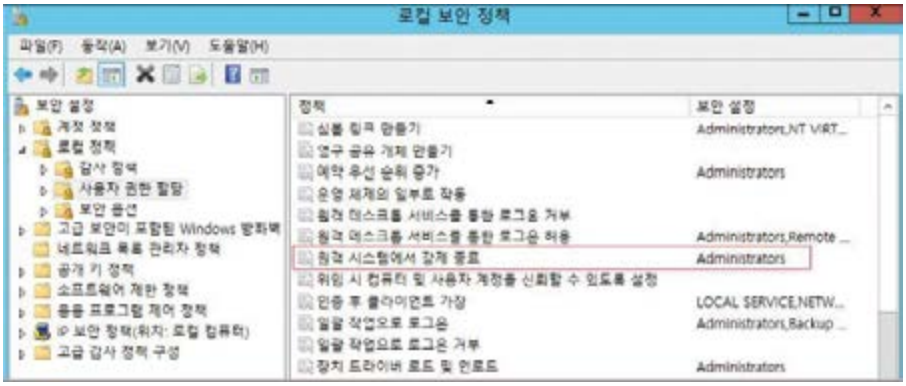
■ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_CURRENT_USER₩Control Panel₩Desktop 에서 아래와 같이 설정되어 있는지 확인
- ScreenSaveActive = 1 (화면보호기 활성화, 1이면 양호)
- ScreenSavelsSecure = 1 (재시작 시 암호로 보호, 1이면 양호)</td></tr>
</table>

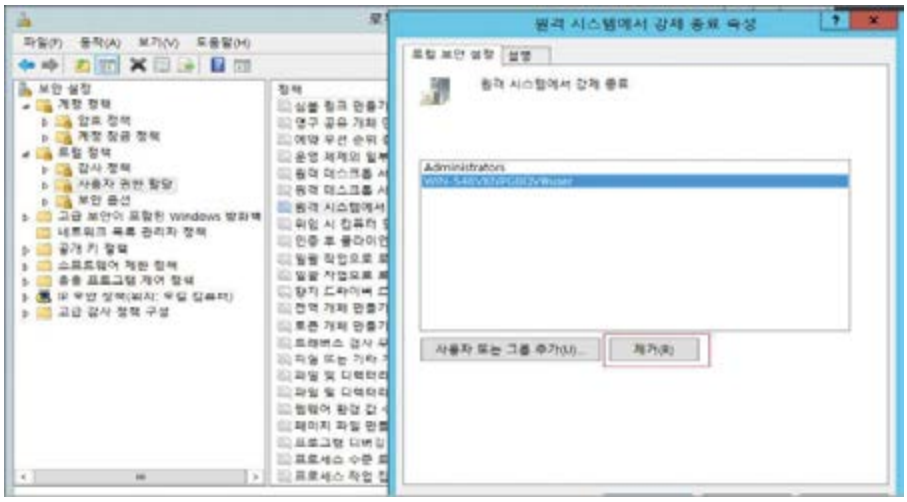
	- ScreenSaveTimeOut = 300 (대기 시간 설정, 초단위) 
조치방법	■ Windows 2012, 2016, 2019 제어판> 디스플레이> 화면보호기 변경> "다시 시작할 때 로그온 화면 표시" 체크, "대기 시간" 10분 설정 
비고	

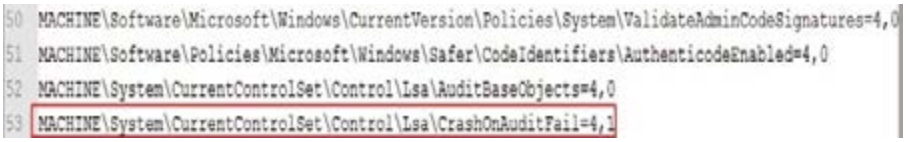
<table>
<tr><td>진단항목</td><td colspan="2">W-27. 로그온하지 않고 시스템 종료 허용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">로그온 창에 "시스템 종료" 버튼이 활성화되어 있으면 로그인을 하지 않고도 불법적인 시스템 종료가 가능하여 정상적인 서비스 운영에 영향을 준다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"로그온 하지 않고 시스템 종료 허용"이 "사용 안 함"으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"로그온 하지 않고 시스템 종료 허용"이 "사용"으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩system에서 ShutdownWithoutLogon 값이 "0" (사용안함) 으로 설정되어 있는지 확인 (값이 0으로 설정되어 있는 경우 양호)
 

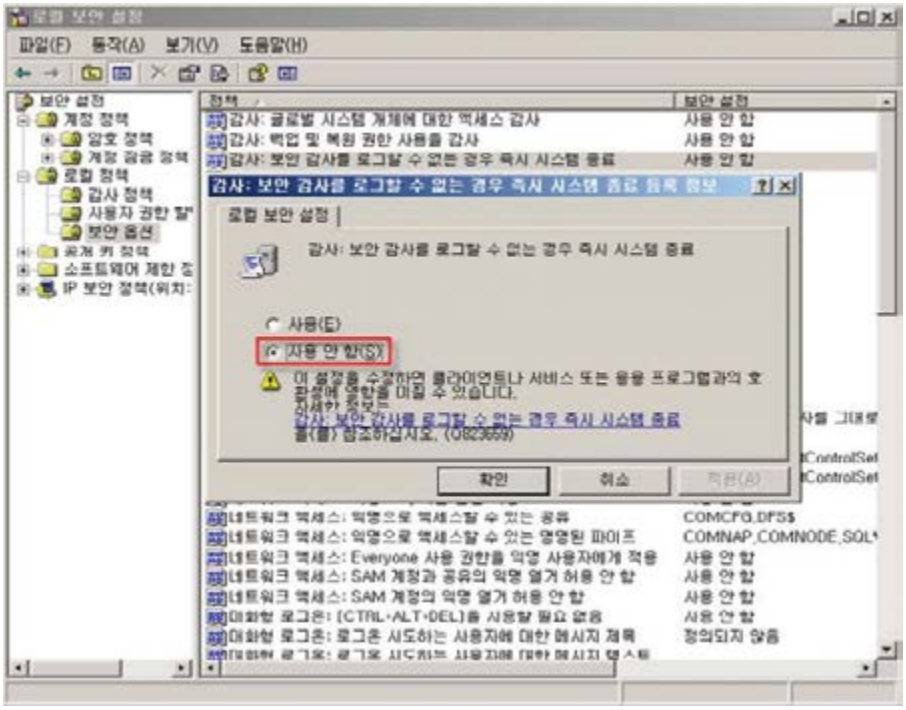
■ 로컬 보안 정책에서 확인
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > "시스템 종료 : 로그온하지 않고 시스템 종료 허용"
정책이 "사용 안 함"으로 되어 있는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ Windows 2012, 2016, 2019
1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2) "시스템 종료: 로그온 하지 않고 시스템 종료 허용"을 "사용 안 함"으로 설정</td></tr>
</table>

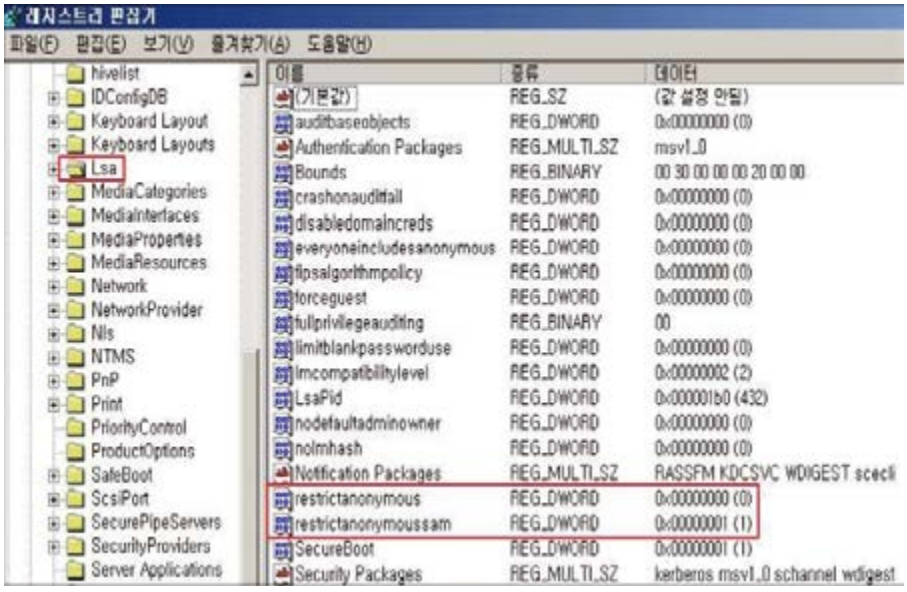
	 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 계정 정책 로컬 정책 감사 정책 사용자 권한 할당 보안 옵션 공개 키 정책 소프트웨어 제한 정책 정책 보안 설정 시스템 설정: 소프트웨어 제한 정책에 대한 Windows 실... 사용 안 함 시스템 설정: 하위 시스템(옵션) Posix 시스템 암호화: 암호화, 해시, 서명에 FIPS 호환 알고리... 사용 안 함 시스템 암호화: 컴퓨터에 저장된 사용자 키에 대해 강력... 정의되지 않음 시스템 종료: 가상 메모리 페이지 파일 지움 사용 안 함 시스템 종료: 로그온하지 않고 시스템 종료 허용 사용 안 함 로컬 보안 설정 시스템 종료: 로그온하지 않고 시스템 종료 허용 사용(E) 사용 안 함(D) 확인 취소
비고	

<table>
<tr><td>진단항목</td><td colspan="2">W-28. 원격 시스템에서 강제로 시스템 종료</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">원격 시스템 강제 종료 설정이 부적절한 경우 서비스 거부 공격 등에 악용될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">“원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators"만 존재하는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 외 다른 계정 및 그룹이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인
- 시작 > 실행 > cmd.exe > secedit /export /cfg c:₩cfg.txt 명령어 실행
- 탐색기 > cfg.txt 파일을 열어서 SeRemoteShutdownPrivilege 설정 값에 S-1-5-32-544만 적용되어 있는지 확인
 
94 SeDebugPrivilege = *S-1-5-32-544
95 SeRemoteShutdownPrivilege = *S-1-5-32-544
■ 로컬 보안 정책에서 확인
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 사용자 권한 할당 > “원격 시스템에서 강제로 시스템 종료” 정책에 “Administrators” 그룹만 존재하는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ [Win2012, Win2016, Win2019]
- 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당
- "원격 시스템에서 강제로 시스템 종료" 정책에 Administrators 외 다른 계정 및 그룹 제거</td></tr>
</table>

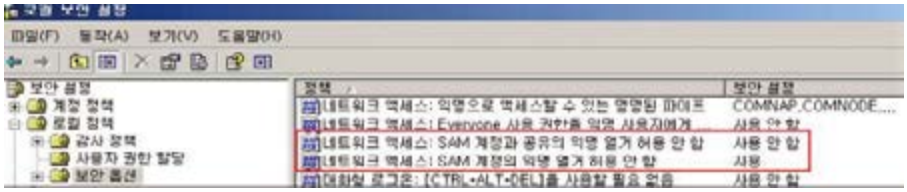
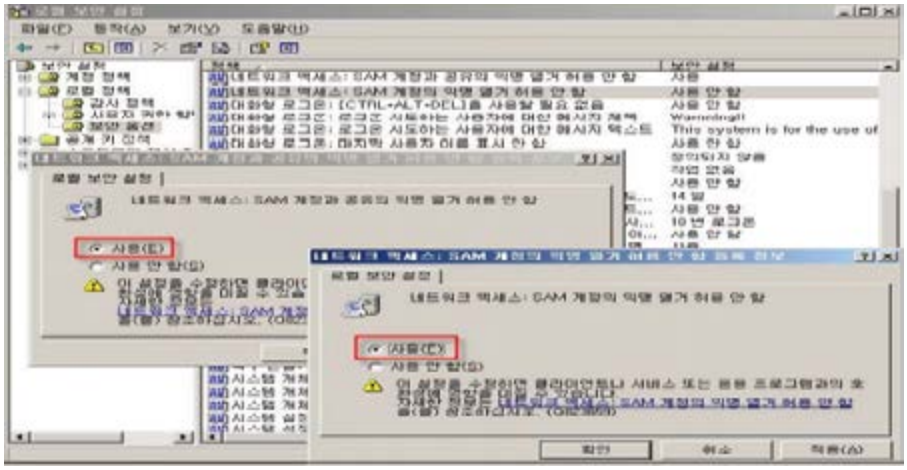
	 원격 시스템에서 강제 종료 속성 로컬 보안 설정 설명 원격 시스템에서 강제 종료 Administrators 사용자 또는 그룹 추가(U)... 제거(R)
비고	

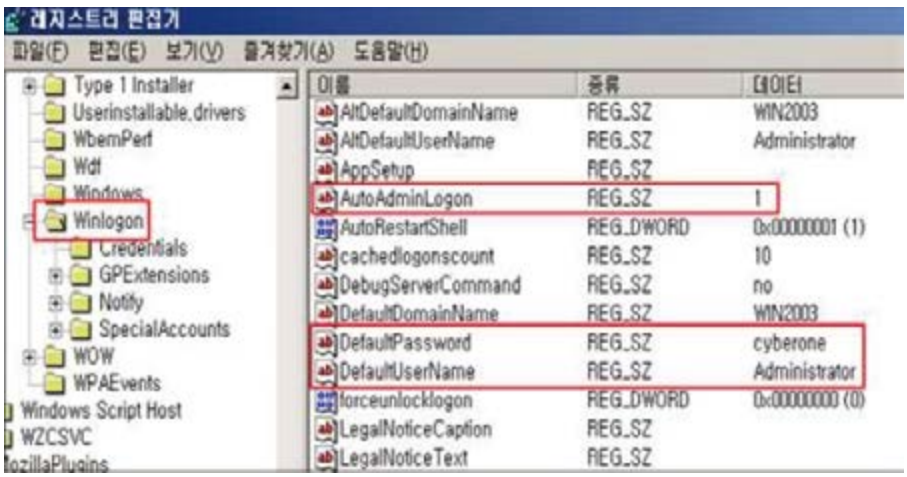
<table>
<tr><td>진단항목</td><td colspan="2">W-29. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">해당 정책이 활성화되어 있는 경우 악의적인 목적으로 시스템 종료를 유발하여 서비스 거부 공격에 악용될 수 있으며, 비정상적인 시스템 종료로 인하여 시스템 및 데이터에 손상을 입힐 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안 함"으로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용"으로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 명령 프롬프트에서 확인
- 시작 > 실행 > cmd.exe > secedit /export /cfg c:₩cfg.txt 명령어 실행
- 탐색기 > cfg.txt 파일을 열어서 CrashOnAuditFail 설정 값이 4, 0으로 되어 있는지 확인
 
- CrashOnAuditFail 4, 0 (보안 감사를 로그할 수 없을 때 즉시종료 안함)
- CrashOnAuditFail 4, 1 (보안 감사를 로그할 수 없을 때 즉시 종료함)
■ 로컬 보안 정책에서 확인
시작 > {프로그램} > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > "감사: 보안 감사를 기록할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안 함"으로 되어 있는지 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ [Win2012, 2016, 2019]
- 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
- "감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함</td></tr>
</table>

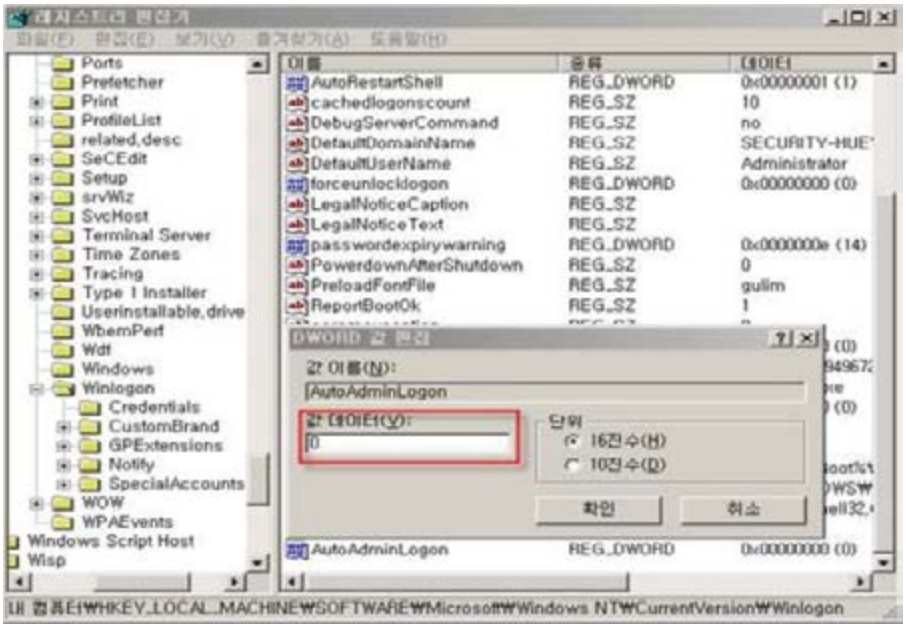
	"으로 설정  로컬 보안 설정 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 계정 정책 암호 정책 계정 잠금 정책 로컬 정책 감사 정책 사용자 권한 할 보안 옵션 공개 키 정책 소프트웨어 제한 정 IP 보안 정책(위치: 정책 보안 설정 감사: 글로벌 시스템 개체에 대한 액세스 감사 사용 안 함 감사: 백업 및 복원 권한 사용을 감사 사용 안 함 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 사용 안 함 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 등록 정보 로컬 보안 설정 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 사용(E) 사용 안 함(S) 이 설정을 수정하면 클라이언트나 서비스 또는 응용 프로그램과의 호 환성에 영향을 미칠 수 있습니다. 자세한 정보: 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 을(를) 참조하십시오. (Q823659) 확인 취소 적용(A) 네트워크 액세스: 익명으로 액세스할 수 있는 공유 COMCFG,DFS$ 네트워크 액세스: 익명으로 액세스할 수 있는 명명된 파이프 COMNAP,COMNODE,SQL\ 네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용 사용 안 함 네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함 사용 안 함 네트워크 액세스: SAM 계정의 익명 열거 허용 안 함 사용 안 함 대화형 로그온: CTRL+ALT+DEL을 사용할 필요 없음 사용 안 함 대화형 로그온: 로그온 사도하는 사용자에 대한 메시지 제목 정의되지 않음
비고	

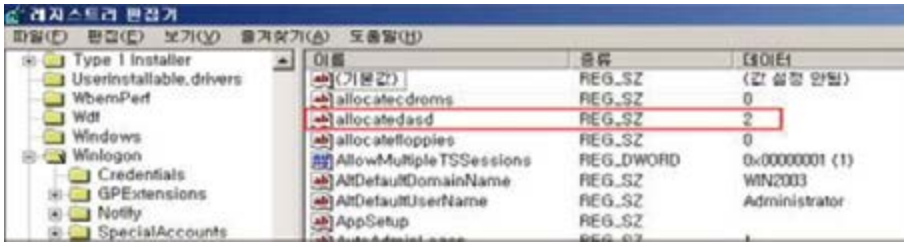
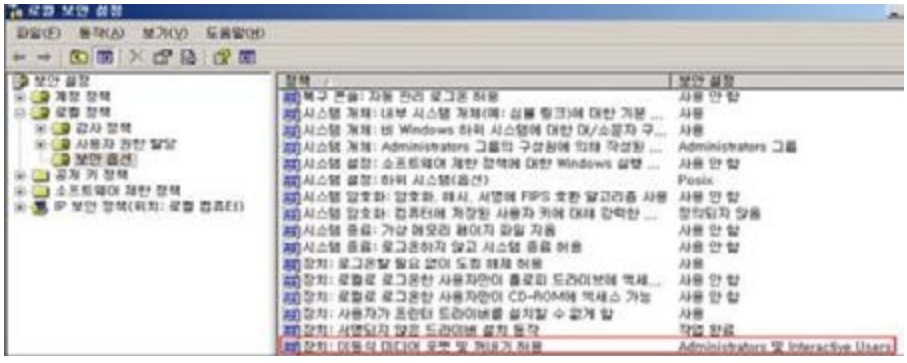
<table>
<tr><td>진단항목</td><td colspan="2">W-30. SAM 계정과 공유의 익명 열거 허용 안함</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Windows에서는 익명의 사용자가 도메인 계정(사용자, 컴퓨터 및 그룹)과 네트워크 공유 이름의 열거 작업을 수행할 수 있으므로 SAM(보안계정관리자) 계정과 공유의 익명 열거가 허용될 경우 악의적인 사용자가 계정 이름 목록을 확인하고 이 정보를 사용하여 암호를 추측하거나 사회 공학적 공격기법을 수행할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">아래의 보안옵션을 모두 사용하고 있을 경우
- 네트워크 액세스: SAM 계정의 익명 열거 허용 안 함
- 네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함</td></tr>
<tr><td>취약</td><td colspan="3">양호의 기준에 맞지 않을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 레지스트리에서 확인
- 시작 > 실행 > regedit
- HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Lsa
- restrictanonymous과 restrictanonymoussam의 값이 1로 되어있는지 확인
 

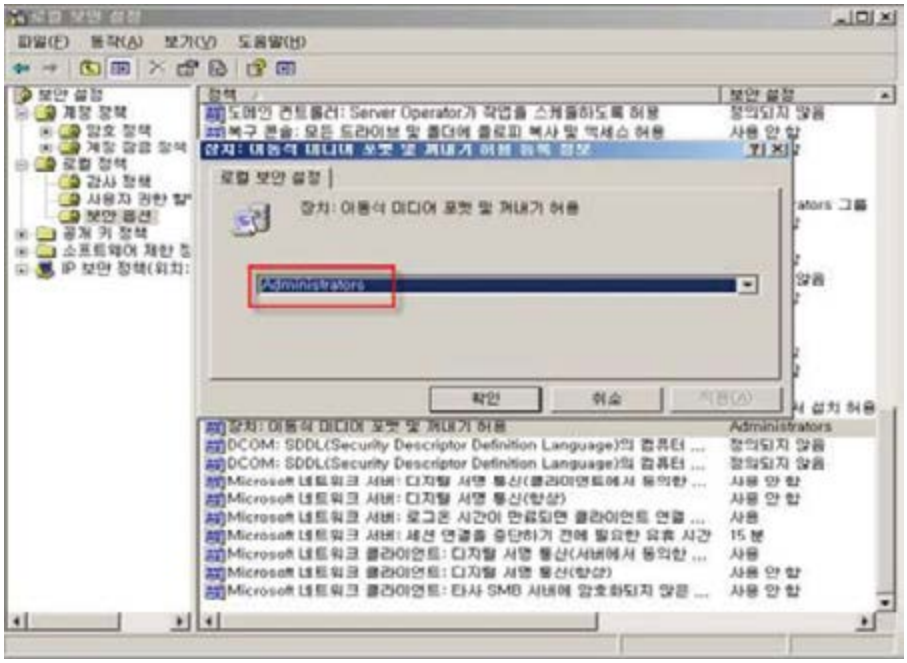
■ 로컬 보안 정책에서 확인
시작 > {프로그램} > 관리도구 > 로컬 보안 정책 > 보안 옵션에서 "네트워크 액세스: SAM 계정과 공유의 익명 열거 허용 안 함" 정책과 "네트워크 액세스: SAM 계정의 익명 열거 허용 안 함" 정책이 모두 "사용"으로 되어있는지 확인</td></tr>
</table>

<table>
<tr><td></td><td>  </td></tr>
<tr><td>조치방법</td><td>[GUI]
■ Windows 2012, 2016, 2019
1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2) "네트워크 액세스 : SAM 계정과 공유의 익명 열거 허용 안 함"과 "네트워크 액세스 : SAM 계정의 익명 열거 허용 안 함"에 "사용" 선택
 
[레지스트리]
■ Windows 2012, 2016, 2019
- 시작> 실행> regedit> HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Control Lsa
- restrictanonymous과 restrictanonymoussam의 값을 1로 변경</td></tr>
<tr><td>비고</td><td>Active Direcory, Clustered system에서는 적용 시 영향 있음</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">W-31. Autologon기능 제어</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에 저장된 로그인 계정 및 패스워드 정보 유출이 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">AutoAdminLogon 값이 1로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩ Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon에서 AutoAdminLogon 가 존재하지 않거나 "0" 으로 설정되어 있는지 확인 (AutoAdminLogon가 존재하지 않거나, 0으로 설정되어 있을 경우 양호)
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[레지스트리]
■ [Win2012, 2016, 2019]
- 시작> 실행> REGEDIT>HKLM₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩Winlogon
- "AutoAdminLogon 값"을 "0"으로 설정
- DefaultPassword 엔트리가 존재한다면 삭제</td></tr>
</table>

	
비고	▪ 반드시 자동 로그인을 사용하여야 할 경우를 제외하고는 조치 시 일반적으로 영향 없음

<table>
<tr><td>진단항목</td><td colspan="2">W-32. 이동식 미디어 포맷 및 꺼내기 허용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자 이외 사용자에게 해당 정책이 설정된 경우 비인가자에 의한 불법적인 매체 처리를 허용할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">"이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 레지스트리에서 확인
시작 > 실행 > regedit > HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon 에서 allocatedasd 값이 "0" 으로 되어 있는지 확인
 
■ 로컬 보안 정책에서 확인
시작 > 프로그램 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어 있는지 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">[GUI]
■ [Win 2012, 2016, 2019]
- 시작> 실행> SECPOL.MSC>로컬 정책>보안 옵션
- "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators"로 설정</td></tr>
</table>

	 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 계정 정책 로컬 정책 보안 옵션 정책 보안 설정 로컬 보안 설정 장치: 이동식 미디어 포맷 및 꺼내기 허용 Administrators 확인 취소 장치: 이동식 미디어 포맷 및 꺼내기 허용 Administrators DCOM: SDDL(Security Descriptor Definition Language)의 컴퓨터 ... 정의되지 않음 DCOM: SDDL(Security Descriptor Definition Language)의 컴퓨터 ... 정의되지 않음 Microsoft 네트워크 서버: 디지털 서명 통신(항상) 사용 안 함 Microsoft 네트워크 서버: 로그온 시간이 만료되면 클라이언트 연결 ... 사용 Microsoft 네트워크 서버: 세션 연결을 중단하기 전에 필요한 유휴 시간 15 분 Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 ... 사용 Microsoft 네트워크 클라이언트: 디지털 서명 통신(항상) 사용 안 함 Microsoft 네트워크 클라이언트: 타사 SMB 서버에 암호화되지 않은 ... 사용 안 함
비고	

2.5. Windows PC

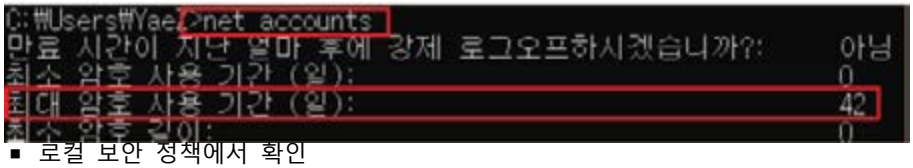
계정 관리(2개 항목), 파일 시스템(3개 항목), 패치 관리(2개 항목), 보안 관리(6개 항목) 총 4개 영역에서 13개 항목으로 구성된다.

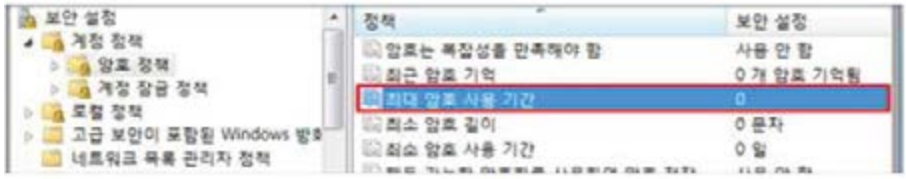
구분	진단코드	진단 항목	취약도
가. 계정 관리	PC-01	패스워드의 주기적 변경	상
	PC-02	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상
나. 파일 시스템	PC-03	공유 폴더 제거	상
	PC-04	불필요한 서비스 제거	상
	PC-05	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상
다. 패치 관리	PC-06	HOT FIX 등 최신 보안패치	상
	PC-07	최신 서비스 팩 적용	상
다. 보안 관리	PC-08	바이러스 백신 프로그램 설치 및 주기적 업데이트	상
	PC-09	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상
	PC-10	OS에서 제공하는 침입차단 기능 활성화	상
	PC-11	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상
	PC-12	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립	상
	PC-13	비인가 무선랜 사용제한	중

[표 5] PC(Windows) 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">PC-01 패스워드의 주기적 변경</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">계정의 패스워드를 주기적으로 변경하지 않고 오랫동안 사용할 경우 계정 패스워드가 외부에 유출될 수 있으며, 관리자 계정의 패스워드가 유출될 시 자료 유출 등 심각한 사고 발생 가능성이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최대 암호 사용 기간이 “90일”이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">암호 사용 기간이 “90일”초과 또는 “제한 없음”으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 최대 암호 사용 기간이 “90일”로 설정되어 있는지 확인한다

▪ 명령 프롬프트에서 확인
[Win10]
1) 시작 > 실행 > cmd > net accounts 명령어
2) 실행하여 “최대 암호 사용 기간(일)”이 “90일”이하로 설정되어 있는지 확인
 

▪ 로컬 보안 정책에서 확인
[Win10]
1) 제어판 > 관리도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 암호 정책
2) “최대 암호 사용 기간”이 “90일”이하로 설정되어 있는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 암호 사용기간 제한 없음 비활성화 여부 확인
1) 명령 프롬프트에서 확인
> wmic useraccount where Disabled=FALSE get Name, PasswordExpires
2) 조치방법
- “암호 사용 기간 제한 없음” 해제(컴퓨터 관리)
- “최대 암호 사용 기간”을 “90일”로 설정
▪ 컴퓨터 관리에서 Administrator 암호 사용 기간 제한 없음 해제
1) 제어판 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자
2) Administrator 마우스 우 클릭 > 속성에서 “암호 사용 기간 제한 없음” 해제</td></tr>
</table>

<table>
<tr>
<td></td>
<td>

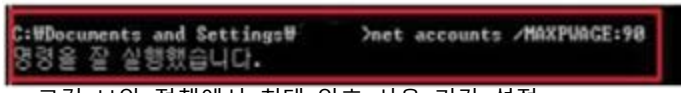

■ 명령 프롬프트에서 암호 사용 기간 제한 없음 해제

> wmic useraccount where Name='계정명' set PasswordExpires=TRUE

■ 명령 프롬프트에서 최대 암호 사용 기간 설정

[Win10]

1) 시작 > 실행 > cmd > net accounts /MAXPWAGE:90 명령어를 입력

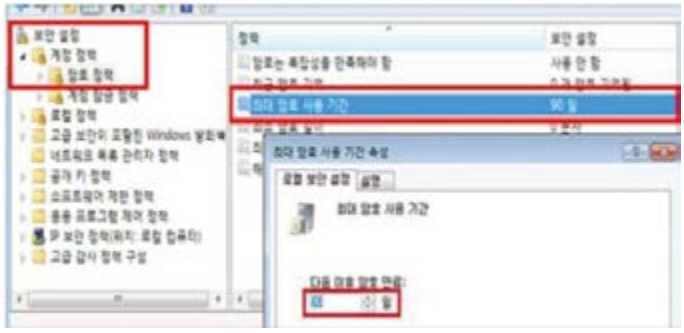
 

■ 로컬 보안 정책에서 최대 암호 사용 기간 설정

[Win10]

1) 제어판 > 관리도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책

2) "최대 아호 사용 기간" 정책의 속성 > "다음 이후 암호 만료" 값을 "90일"로 설정

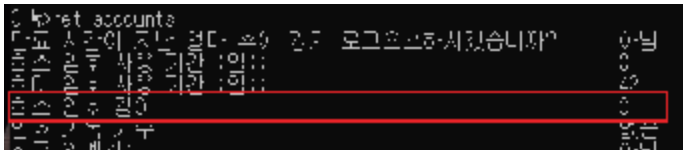
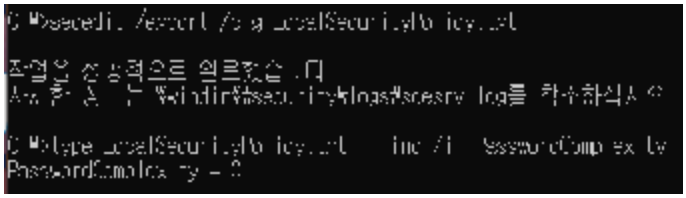
 
</td>
</tr>
<tr>
<td>비고</td>
<td>※ 최대 암호 사용 기간을 "90일"이하로 설정하고, 이 정책이 활성화되기 위해 우선적으로 암호 사용 기간 제한을 없음을 해제해야 함

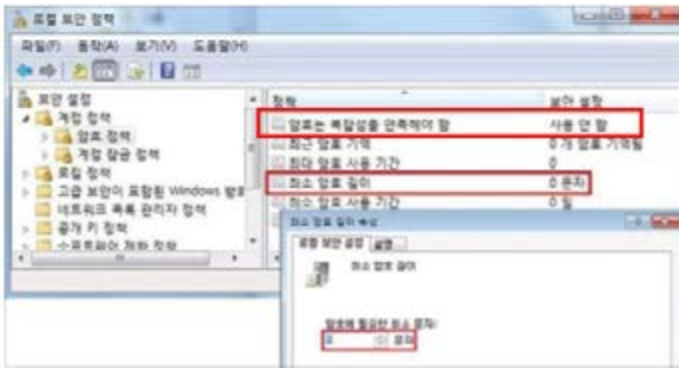
※ 환경에 따라 30에서 90일마다(기본 값: 42) 암호가 만료되도록 설정하는 것이 보안을 위해 가장 좋으며, 이 방법을 사용하면 침입자가 사용자의 암호를 도용하여 네트워크 리소스에 무단으로 액세스하는 횟수가 제한되어야 함

※ 명령 프롬프트(cmd)는 관리자 권한으로 실행해야 함</td>
</tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">PC-02. 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">대부분의 환경에서 3종류(영문·숫자·특수문자)조합의 경우 8자리 패스워드 사용, 2종류(영문·숫자) 조합의 경우 10자리 암호 사용을 권고하고 있다. 패스워드 정책에 적합하게 패스워드가 설정된 경우 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing)에 대한 대비가 가능하다.

* 무작위 대입 공격(Brute Force Attack) : 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도를 말한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최소 암호 길이 및 패스워드 복잡성 정책이 반영되어 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 복잡성 정책이 반영되지 않고, 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 최소 암호 길이가 해당 기관의 보안 정책에 적합하게 설정되어 있는지 확인

■ 명령 프롬프트에서 "최소 암호 길이"와 "패스워드 복잡도 설정" 확인
[Win10]
1) 시작 > 실행 > cmd > net accounts 명령어를 실행하여 "최소 암호 길이" 확인
 
2) secedit /export /cfg LocalSecurityPolicy.txt
type LocalSecurityPolicy.txt | find /i "PasswordComplexity"
 
■ 로컬 보안 정책에서 "최소 암호 길이"와 "암호는 복잡성을 만족해야 함" 값 확인
[Win10]
1) 제어판 > 관리도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 암호 정책
2) "최소 암호 길이 속성"과 "암호는 복잡성을 만족해야 함" 값 확인</td></tr>
</table>

	
조치방법	※ 최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정 ※ 명령 프롬프트(cmd)는 관리자 권한으로 실행해야 함 ■ 명령 프롬프트에서 "최소 암호 길이" 설정 [Win10] 1) 시작 > 실행 > cmd > net accounts /MINPWLEN:8 명령어를 입력 ■ 로컬 보안 정책에서 "최소 암호 길이"와 "암호는 복잡성을 만족해야 함" 설정 [Win10] 1) 제어판 > 관리도구 > 로컬 보안 정책 > 보안 설정 > 계정 정책 > 암호 정책 2) "최소 암호 길이" 정책의 속성 > "암호에 필요한 최소 문자" 값을 "8문자"로 설정하고 "암호는 복잡성을 만족해야 함" 설정 값을 "사용"으로 설정
비고	■ 패스워드 설정 기준 1) 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정 (다음 각 항목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성) - 영문 대문자(26개) - 영문 소문자(26개) - 숫자(10개) - 특수문자(32개) 2) 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계 - Null(공백) 패스워드 사용 금지 - 문자 또는 숫자만으로 구성 금지 - 사용자 ID와 동일하거나 유사한 패스워드 금지 - 연속적인 문자나 숫자 사용 (예) 1111, 1234, abcd) 사용 금지 - 주기성 패스워드 재사용 금지 - 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지

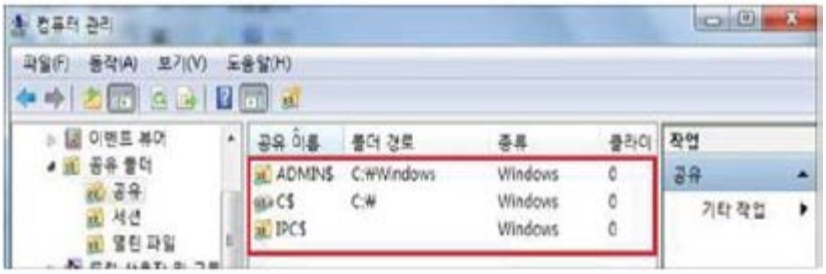
	3) SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용을 권장(8자로 이루어진 암호 사용 권장) 4) 아래와 같은 암호 설정 지양 Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명 예) root, rootroot, root123, 123root, admin, admin123, 123admin, osadmin, adminos

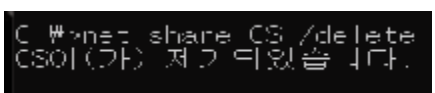
나. 파일 시스템

<table>
<tr><td>진단항목</td><td colspan="2">PC-03. 공유 폴더 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">시스템의 기본 공유 항목이 제거되지 않으면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있다. 2001년에 발생한 *Win32.Nimda 바이러스도 여러 가지 방법 중에서 이러한 공유 기능 치무의 한 경로를 이용한 것이다. 따라서 불필요한 공유라고 판단되면 공유를 해제해야 하며, 공유를 해제한 후에 레지스트리 AutoShareServer 값 설정을 통해 재부팅 시 기본 공유 폴더의 자동 공유 설정을 방지할 수 있다. (하드디스크 기본 공유 폴더 예: C$, D$, Admin$, IPC$ 등) 또한, 기본 공유 폴더를 제외한 일반 공유 폴더의 권한이 Everyone으로 설정되었는지 확인하고, 공유 금지 설정을 통해 익명 사용자에 의한 접근을 차단해야 한다.

* Win32.Nimda 바이러스: 2001년 9월 17일 미국·유럽·라틴아메리카에서 동시에 발생한 뒤 한국에서도 다음 날 저녁 발견될 정도로 빠르게 확산하는 악성 컴퓨터 바이러스이다. 두 종류가 있는데, 하나는 정부를 뜻하는 영어 단어 'admin'의 철자를 거꾸로 나열해 명명한 것이고, 다른 하나는 제3차 세계대전을 뜻하는 'To 3W'를 거꾸로 나열한 'W32' 이다. 이 바이러스는 이메일뿐만 아니라 감염된 웹 사이트를 통해서도 전염되며, 네트워크상에서 패스워드 없이 읽기·쓰기가 가능한 공유 디렉터리를 통해서도 감염되는 특징을 가진다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 공유 폴더가 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 공유 폴더가 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 불필요한 기본 공유 폴더 및 일반 공유 폴더가 존재하는지 확인

▪ 명령 프롬프트에서 공유 폴더 확인
[Win10]
1) 시작 > 실행 > cmd > net share 명령어를 입력하여 불필요한 공유 폴더 확인
 
▪ 컴퓨터 관리에서 공유 폴더 확인
1) 제어판 > 관리도구 > 컴퓨터 관리 > 공유 폴더 > 공유에서 불필요한 공유 폴더 확인</td></tr>
</table>

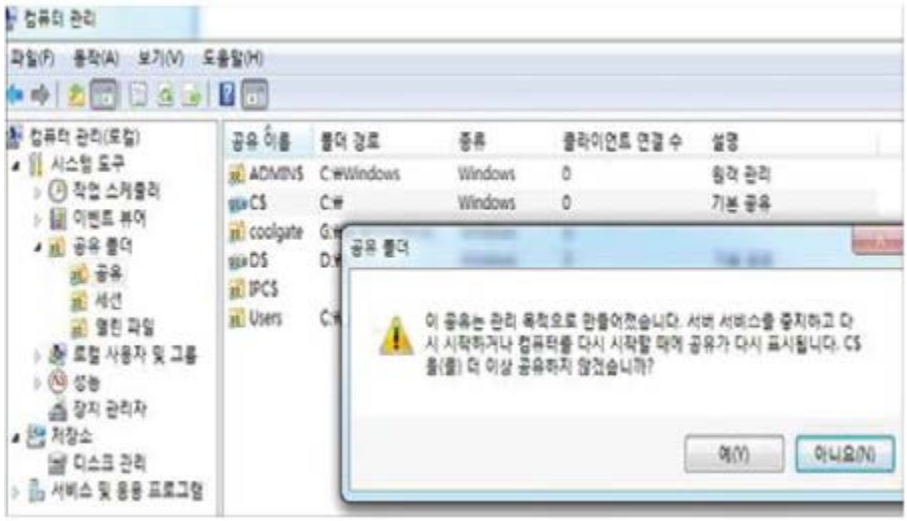
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>조치방법</td><td>※ 기본 공유 폴더 및 일반 공유 폴더 존재 시 제거하고, 재부팅 후 자동 공유 되지 않도록 설정
※ 기본 공유에 대한 조치 시 반드시 [기본 공유 삭제], [비활성화 레지스트리 값]을 모두 설정해야 함

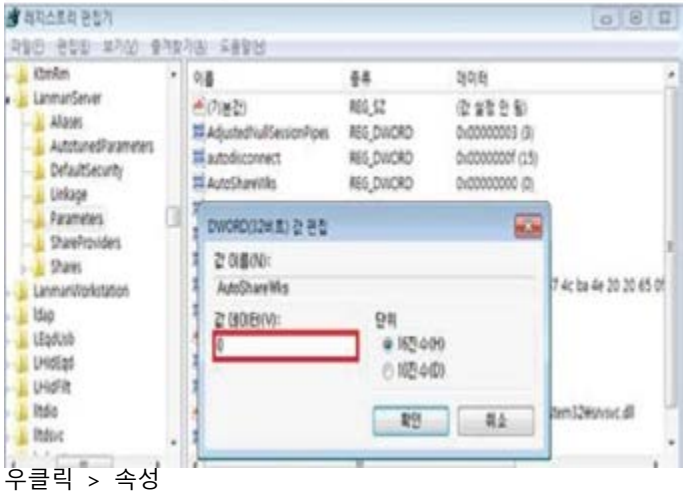
■ 명령 프롬프트에서 기본 공유 중지
[Win10]
1) 시작 > 실행 > cmd > net share “삭제할 공유 폴더명” /delete 명령을 통해 공유 디렉터리 삭제
 

■ 컴퓨터 관리에서 기본 공유 중지
[Win10]
1) 제어판 > 관리도구 > 컴퓨터 관리 > 공유 폴더 > 공유 > 불필요한 공유 폴더 우클릭
2) 공유 중지 (하드디스크 기본 공유 폴더는 C$, D$, Admin$, IPC$가 있으며, C$, D$, Admin$ 폴더의 공유 제거

■ 시스템 재부팅 시 기본 공유 폴더 자동 공유 방지 설정
1) 시작 > 실행 > regedit 입력
2) HKLM₩System₩CurrentControlSet₩Services₩LanmanServer₩Parameters
3) AutoShareWks 의 데이터 값을 0으로 설정
4) 값이 없는 경우, “DWORD 값” 선택하고 AutoShareWks를 추가하여 값을 “0”으로 입력

■ 일반 공유 폴더 사용 시 접근 권한 설정, 사용 권한, 암호 설정
1) 일반 공유 폴더에 Everyone 공유 제거
① 제어판 > 관리 도구 > 컴퓨터 관리 > 공유 폴더 > 공유 > 사용할 공유 폴더</td></tr>
</table>



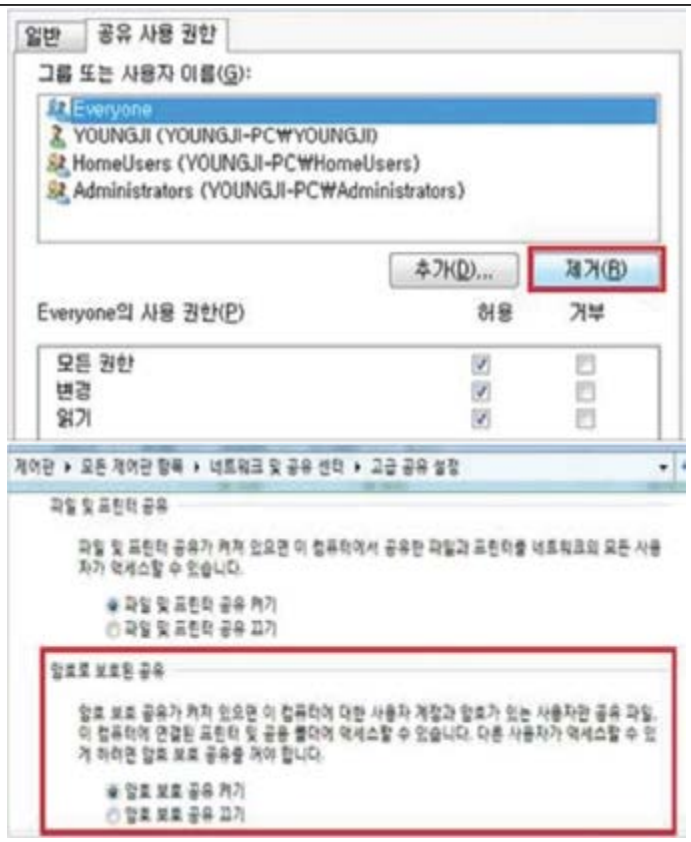


우클릭 > 속성

② [공유 사용 권한] 탭에서 "Everyone"으로 된 공유 제거, 접근이 필요한 계정만 권한 추가

2) 공유 폴더의 접근 암호 설정

① 제어판 > 네트워크 및 공유 센터 > 고급 공유 설정에서 "암호 보호 공유 켜기" 설정

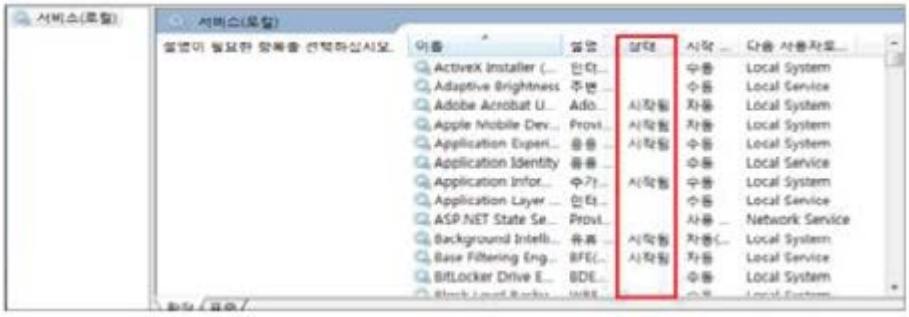
<table>
<tr>
<td></td>
<td>


3) 공유 폴더 접근 가능 여부 확인
① 시작 > 실행 > 공유 폴더 PC 계정명 또는 IP 주소 입력 후 패스워드 입력 팝업 확인

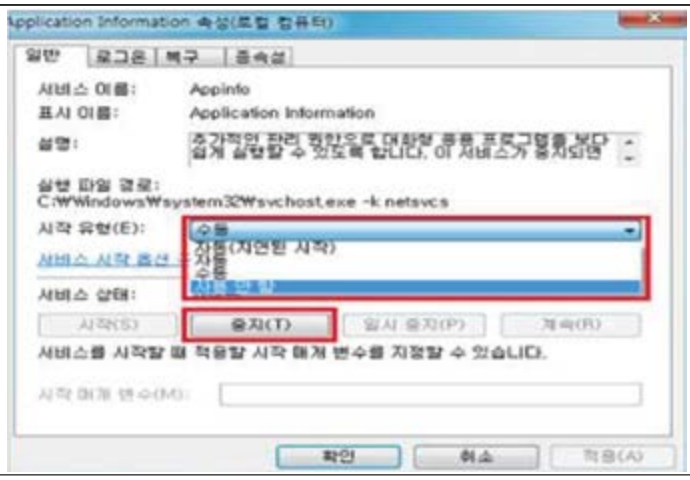

</td>
</tr>
<tr>
<td>비고</td>
<td>
■ 공유 폴더 설정 기준
1) C$, D$, Admin$ 등의 기본 공유 폴더 제거
2) 기본 공유 폴더 제거 후 시스템 재부팅 시 "기본 공유 폴더가 자동으로 공유되는 것"을 방지하기 위해 해당 레지스트리의 AutoShareServer 값을 "0"으로 설정
3) 일반 공유 폴더 사용 시 공유 폴더 접근 권한에 "Everyone" 제거
</td>
</tr>
</table>

	4) 일반 공유 폴더 사용 시 접근이 필요한 계정에만 적절한 (읽기, 변경)권한 설정 5) 일반 공유 폴더 사용 시 공유 폴더 접근을 위한 암호 설정 ※ 업무에 필요한 공유 폴더 사용 시 사용자별 권한 부여 필요 ※ 방화벽과 라우터에서 135, 139(TCP/UDP)포트를 차단하여 외부로부터 위험을 제거함으로써 보안성을 높일 수 있음

<table>
<tr><td>진단항목</td><td colspan="2">PC-04. 불필요한 서비스 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">불필요한 서비스가 시스템에 디폴트로 설치되어 실행되는 경우 시스템 자원을 낭비하게 될 뿐만 아니라, 이 서비스를 통해 악의적인 공격자가 침입할 수 있으므로 필요하지 않은 서비스는 중지시켜야 한다. 시스템 관리자는 대상 시스템의 용도를 정확히 파악한 후 특별한 목적으로 사용하는 업무 관련 서비스를 제외한 다른 불필요한 서비스를 제거해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">업무에 필요한 서비스만 실행되고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">디폴트로 설치된 서비스가 실행되고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 업무에 불필요한 서비스가 실행되고 있는지 확인한다.

■ 서비스에서 확인
[Win10]
1) 제어판 > 관리도구 > 서비스 > 서비스 상태를 확인하여 불필요한 서비스가 실행 중인지 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 업무에 불필요한 서비스를 중지시키고 시작 유형을 “사용 안 함”으로 설정한다.

■ 서비스에서 설정
[Win10]
1) 제어판 > 관리도구 > 서비스 > 해당 서비스 선택 > 속성 > [일반] 탭
2) 불필요한 서비스 → 중지, 시작 유형 → 사용 안 함</td></tr>
</table>



비고

※ 해당 서비스의 속성에서 "시작 유형" 선택 및 "시작 시 로그온 계정" 별도 설정이 가능

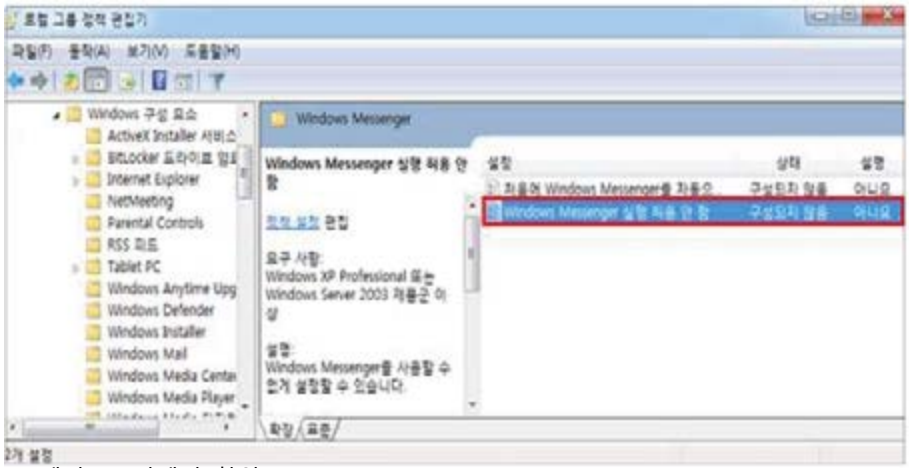
서비스 시작 유형	설명
사용 안 함	설치되어 있으나 실행되지 않음
수동	다른 서비스나 응용 프로그램에서 당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영체제에 의해 시작됨

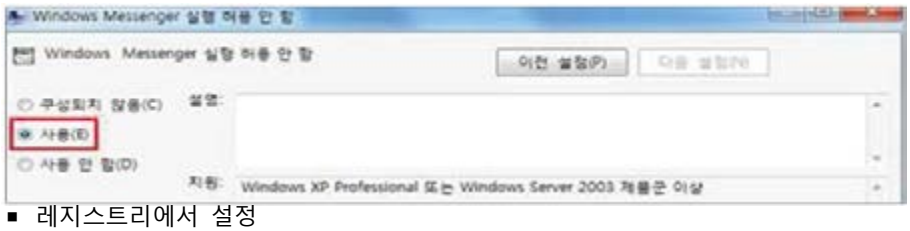
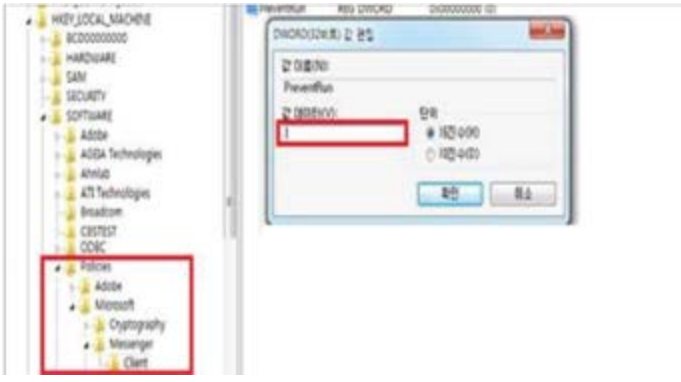
※ 서비스 리스트

불필요한 서비스 리스트	windows 운영을 위한 최소한의 서비스
- Alerter - Clipbook - ComputerBrowser - DHCP Client - TerminalService - Print spooler - Messenger - NetLogon - Network DDE - Network DDE DSDM - FTP Publishing Service - InternetConnectionSharingService - IndexingService - InfaredMonitorService - NetMeetingRemoteDesktopSharingService - RemoteRegistryService - RoutingandRemoteAccessService - SimpleTCP/IPService - SMTPService - TaskSchedulerService - TCPIP NetBIOS Helper	- Logical Logging Manager - Network Connections - NTLM Security Support Provider - Plug and Play - Server - Workstation - Removeable Storage - Security Accounts Manager - Windows Management Instrumentation - Windows Management Instrumentation driver extensions - WMDM PMSP Service - Application Management

<table>
<tr><td>진단항목</td><td colspan="2">PC-05. Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자 PC에서 Windows Messenger를 사용할 경우, *메신저(Messenger)를 통해서 주요 정보가 유출될 수 있을 뿐만 아니라 *악성코드가 유입될 수 있다.

* 메신저(Messenger): 인터넷을 통해 실시간으로 대화를 나눌 수 있는 서비스.
* 악성코드: 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Windows Messenger가 실행되고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">Windows Messenger가 실행되고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ Windows Messenger가 실행되고 있는지 확인

■ 로컬 그룹 정책 편집기에서 확인
[Win10]
1) 시작 > 실행 > gpedit.msc 입력 > 컴퓨터 구성 > 관리 템플릿 Windows 구성 요소
2) Windows Messenger 에서 "Windows Messenger를 실행 허용 안 함" 확인 ("사용" 으로 설정되어 있는 경우 양호)
 
■ 레지스트리에서 확인
[Win10]
1) 시작 > 실행 > regedit 입력
2) HKLM₩Software₩Policies₩Microsoft₩Messenger₩Client
3) PreventRun의 데이터 값이 1로 설정되어 있는지 확인 (1일 경우 양호)</td></tr>
</table>

조치방법	※ Windows Messenger를 실행하지 않음으로 설정 ■ 로컬 그룹 정책 편집기에서 설정 [Win10] 1) 시작 > 실행 > gpedit.msc 입력 2) 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > Windows Messenger 3) "Windows Messenger를 실행 허용 안 함" 정책 마우스 우클릭 > 편집에서 "사용"으로 설정  ■ 레지스트리에서 설정 [Win10] 1) 시작 > 실행 > regedit 입력 2) HKLM₩Software₩Policies₩Microsoft₩Messenger₩Client 3) PreventRun 마우스 우클릭 > 수정에서 값 데이터를 1로 설정 
비고	※ Windows Messenger 사용 불가 ※ 원격 지원에서도 Windows Messenger를 사용할 수 없음

다. 패치 관리

<table>
<tr><td>진단항목</td><td colspan="2">PC-06. HOT FIX 등 최신 보안패치</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">HOT FIX 설치 및 자동 업데이트가 설정되어 있지 않은 경우 취약점으로 인한 공격이 발생할 수 있으므로 Hot Fix 출시 즉시 신속하게 설치하고 항상 최신의 보안 업데이트가 이루어져야 한다.

* Hot Fix : 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련)을 패치하기 위해 배포되는 프로그램으로 서비스 팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표된다.
* 업데이트(Update) : 문제를 예방 또는 해결하거나 컴퓨터 작동 방식을 향상시키거나 컴퓨팅 경험을 향상시킬 수 있도록 추가되는 소프트웨어를 말한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최근 한 달 이내 HOT FIX 설치 및 자동 업데이트 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최근 한 달 이내 HOT FIX가 설치되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 시스템의 최신 패치 여부를 확인

■ 최신 패치 여부 확인
[Win10]
1) 시작 > 설정 > 업데이트 및 복구 > "업데이트 확인"을 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ HOT FIX, 최신 보안 업데이트 등을 설치한다.

■ 최신 패치
[Win10]
1) 시작 > 설정 > 업데이트 및 복구 > "업데이트 확인", "지금 설치"를 통하여 HOT FIX, 최신 보안 업데이트 등의 설치 여부 확인 및 설정 변경</td></tr>
</table>

	
비고	

<table>
<tr><td>진단항목</td><td colspan="2">PC-07. 최신 서비스 팩 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 *서비스 팩을 적용하지 않을 경우, 공격에 쉽게 노출될 수 있다.

* 서비스 팩 : Windows 시스템을 마이크로소프트에서 출시하고 난 뒤 Windows와 관련된 응용프로그램,서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 프로그램을 말한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 서비스 팩이 적용 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 서비스 팩이 적용 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 최신 서비스 팩이 설치되어 있는지 확인

▪ 실행을 통한 확인
[Win10]
1) 시작 > 실행 > winver 입력 > Windows 정보 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 최신 서비스 팩을 설치한다.
※ 네트워크와 분리된 상태에서 서비스 팩 설치를 권장한다. 현재 많은 인터넷 웜(Worm)이 Windows의 취약점을 이용하여 공격하므로 OS 설치 후 곧바로 네트워크에 연결하는 것은 서버에 피해를 입을 수 있다.

▪ 수동 조치
[Win10]
1) 서비스 팩 확인 후 최신 버전이 아닐 경우 Microsoft 홈페이지에서 다운로드 하여 설치
1. 참고 사이트
http://windows.microsoft.com/ko-kr/windows/service-packs-download#sptabs=win7</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

라. 보안 관리

진단항목	PC-08. 바이러스 백신 프로그램 설치 및 주기적 업데이트	취약도	상
항목설명	바이러스 백신 프로그램 *바이러스, *웜 등으로부터 시스템을 보호하기 위한 중요한 보안 요소이다. 최신 바이러스 탐지를 위하여 패턴 업데이트가 자주 발생하므로 이를 즉각적으로 반영하는 것이 중요하다. * 바이러스(Virus) : 바이러스는 스스로를 복제하려는 명백한 의도를 갖고 만들어진 코드 사용을 통해 호스트 프로그램에 침투하여 컴퓨터 사이에서 확산을 시도한다. 호스트가 실행되면 바이러스도 함께 실행되어 새로운 숙주를 감염시키는 등 시스템에 직접적인 피해를 줄 수 있고, 이메일이나 다른 외부저장장치를 통해서 다른 PC들로도 전파가 가능하고 전염성이 매우 강해서 PC 내로 들어오면 다른 파일들까지 급속하게 감염시킬 수 있다. * 웜(Worm): 컴퓨터 바이러스의 하나로 컴퓨터 바이러스와 비슷하지만, 바이러스가 다른 실행 프로그램에 기생하여 실행되는 데 반해 웜은 독자적으로 실행되며, 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼지는 부정 프로그램을 말한다.		
진단기준	양호	백신이 설치되어 있고, 최신 업데이트가 적용 되어 있는 경우	
	취약	백신이 설치되어 있지 않거나, 최신 업데이트가 적용 되어 있지 않은 경우	
진단방법	▪ 수동 점검 [Win10] 백신 프로그램의 설치 여부와 최신 Update 여부를 수동으로 점검		
조치방법	▪ 바이러스 백신 설치 후 최신 업데이트를 적용		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">PC-09. 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">바이러스 백신 프로그램의 실시간 감시 기능으로 바이러스, 스파이웨어 탐지 및 방화벽 설정 등이 가능하다. 시스템에 대한 위협 발생 시 즉시 대응이 가능하도록 실시간 감시 기능을 사용할 것을 권고한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">설치된 백신의 실시간 감시 기능이 활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">백신이 설치되어 있지 않거나, 실시간 감시 기능이 비활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 수동 점검
[Win10]
1) 백신의 실시간 감시 기능이 활성화 되어 있는지 수동으로 점검</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 백신의 실시간 감시 기능을 활성화</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">PC-10 OS에서 제공하는 침입차단 기능 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">윈도우에서 제공하는 침입차단 기능인 윈도우 방화벽을 사용함으로써 PC의 자료 유출 방지, 불법 접근 차단 등을 가능하게 한다. 네트워크 방화벽과 더불어 각각의 PC에 윈도우 방화벽과 같은 호스트 기반의 방화벽을 구현할 때 네트워크의 방어 수준이 향상 될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Windows 방화벽이 “사용”으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Windows 방화벽이 “사용 안 함”으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 제어판에서 확인
[Win10]
1) 제어판 > Windows 방화벽(또는 시작 > 실행 > “firewall.cpl” 입력)
2) Windows 방화벽 사용 여부를 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">※ Windows 방화벽을 사용하도록 설정
■ 제어판에서 설정
[Win10]
1) 시작 > 제어판 > Windows 방화벽 > Windows 방화벽 설정 또는 해제
2) Windows 방화벽 “사용” 설정
 
■ 레지스트리에서 설정
[Win10]
1) 시작 > 실행 > “regedit” 입력
2) HKLM₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile</td></tr>
</table>

	
비고	

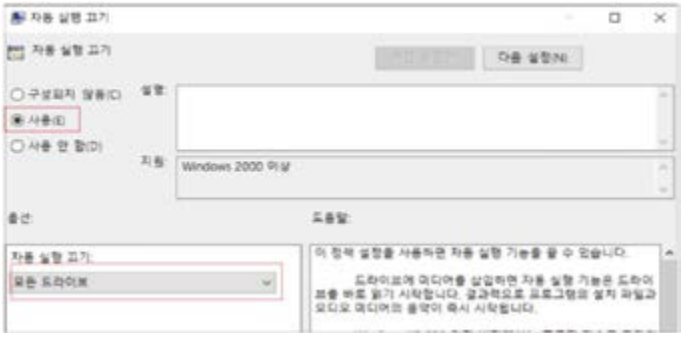
<table>
<tr><td>진단항목</td><td colspan="2">PC-11 화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프되거나 워크스테이션이 잠기도록 설정하여야 한다. 해당 기능을 설정하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있으므로 화면보호기 대기 시간 및 암호 사용 설정을 이용해서 비인가자의 물리적 접근을 차단한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">화면보호기 설정 및 암호로 보호가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">화면보호기 설정 및 암호로 보호가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 화면보호기 설정이 되어 있는지 확인
[Win10]
1) 시작 > 제어판 > 개인 설정 > 화면보호기에서 화면보호기 설정 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 화면보호기 설정이 되어 있는지 확인
[Win10]
1) 시작 > 제어판 > 개인 설정 > 화면보호기에서 화면보호기 설정
2) 대기 시간을 5분~10분 사이로 설정 후 “다시 시작할 때 로그온 화면 표시(R)” 체크</td></tr>
</table>

	 화면 보호기 설정 화면 보호기 화면 보호기(S) 리본 설정(T)... 미리 보기(V) 대기(W): 5 분 다시 시작할 때 로그온 화면 표시(R)
비고	

<table>
<tr><td>진단항목</td><td colspan="2">PC-12 CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안 대책 수립</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">CD/DVD, USB 메모리 등과 같은 미디어에 탑재된 *Autorun.inf 파일을 통해 다른 응용 프로그램이 자동 실행될 수 있다. 대부분의 USB 관련 악성코드들은 Autorun.inf 파일을 통해 자동 실행되도록 제작되므로 이를 통해 악성코드가 PC로 쉽게 유입될 가능성이 존재한다.

* Autorun.inf 파일 : 윈도우 운영체제의 AutoRun, AutoPlay 기능에 사용되는 텍스트 파일, 미디어 장치의 루트 디렉터리에 위치하며, 미디어(CD/DVD, USB) 연결 시 특정 프로그램이 자동으로 실행되도록 제어한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">미디어 사용 시 자동 실행되지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">미디어 사용 시 자동 실행되는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 미디어 사용 시 자동 실행 되지 않도록 설정되어 있는지 확인

■ 로컬 그룹 정책 편집기에서 확인
[Win10]
1) 시작 > 실행 > “gpedit.msc” 입력
2) 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 자동 실행 정책
3) “자동 실행 끄기” 정책이 “사용”으로 되어 있는지 확인
 
■ 레지스트리에서 확인
[Win10]
1) 시작 > 실행 > “regedit” 입력
2) HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer
3) NoDriveTypeAutoRun의 데이터 값이 ff로 되어 있는지 확인
  </td></tr>
</table>

조치방법	※ 미디어 사용 시 자동 실행되지 않도록 설정 ■ 로컬 그룹 정책 편집기에서 설정 [Win10] 1) 시작 > 실행 > "gpedit.msc" 입력 2) 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 자동 실행 정책 3) "자동 실행 끄기" 정책을 "사용 – 모든 드라이브"로 설정  ■ 레지스트리에서 설정 [Win10] 1) 시작 > 실행 > "regedit" 입력 2) HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer 3) NoDriveTypeAutoRun 의 데이터 값을 ff로 설정  ■ 제어판에서 설정 [Win10] 1) 시작 > 제어판 > 자동 실행 > "모든 미디어 및 장치에 자동 실행 사용(U)" 체크 해제
비고	

<table>
<tr><td>진단항목</td><td colspan="2">PC-13 비인가 무선 랜 사용제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">내부에 설치된 비인가 AP 또는 사용자의 잘못된 설정으로 인한 Ad-Hoc 네트워크가 기업 네트워크의 백도어 역할을 하여 해당 위협 요소를 통해 불법 침입자가 내부 네트워크로 접근할 수 있다. 공공장소 무선 AP의 경우 해킹이나 관리자 계정의 중요성을 알지 못하거나, 손님 편의를 위해 패스워드를 공개하고, 번거롭다는 이유로 보안에 취약한 펌웨어 업데이트를 하지 않는 등 다양한 보안 위협요소가 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">비인가 무선 랜을 사용하고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">비인가 무선 랜을 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 무선 랜 사용 여부를 확인

▪ 명령프롬프트에서 확인
[Win10]
1) 시작 > 실행 > cmd > netsh wlan show profile 입력
2) 사용자 프로필에서 비인가 무선 랜 사용 여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 비인가 무선 랜을 차단
※ 허용할 무선 랜들을 접근 허용으로 설정 후 denyall 정책을 설정
※ 명령 프롬프트(cmd)는 관리자 권한으로 실행

▪ 명령프롬프트에서 설정
[Win10]
1) 시작 > 실행 > cmd
2) netsh wlan add filter permission=allow ssid=허용할 무선 랜 SSID networktype=infrastructure 입력
3) netsh wlan add filter permission=denyall networktype=infrastructure 입력</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

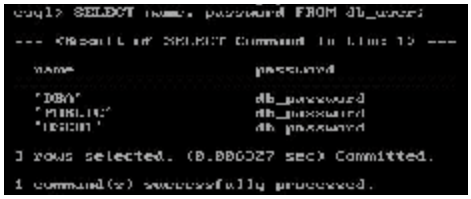
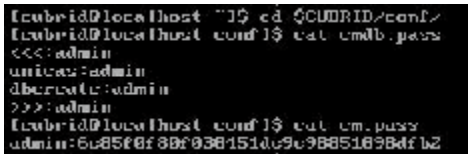
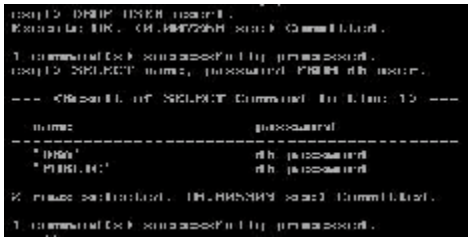
2.6. Cubrid

계정 관리(2개 항목), 보안 설정(5개 항목), 패치 및 로그관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

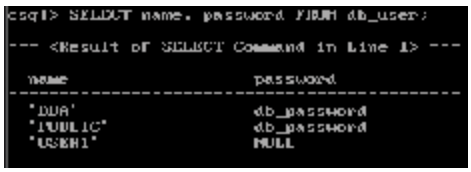
구분	진단코드	진단 항목	취약도
가. 계정 관리	CU-01	불필요한 계정 제거	중
	CU-02	취약한 패스워드 사용 제한	상
나. 보안 설정	CU-03	타 사용자에 권한 부여 옵션 사용 제한	중
	CU-04	root 권한으로 서버 구동 제한	상
	CU-05	환경설정 파일 접근 권한	중
	CU-06	demodb 제거	상
	CU-07	안전한 암호화 알고리즘 사용	상
다. 패치 및 로그관리	CU-08	로그 활성화	하
	CU-09	최신 패치 적용	상

[표 6] Cubrid 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">CU-01. 불필요한 계정 제거</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 계정 중 비인가 계정, 퇴사자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 생성, 읽기, 갱신, 삭제(CRUD) 등을 할 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DB 설치 시 생성되는 기본 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DB 설치 시 생성되는 기본 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 사용자 계정 목록 조회
csql> SELECT name, password FROM db_user;
 
▪ 웹 매니저 계정 목록 조회
cd $CUBRID/conf/
cat cmdb.pass
cat cm.pass
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 불필요한 계정 삭제
csql> DROP USER '삭제할 계정';
 
▪ 웹 매니저 계정 삭제
1) 웹페이지(http://IP:8001)로 접속 후 admin 계정으로 로그인
2) main(홈)에 Users > 해당 계정 삭제</td></tr>
</table>

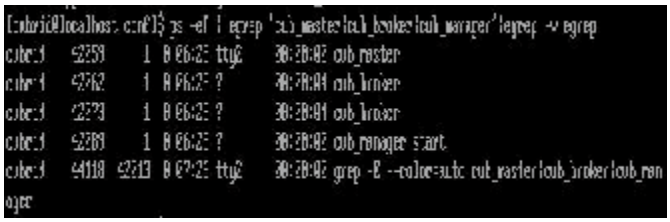
	※ 열린 계정 목록 중 불필요한 계정(인가되지 않은 계정, 퇴직자 계정 등 담당자가 실질적인 업무에 필요없다고 판단하는 계정)은 삭제 또는 잠금/만료 설정 ※ DB 연결/접근 시에는 가능한 시스템 계정 사용은 지양하고 일반계정에 최소권한을 부여하여 사용하기를 권고
비고	

<table>
<tr><td>진단항목</td><td colspan="2">CU-02. 취약한 패스워드 사용제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드가 계정명과 동일하거나 Default 패스워드를 사용하는 경우 비인가자가 쉽게 데이터베이스에 접근할 위험이 있고, 접근 시 데이터베이스 삭제, 변경 등의 심각한 침해 사고를 일으킬 가능성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">계정명과 같거나, 추측 가능한 패스워드를 사용하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">계정명과 같거나, 추측 가능한 패스워드를 사용하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 사용자 계정의 취약한 패스워드 사용 여부 점검
csql> SELECT name, password FROM db_user;
 
csql> SELECT * FROM db_password;
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 영어/숫자/특수문자를 혼용하여 8자리 이상으로 변경 필요.
영어/숫자/특수문자 3종류를 혼용하여 8자리 이상 또는 2종류를 혼용하여 10자리 이상
▪ 패스워드 관리 적용
패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(KISA 암호 알고리즘 및 키 길이 이용 안내서 참고)
▪ 패스워드 변경기능 구현
사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공 패스워드 설정은 다음과 같은 방법으로 가능
csql> alter user 변경할 계정 password '변경할 패스워드';
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

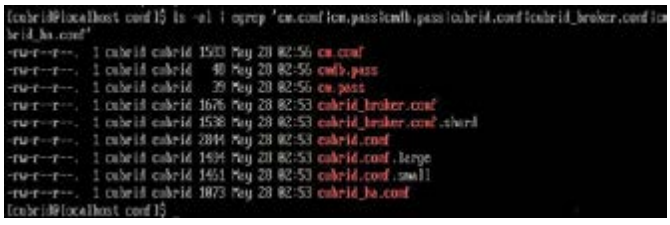
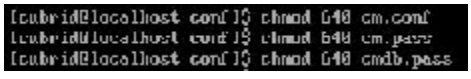
나. 권한 관리

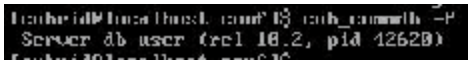
<table>
<tr><td>진단항목</td><td colspan="2">CU-03. 타사용자에 권한 부여 옵션 사용제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">With grant option과 함께 권한을 받은 사용자는 해당 권한을 다른 사용자에게 grant 할 수 있다. 그러므로, 다른 object의 사용권한 부여는 DBA만 할 수 있도록 제한해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">grant_priv 권한이 적절한 사용자에게 부여되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">grant_priv 권한이 적절하지 않은 사용자에게 부여되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ grant_priv을 부여 받은 사용자 조회
csql> SELECT * FROM db_auth WHERE is_grantable='YES';
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 필요한 옵션일 경우 with grant option을 제외하고 권한 재부여
1) csql> grant 특정권한 on 테이블 to 계정;
ex) grant select on test1 to nobiz;
 

▪ 불필요한 권한일 경우
1) csql> revoke 특정권한 on 테이블 from 계정;
ex) revoke select on test1 from nobiz;
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단 항목</td><td colspan="2">CU-04. root 권한으로 서버 구동 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">root 권한은 데이터베이스의 최고 상위 권한으로 소수의 관리자만이 제한적으로 사용되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DBMS가 root 계정 또는 root 권한으로 구동되고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">DBMS가 root 계정 또는 root 권한으로 구동되고 있을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ cub_master/cub_broker/cub_manager 데몬이 root 계정 또는 root 권한으로 구동되고 있는지 확인
- 실행중인 프로세스를 통해 확인
ps -ef | egrep 'cub_master|cub_broker|cub_manager' | egrep –v egrep
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ cubrid 계정으로 재설치 후 같은 DB를 생성 후에 언로드 / 로드를 통해 기존 데이터를 이관</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">CU-05. 환경설정 파일 접근 권한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Cubrid 중요 파일 중 하나인 환경설정 파일의 변경으로 인한 시스템 장애 발생이 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">환경설정 파일 접근 권한이 640(rw-r-----) 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">환경설정 파일 접근 권한이 640(rw-r-----) 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 환경설정파일 : cm.conf, cm.pass, cmdb.pass, cubrid.conf, cubrid_broker.conf, cubrid_ha.conf

▪ 환경설정 파일 접근 권한 확인
cd $CUBRID설치경로/CUBRID/conf
ls –al | egrep ‘cm.conf|cm.pass|cmdb.pass|cubrid.conf|cubrid_broker.conf|cubrid_ha.conf’
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 환경설정 파일의 접근 권한을 640 이하로 설정
chmod 640 환경설정파일
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">CU-06. DEMODB 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Cubrid 설치시 자동으로 설치되는 Demo 데이터베이스를 구동 중일 경우 불필요한 자원을 낭비하게되며, 해당 데이터베이스를 사용하여 데이터를 저장할 경우 공격자에 의해 해당 데이터베이스의 데이터가 탈취될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">demodb가 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">demodb가 구동중이거나 설치되어 있을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 데이터베이스 운영 여부 확인
cub_commdb –P (중지가 되어있을 경우 나타나지 않음)
 
▪ 설치되어 있는 데이터베이스 확인
cat [Cubrid 설치경로]/CUBRID/databases/databases.txt
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 데이터베이스 삭제
cubrid deletedb demodb
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	CU-07. 안전한 암호화 알고리즘 사용		취약도	상
항목설명	SHA-1의 취약점이 발견됨에 따라 SHA-1은 더 이상 안전한 알고리즘이 아니다. 따라서 SHA-256 이상의 암호화 알고리즘을 사용해야 한다.			
진단기준	양호	해시 알고리즘 SHA-256 이상을 사용하고 있는 경우		
	취약	해시 알고리즘 SHA-256 미만을 사용하고 있는 경우		
진단방법	▪ 수동 점검 1) 패스워드 저장 시 사용하는 해시 알고리즘 확인			
조치방법	▪ 수동 조치 1) 패스워드 저장 시 SHA-256 이상의 해시 알고리즘으로 암호화하여 저장			
비고				

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">CU-08. 로그 활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">로그 기능을 수행할 수 있게 설정함으로써 사용자에 의한 문장에 대한 감사, 권한에 대한 감사, 객체에 대한 감사를 수행할 수 있다. 또한, 침해사고 및 장애 시 로그 자료를 분석하여 정확한 분석을 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로그 기능이 활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로그 기능이 비활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ $CUBRID설치경로/CUBRID/conf/cubrid_broker.conf에서 로그 기능 활성화 여부 확인
cat cubrid_broker.conf | grep 'SQL_LOG' -B 8
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 로그 기능 활성화
vi $CUBRID설치경로/CUBRID/conf/cubrid_broker.conf
'SQL_LOG = ON'을 추가</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	CU-09. 최신 패치 적용		취약도	상
항목설명	버그 또는 알려진 취약점으로 인한 침해사고가 발생할 수 있다. 따라서 주기적으로 최신 패치를 적용하여 취약점을 제거해야 한다.			
진단기준	양호	최신 버전 및 취약점이 존재하지 않는 버전 패치가 되어있는 경우		
	취약	최신 버전 및 취약점이 존재하지 않는 버전 패치가 되어있지 않은 경우		
진단방법	▪ Cubrid 버전 확인 후 최신 패치 적용 여부 확인 # cubrid_rel 			
조치방법	▪ 데이터베이스에 대한 최신의 버전을 확인 후 업그레이드 및 패치 수행 큐브리드 공식 홈페이지 : https://www.cubrid.com/			
비고	▪ 시스템 업데이트는 영향도를 산정하여 진행하여야 함			

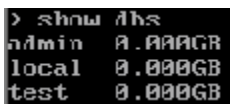
2.7. MongoDB

계정 관리(4개 항목), 접근제어 및 서비스 관리(3개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	MG-01	불필요한 데이터베이스 및 테이블 제거	상
	MG-02	불필요한 계정 제거	상
	MG-03	데몬 실행 시 인증 옵션 사용	상
	MG-04	관리자 계정 생성 여부	상
나. 접근제어 및 서비스 관리	MG-05	주요 실행 및 설정 파일 권한 관리	중
	MG-06	http interface 접근 통제	중
	MG-07	데이터베이스 접근 제한 설정	상
다. 패치 및 로그 관리	MG-08	데이터베이스에 대해 최신 보안패치와 벤더 권고사항 적용 여부	상
	MG-09	데이터베이스의 접근, 변경, 삭제 감사 기록 및 백업	상

[표 7] MongoDB 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">MG-01. 불필요한 데이터베이스 및 테이블 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용하지 않는 데이터베이스(collection)가 존재하면 해당 데이터베이스 및 collection의 관리 미흡으로 인한 알려진 취약점에 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">운영에 불필요한 데이터베이스, collection이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">운영에 불필요한 데이터베이스, collection이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 존재하는 데이터베이스 확인
> show dbs
 
■ 존재하는 collection 확인
1) 해당 데이터베이스에 접근해서 show collections로 확인
> show collections
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 불필요한 데이터베이스 삭제
1) > use [해당 DB명]
2) > db.dropDatabase();
 
■ 불필요한 collection 삭제
1) > use [해당 DB명]
2) > db.[collection명].drop();</td></tr>
</table>

	 > use admin switched to db admin > db.test.drop(); true > show collections system.users system.version
비고	

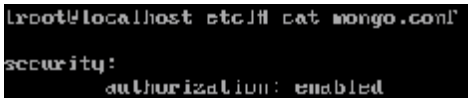
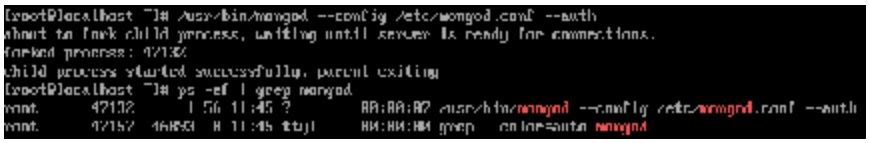
진단항목	MG-02. 불필요한 계정 제거	취약도	상
항목설명	사용하지 않는 데이터베이스 계정이 존재하면 해당 계정의 관리 미흡으로 인한 비인가된 사용자가 접근할 위험이 존재한다,		
진단기준	양호	운영에 불필요한 계정이 존재하지 않는 경우	
	취약	운영에 불필요한 계정이 존재하는 경우	
진단방법			

■ 존재하는 계정 확인

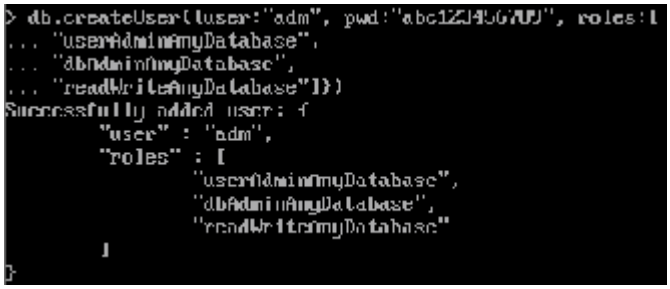
> use admin

> show users

조치방법	▪ 불필요한 계정 삭제 > db.removeUser("[계정명]") //이전버전(실행은 되나 경고문구가 뜸)  > db.dropUser("[계정명]") //현재버전 
비고	

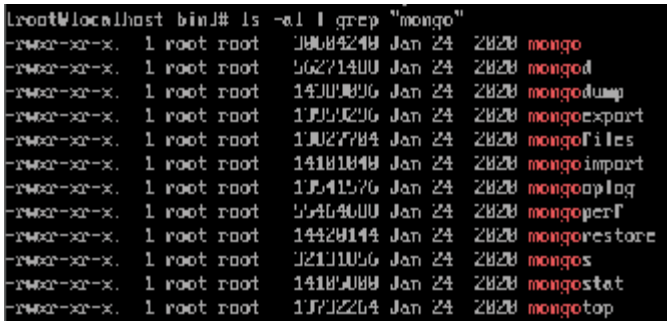
<table>
<tr><td>진단항목</td><td colspan="2">MG-03. 데몬 실행시 인증 옵션 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">MongoDB의 실행 데몬인 mongod를 실행할 때, 인증을 사용하는 옵션을 함께 사용하지 않으면 인증없이 접근이 가능하게 되므로 비인가된 사용자가 데이터베이스에 접근하여 악의적인 행위를 할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">데몬 또는 conf파일에 auth가 명시되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">데몬 또는 conf파일에 auth가 명시되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ mongod 데몬 확인
1) 옵션에서 --auth가 존재하는지 확인
ps –ef | grep mongodb
 
▪ conf 파일 확인
1) 옵션에서 security:authorization:enable 또는 auth=true가 존재하는지 확인(버전별 상이)
cat mongo.conf
 
cat mongodb.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ mongod 데몬에 auth 옵션 추가
1) mongod 데몬 종료
kill –9 [mongod pid]
 
2) --auth 옵션 설정 후 데몬 구동
/usr/local/mongodb/bin/mongod --config/usr/local/mongodb/conf/mongodb.conf --auth
  </td></tr>
</table>

	■ conf 파일에 추가 # vi mongo.conf(관리자마다 파일이름이 상이할 수 있음) security : authorization: enabled 또는 auth = true
비고	

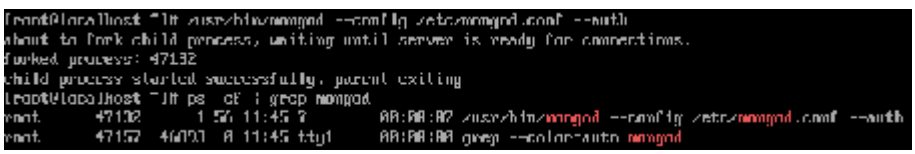
<table>
<tr><td>진단항목</td><td colspan="2">MG-04. 관리자 계정 생성 여부</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자 계정이 없으면 인증없이 데이터베이스에 접근하거나 database 서버를 임의로 종료시키는 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">관리자 계정이 생성되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">관리자 계정이 생성되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 관리자 계정 확인
> use admin
> show users
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 관리자 계정 생성
> use admin
> db.createUser({ user: "<username>", pwd: "<password>", roles: ["userAdminAnyDatabase", "dbAdminAnyDatabase", "readWriteAnyDatabase"]})
  </td></tr>
</table>

	 > show users { "_id" : "admin.adm", "userId" : BinData(4,"UUFyUDMFUMSD2UKwgYUUgg=="), "user" : "adm", "db" : "admin", "roles" : [{ "role" : "userAdminAnyDatabase", "db" : "admin" }, { "role" : "dbAdminAnyDatabase", "db" : "admin" }, { "role" : "readWriteAnyDatabase", "db" : "admin" }] }
비고	

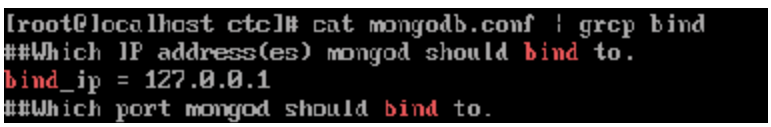
나. 접근제어 및 서비스 관리

<table>
<tr><td>진단항목</td><td colspan="2">MG-05. 주요 실행 및 설정 파일 권한 관리</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">실행 파일로 이루어진 파일은 전체시스템 손상을 방지하기 위해 별도의 계정이나 관리자가 소유해야하며, others 권한에 읽기, 쓰기, 실행 권한을 제거하여 임의의 실행 및 정보탈취의 위험으로부터 보호하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">해당 실행파일 및 설정파일의 소유자 및 그룹이 별도의 계정의 소유여야 하며, 파일의 권한이 750 이하일 경우</td></tr>
<tr><td>취약</td><td colspan="3">해당 실행파일 및 설정파일 소유자 및 그룹이 별도의 계정의 소유가 아니거나, 파일의 권한이 750 초과일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 실행파일 권한 확인
ls –al | grep “mongo”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 별도의 계정으로 변경 후 others에 실행 권한 제거
chown dba:dba [file 명]
chmod 750 [file 명]
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

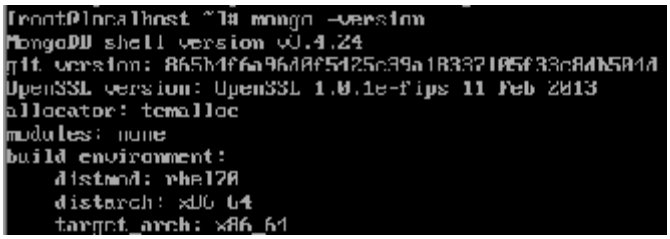
<table>
<tr><td>진단항목</td><td colspan="2">MG-06. http interface 접근 통제</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">http interface에 접근 제한이 설정되어 있지 않으면 누구나 http interface를 통해 MongoDB를 모니터링할 수 있어 해당 정보를 통해 제 2차 공격에 정보수집으로 이용될 위험이 존재한다.

※ http://주소:포트번호 > 포트번호는 mongod DB 인스턴트가 사용하는 port 번호에 +1000으로 설정됨</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">해당 http://주소:포트번호로 접근했을 때, 인증창이 활성화된 경우</td></tr>
<tr><td>취약</td><td colspan="3">해당 http://주소:포트번호로 접근했을 때, 인증없이 바로 모니터링이 가능한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ http://주소:포트번호로 확인
해당 http서비스를 사용하고 있는지 확인 필요
<table><tr><th>인증이 되어 있지 않을 경우의 화면</th><th>설정이 되어 있을 경우</th></tr><tr><td>  </td><td>  </td></tr></table></td></tr>
<tr><td>조치방법</td><td colspan="4">▪ mongod 데몬에 auth 옵션 추가
1) mongod 데몬 종료
kill –9 [mongod pid]
 
2) --auth 옵션 설정 후 데몬 구동
/usr/local/mongodb/bin/mongod --config/usr/local/mongodb/conf/mongodb.conf --auth
 
▪ conf 파일에 추가</td></tr>
</table>

	# vi mongo.conf(관리자마다 파일이름이 상이할 수 있음) security : authorization: enabled 또는 auth = true
비고	

<table>
<tr><td>진단항목</td><td colspan="2">MG-07. 데이터베이스 접근 제한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">접근 제한이 설정되어 있지 않으면 비인가된 사용자가 해당 데이터베이스에 접근하여 무차별 대입 공격을 통해 DBA 권한을 획득하여 데이터베이스를 조작할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인가된 IP만 접근가능하도록 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">비인가된 IP가 접근 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ conf 파일에서 확인
cat [설치위치]/conf/mongodb.conf | grep bind
 
▪ Linux의 경우 iptables로 확인
iptables -L</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ conf파일에 bind_ip에 인가된 ip 설정
ex)
bind_ip = 127.0.0.1, 172.30.1.23
 
▪ Linux의 경우 iptables 설정</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">MG-08. 데이터베이스에 대해 최신 보안패치와 벤더 권고사항 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 주요한 보안 패치 등을 설치하지 않은 경우, 데이터베이스의 자체의 취약점에 노출되어 공격자가 데이터베이스 손상 및 비인가된 접근을 할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 버전을 사용하고 있거나 최신 보안패치 및 벤더의 권고사항을 적용하고 있거나 패치가 공표되었을 때 회의록을 통해 적용여부를 결정</td></tr>
<tr><td>취약</td><td colspan="3">최신 보안패치가 발표되었으나 이에 대한 검토를 하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령어를 통해 확인
mongo –version 또는 > db.version()
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 수동 조치
최신 버전이 아닐 경우 최신버전으로 업데이트 권고. 호환성의 문제로 업데이트가 불가능할 경우, 벤더사에서 권고한 보안 패치를 따로 적용하여야 함
<table><tr><th>버전</th><th>출시날짜</th><th>만료날짜</th></tr><tr><td>4.4</td><td>2020. 07</td><td>-</td></tr><tr><td>4.2</td><td>2019. 08</td><td>-</td></tr><tr><td>4.0</td><td>2018. 06</td><td>2022. 01</td></tr><tr><td>3.6</td><td>2017. 11</td><td>2021. 04</td></tr><tr><td>3.4</td><td>2016. 11</td><td>2020. 01</td></tr><tr><td>3.2</td><td>2015. 12</td><td>2018. 09</td></tr><tr><td>3.0</td><td>2015. 03</td><td>2018. 02</td></tr></table>https://www.mongodb.com/try/download</td></tr>
<tr><td>비고</td><td colspan="4">시스템 업데이트는 영향도를 산정하여 진행하여야 함</td></tr>
</table>

진단항목	MG-09. 데이터베이스의 접근, 변경, 삭제 감사 기록 및 백업		취약도	상
항목설명	데이터베이스의 감사기록이 기관에서 정의한 감사 기록 정책에 적합하도록 설정되어 있어야 하며, 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립하여야 한다.			
진단기준	양호	감사 로그 기록을 기관 정책에 맞게 시행하고 있으며, 백업 정책대로 주기적으로 백업을 하고 있는 경우		
	취약	감사 로그 기록과 관련된 정책이 존재하지 않거나 정책대로 시행하고 있지 않거나 백업 정책 및 시행을 하고 있지 않은 경우		
진단방법	▪ 수동점검 1) 로그 설정 및 백업 설정에 대해 해당 DBA와 인터뷰 실시 2) 담당자와 인터뷰를 통해 주기적인 백업 여부 점검 3) ls –l dbpath ([설치파일]/conf/conf파일에 dbpath 확인)			
조치방법	▪ 수동조치 1) 로그 감사 정책 및 주기적인 백업 절차를 수립 2) DBMS의 유지보수 및 upgrade 작업 시에는 전체 full 백업 절차 수립(권고) 3) 로그 감사 설정 및 주기적인 백업 설정			
비고				

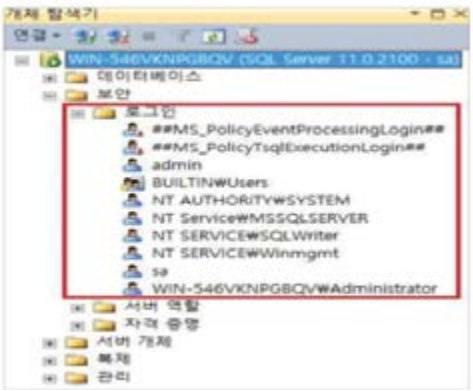
2.8. MS-SQL

계정 관리(4개 항목), 보안 설정(2개 항목), 패치 및 로그관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	DS-01	불필요한 계정 제거	상
	DS-02	SYSADMIN 권한 제한	상
	DS-03	SA 계정 패스워드 관리	상
	DS-04	guest 계정 사용 제한	중
나. 보안 설정	DS-05	Registry Procedure Permission 제한	중
	DS-06	xp_cmdshell 사용 제한	상
다. 패치 및 로그관리	DS-07	로그 활성화	하
	DS-08	최신 패치 적용	상

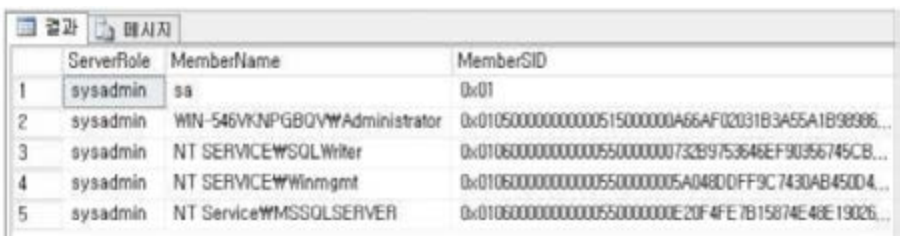
[표 8] DBMS(MS-SQL) 진단 체크리스트

가. 계정 관리

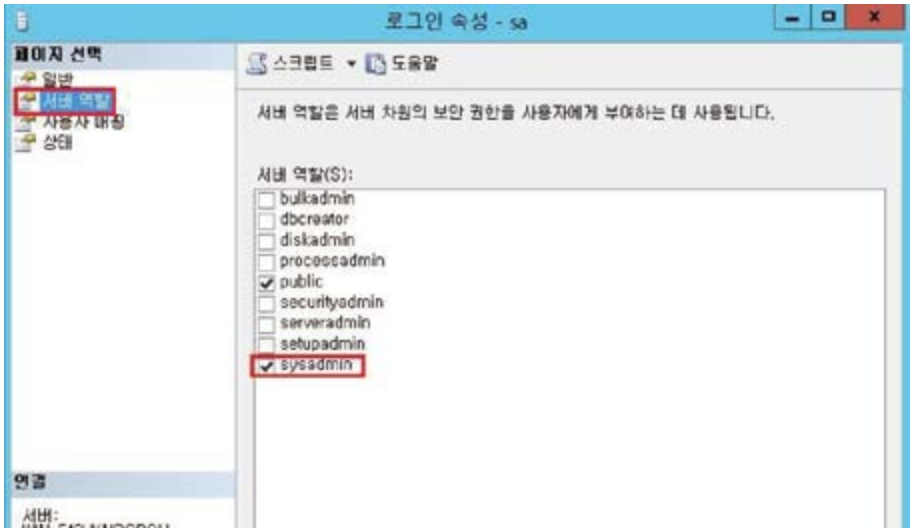
<table>
<tr><td>진단항목</td><td colspan="2">DS-01. 불필요한 계정 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 쿼리문을 통해 확인
sql> SELECT name, dbname FROM syslogins
▪ 개체탐색기를 통해 불필요한 계정 삭제
Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 보안 > 로그인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 새 쿼리를 통해 불필요한 계정 삭제
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) DROP login <login_user_name>

▪ 개체탐색기를 통해 불필요한 계정 삭제
1) Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 보안 > 로그인
2) 해당 계정 오른쪽 마우스 > 삭제 > 확인</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DS-02. SYSADMIN 권한 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">sysadmin(System administrators)의 역할은 sql 서버와 설치된 데이터베이스에 대해서 완전한 관리 권한을 필요로 하는 사용자를 위해 만들어진 역할로써 이 역할의 구성원은 sql서버에서 모든 작업을 수행할 수 있어 비 인가된 사용자가 해당 역할의 구성원으로 등록되어 있을 경우, 데이터베이스에 직접적인 공격이 가능한 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">sysadmin 서버 role의 멤버 목록을 확인 후 해당 서버 role에 불필요한 멤버가 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">sysadmin 서버 role의 멤버 목록을 확인 후 해당 서버 role에 불필요한 멤버가 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ sysadmin 역할 구성원 확인

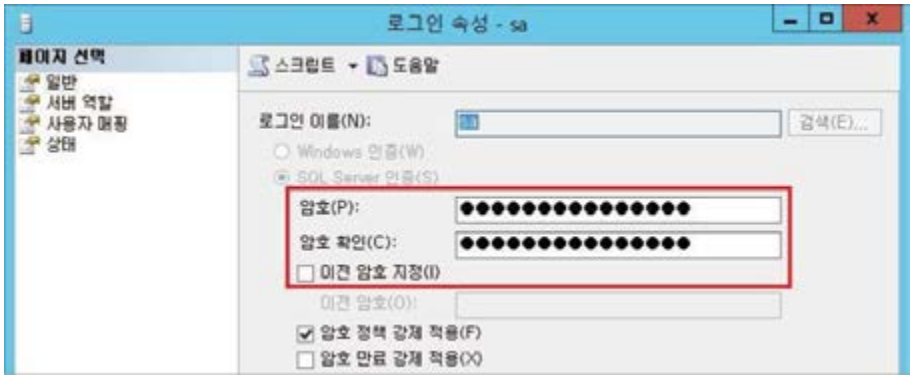
■ 새 쿼리를 통해 확인
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) sql> SELECT name, type_desc, is_disabled, create_date
FROM sys.server_principals
WHERE type IN ('S', 'U', 'R') -- SQL_LOGIN, WINDOWS_LOGIN, SERVER_ROLE
AND IS_SRVROLEMEMBER('sysadmin', name) = 1
ORDER BY name
GO
또는
sql> sp_helpsrvrolemember 'sysadmin'
 
결과 메시지
ServerRole | MemberName | MemberSID
1 sysadmin | sa | 0x01
2 sysadmin | WIN-546VKNPGBQV₩Administrator | 0x0105000000000005150000000A66AF02031B3A55A1B98986...
3 sysadmin | NT SERVICE₩SQLWriter | 0x0106000000000005500000007328975364BEF90356745CB...
4 sysadmin | NT SERVICE₩Winmgmt | 0x0106000000000005500000005A048DDFF9C7430AB450D4...
5 sysadmin | NT Service₩MSSQLSERVER | 0x0106000000000005500000000E20F4FE7B15874E48E19026...

■ 개체 탐색기를 통해 확인
1) Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 보안 >로그인
2) 계정 별 오른쪽 마우스 속성 > Server Roles에서 확인</td></tr>
</table>

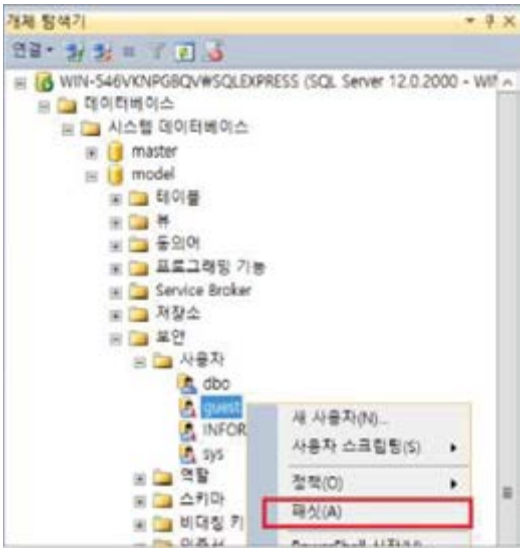
	
조치방법	1. 새 쿼리를 통해 불필요한 계정 삭제 1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리 2) EXEC sp_droprolemember '<member_name>', 'sysadmin' 2. 개체탐색기를 통해 불필요한 계정 삭제 1) Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 보안 > 로그인 2) 계정 별 오른쪽 마우스 속성 > Server Roles에서 sysadmin 권한 체크 해제 후 확인
비고	

<table>
<tr><td>진단항목</td><td colspan="2">DS-03. SA 계정 패스워드 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">sa계정의 경우, MS-SQL 설치 시 디폴트로 존재하는 계정이며 sysadmin 권한을 가지고 있는 계정이다. 해당 계정에 패스워드가 존재하지 않을 경우, 악의적인 사용자가 해당 계정을 통해 데이터베이스의 모든 권한을 행할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">sa 계정에 대한 패스워드가 NULL 값이 아닌 경우</td></tr>
<tr><td>취약</td><td colspan="3">sa 계정에 대한 패스워드가 NULL 값인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 쿼리문을 통해 확인
sql> SELECT count(name) FROM syslogins WHERE password is null AND name='sa' // sa 계정의 패스워드가 Null인 경우
또는
sql> SELECT name, password FROM syslogins WHERE password is null</td></tr>
<tr><td>조치방법</td><td colspan="4">※ sa 패스워드 설정 변경

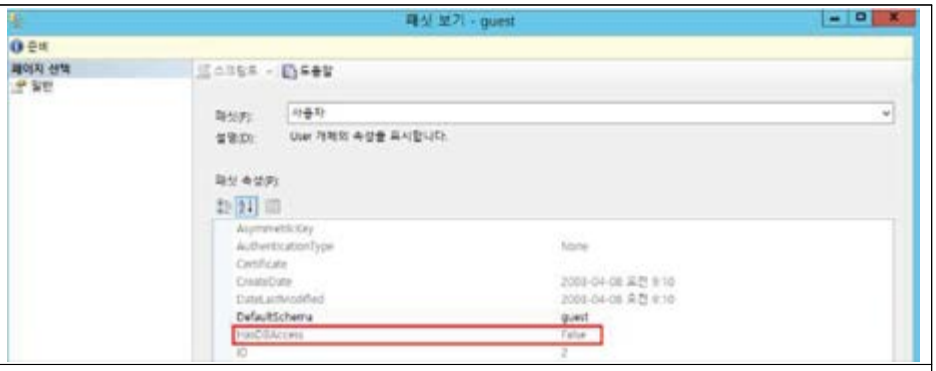
■ 새 쿼리를 통해 변경
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) ALTER LOGIN sa WITH password='<new_passwd>';

■ 개체탐색기를 통해 변경
1) Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 보안 > 로그인
2) sa 오른쪽 마우스 속성 > 일반 > 암호에서 변경 후 확인
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DS-04. guest 계정 사용 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">guest 계정은 특별한 로그인 계정으로 SQL 모든 사용자가 guest의 권한으로 접근할 수 있게 하는 계정이다. 비 인가된 사용자의 접근을 허가하므로 데이터베이스에 guest권한을 제거하여야 한다.

※ 이 계정은 masterDB와 TempDB에 디폴트로 설정되어 있으며, 해당 DB들에 Guest 계정 삭제가 불가능함</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">데이터베이스에 불필요한 guest 권한이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">데이터베이스에 불필요한 guest 권한이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 데이터베이스에 부여된 guest 계정 확인
1) Microsoft SQL Server Management Studio(관리자) > 개체 탐색기 > 데이터베이스
2) [데이터베이스]별 > 보안 > 사용자 > guest > 마우스 오른쪽 패싯
 

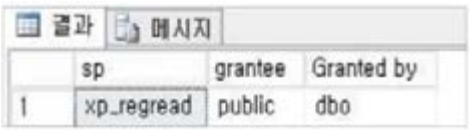
3) 패싯 속성에서 HasDBAccess 설정이 false 인지 확인</td></tr>
</table>

	
조치방법	■ 데이터베이스에 부여된 guest 계정 비활성화 1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리를 통해 변경 2) use[해당 데이터베이스] 3) revoke connect from guest
비고	

나. 보안 설정

<table>
<tr><td>진단항목</td><td colspan="2">DS-05. Registry Procedure Permission 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">레지스트리 확장 저장 프로시저를 이용하면 Windows 레지스트리에 액세스할 수 있다. 레지스트리에는 SQL에 대한 구성 정보가 들어있으며 원격 또는 로컬시스템에 대한 암호가 포함되어 있을 수 있으므로 악의적인 사용자가 windows 레지스트리에 서버 및 데이터베이스에 손상 및 비 인가된 접근을 할 위험이 존재한다.

※ 시스템 확장 저장 프로시저 제한 목록
<table>
<tr><td>sys.xp_regaddmultistring</td><td>sys.xp_regdeleteky</td><td>sys.xp_regdeletevalue</td></tr>
<tr><td>sys.xp_regenumvalues</td><td>sys.xp_regread</td><td>sys.xp_regremovemultistring</td></tr>
<tr><td>sys.xp_regwrite</td><td></td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Registry extended stored procedure 프로시저의 사용권한('execute')이 DBA외 guest/public에게 부여되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">Registry extended stored procedure 프로시저의 사용권한('execute')이 DBA외 guest/public에게 부여되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 새 쿼리를 통해 프로시저 확인
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) select object_name(id) AS sp, user_name(uid) AS grantee, user_name(grantor) AS 'Granted by'FROM sysprotects WHERE object_name(id) LIKE '%xp_reg%'

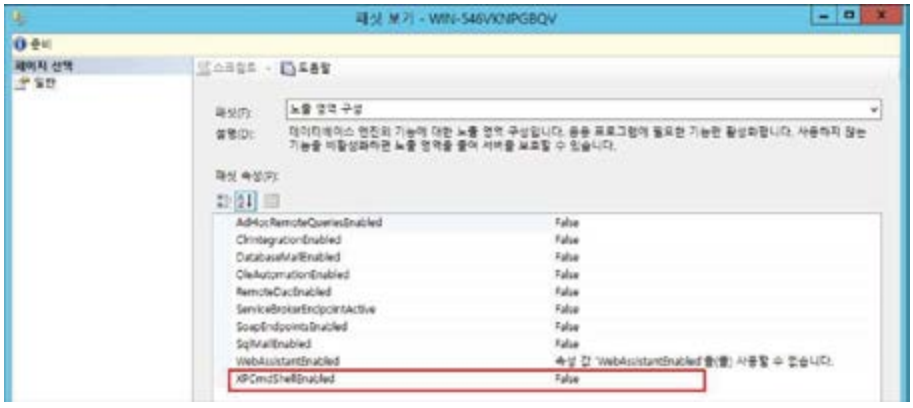
■ Management Studio에서 확인
1) 개체탐색기 > 데이터베이스 > 시스템 데이터베이스 > master > 프로그래밍 기능 > 시스템 확장 저장 프로시저
2) sys.xp_regaddmultistring, sys.xp_regdeletekey, sys.xp_regdeletevalue, sys.xp_regenumvalues, sys.xp_regread, sys.xp_regremovemultistring, sys.xp_regwrite> 속성
3) 사용권한 > public의 실행 권한 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">※ 시스템 확장 저장 프로시저에서 public 권한이 설정되어 있는 프로시저 제거

■ 새 쿼리를 통해 프로시저 확인
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리</td></tr>
</table>

	2) use master 3) revoke <permission> on object :: <시스템 확장 저장 프로시저명> to public; ■ Management Studio에서 프로시저 확인 1) 개체탐색기 > 데이터베이스> 시스템 데이터베이스 > master > 프로그래밍 기능 > 시스템 확장 저장 프로시저 2) sys.xp_regaddmultistring, sys.xp_regdeletekey, sys.xp_regdeletevalue, sys.xp_regenumvalues, sys.xp_regread, sys.xp_regremovemultistring, sys.xp_regwrite> 속성 3) 사용권한 > public의 실행 권한 제거 
비고	

<table>
<tr><td>진단항목</td><td colspan="2">DS-06. xp_cmdshell 사용 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">서버의 유지 관리를 위해 MS-SQL에서 제공하고 있는 확장 프로시저 중, 자주 해킹에 이용되고 있는 특정 프로시저를 제거한다. 특히 xp_cmdshell은 중국에서 제작된 해킹 툴에서 자주 이용되고 있으므로 불필요한 경우 반드시 제거하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">xp_cmdshell 사용을 제한한 경우</td></tr>
<tr><td>취약</td><td colspan="3">xp_cmdshell 사용을 제한하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 쿼리문으로 확인
sql> select count(name) from sysobjects where name = 'xp_cmdshell'
// 0이면 양호

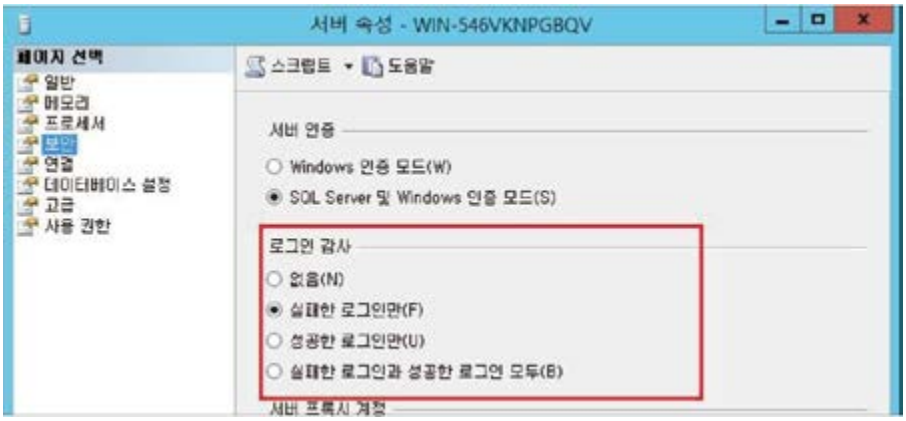
■ 새 쿼리를 통해 프로시저 확인
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) SELECT name, value FROM sys.configurations WHERE name = 'xp_cmdshell'
※ *값이 0일 경우, false로 설정된 것이므로 양호함
 

■ 개체탐색기를 통해 프로시저 확인
Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 컴퓨터이름 > 오른쪽 마우스 > 패싯 > 일반 > XPCmdShellEnabled 값이 False인지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">※ XPCmdShellEnabled 설정 제한</td></tr>
</table>

	■ 새 쿼리를 통해 프로시저 확인 1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리 2) EXEC sp_configure 'xp_cmdshell', 0 ■ 개체탐색기를 통해 프로시저 확인 Microsoft SQL Server Management Studio(관리자) > 개체탐색기 > 컴퓨터이름 > 오른쪽 마우스 > 패싯 > 일반 > XPCmdShellEnabled 값을 false로 설정
비고	※ EXEC sp_configure 'xp_cmdshell' 쿼리 실행 시 다음과 같은 에러가 출력된다면 이 문제는 sp_configure 저장 프로시저의 업데이트 허용 매개 변수가 1로 설정된 경우 발생한다. 이 문제를 해결하려면 업데이트 허용 매개 변수를 0으로 설정 한다. 1. EXEC sp_configure 'xp_cmdshell' 쿼리 실행 '시스템 카탈로그에 대한 임의 업데이트는 지원되지 않습니다. 2. SELECT * FROM sys.configurations WHERE name = 'allow updates' 3. allow updates 의 설정값이 1로 되어있을 경우 아래의 스크립트를 실행하여 0으로 변경한다. EXEC sp_configure 'allow updates', '0' go RECONFIGURE WITH OVERRIDE go EXEC sp_configure 'show advanced options', 1 go RECONFIGURE

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">DS-07. 로그 활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 감사기록이 기관에서 정의한 감사기록 정책에 적합하도록 설정되어 있어야 하며, 데이터베이스는 데이터, 로그와 응용프로그램에 대한 백업 정책을 수립하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">감사 로그 기록을 기관 정책에 맞게 시행하고 있으며, 백업 정책대로 주기적으로 백업을 하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">감사 로그 기록과 관련된 정책이 존재하지 않거나 정책대로 시행하고 있지 않거나 백업 정책 및 시행을 하고 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 로그 설정 확인 후 DBA와 인터뷰 실시 (로그, 백업 설정 및 주기 확인)

▪ 개체 탐색기에서 확인
1) Microsoft SQL Server Management Studio(관리자) > 개체 탐색기 > 컴퓨터이름 > 오른쪽 마우스
2) 속성 > 보안 > 로그인 감사 > 설정 유무 확인
3) 실패, 성공, 실패/성공 모두 중 하나만 선택되어 있으면 양호
 

▪ 수동 점검
1) 로그 감사 정책 및 주기적인 백업 절차를 DBA와 인터뷰</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 수동 조치
1) 로그 감사 정책 및 주기적인 백업 절차를 수립
2) DBMS의 유지보수 및 Upgrade 작업 시에는 전체 full 백업 절차 수립(권고)</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DS-08. 패치 및 로그 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 주요한 보안 패치 등을 설치하지 않은 경우, 데이터베이스 자체의 취약점에 노출되어 공격자가 데이터베이스 손상 및 비 인가된 접근을 할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 버전을 사용하고 있거나 최신 보안패치 및 벤더의 권고사항을 적용하고 있거나 패치가 공표되었을 때 회의록을 통해 적용 여부를 결정한 증적을 보유하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 보안패치가 발표되었으나 아무 행위도 하지 않는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 새 쿼리를 통해 현재 버전 확인
1) Microsoft SQL Server Management Studio(관리자) > 새 쿼리
2) select @@version
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 수동 조치
1) 최신버전 및 벤더사가 권고한 보안 패치 업데이트
<table><tr><th>서버 버전</th><th>Service Pack</th></tr><tr><td>SQL Server 2012</td><td>SP4-</td></tr><tr><td>SQL Server 2014</td><td>SP3</td></tr><tr><td>SQL Server 2016</td><td>SP2</td></tr><tr><td>SQL Server 2017</td><td>-</td></tr><tr><td>SQL Server 2019</td><td>-</td></tr></table></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

2.9. My-SQL

계정 관리(4개 항목), 보안 설정(3개 항목), 패치 및 로그관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	DY-01	불필요한 계정 제거	중
	DY-02	취약한 패스워드 사용 제한	상
	DY-03	타 사용자에 권한 부여 옵션 사용 제한	중
	DY-04	DB 사용자 계정 정보 테이블 접근 권한	중
나. 보안 설정	DY-05	root 권한으로 서버 구동 제한	상
	DY-06	환경설정 파일 접근 권한	중
	DY-07	안전한 암호화 알고리즘 사용	상
다. 패치 및 로그관리	DY-08	로그 활성화	하
	DY-09	최신 패치 적용	상

[표 9 MySQL 진단 체크리스트

가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">DY-01. 불필요한 계정 제거</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 사용자 계정 목록 조회
mysql> USE mysql;
mysql> SELECT host, user FROM user;</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 불필요한 계정 삭제
mysql> Delete from user where user='삭제할 계정';</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	DY-02. 취약한 패스워드 사용제한		취약도	상
항목설명	패스워드가 계정명과 동일하거나 Default 패스워드를 사용하는 경우 비 인가자가 쉽게 데이터베이스에 접근할 위험이 있고, 접근 시 데이터베이스 삭제, 변경 등의 심각한 침해 사고를 일으킬 가능성이 있다.			
진단기준	양호	기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있는 경우		
	취약	기관 정책에 맞게 패스워드 복잡도 설정이 적용되어 있지 않은 경우		
진단방법	■ 사용자 계정의 취약한 패스워드 사용 여부 점검 - 사용자 계정과 패스워드가 동일한지 여부 조회 mysql> USE mysql; mysql> SELECT host, user FROM user WHERE password=password(user); - 사용자 계정의 패스워드가 Null인지 여부 조회 mysql> USE mysql; mysql> SELECT host, user FROM user WHERE password=''';			
조치방법	■ 패스워드 설정 규칙 적용 패스워드 설정 규칙에 맞추어 패스워드를 설정할 수 있도록 시스템 차원에서 기능 제공 ■ 패스워드 관리 적용 패스워드 신규 적용 및 초기화 시 설정 규칙에 맞추어 관리하고, 저장 시에는 일방향 암호 알고리즘을 통한 암호화 처리(One-Way Encryption) ■ 패스워드 변경기능 구현 사용자가 패스워드 설정규칙 내에서 스스로 패스워드를 변경할 수 있도록 기능 제공 패스워드 설정은 다음과 같은 방법으로 가능 mysql> use mysql; mysql> update user set password=password('new password') where user='user name' ; mysql > flush privileges ; 또는 mysql > set password for 'user name'@'%'=password('new password') ; mysql > flush privileges ;			
비고	패스워드 복잡도 설정 : 영어/숫자/특수문자 3종류를 혼용하여 8자리 이상 또는 2종류를 혼용하여 10자리 이상			

나. 보안 설정

<table>
<tr><td>진단항목</td><td colspan="2">DY-03. 타사용자에 권한 부여 옵션 사용제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">With grant option과 함께 권한을 받은 사용자는 해당 권한을 다른 사용자에게 grant 할 수 있다. 그러므로, 다른 object의 사용권한 부여는 DBA만 할 수 있도록 제한해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">grant_priv 권한이 적절한 사용자에게 부여되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">grant_priv 권한이 적절하지 않은 사용자에게 부여되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ grant_priv을 부여 받은 사용자 조회
mysql> USE mysql;
mysql> SELECT host, user, Grant_priv FROM user WHERE Grant_priv='Y';</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 불필요한 grant_priv 권한 제거
1) mysql> USE mysql;
2) mysql> UPDATE user SET grant='N' WHERE user='<M45>';
3) mysql> UPDATE db SET grant_priv='N' WHERE user='<grant 권한을 제거하고자 하는 계정명>';</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DY-04. DB 사용자 계정 정보 테이블 접근 권한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자의 mysql.user 테이블 접근이 허용될 경우, 일반사용자가 DB에 등록되어 있는 사용자 계정 및 패스워드를 알 수 있게 된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DB사용자 계정 정보 테이블의 접근 권한이 적절한 사용자에게 부여되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DB사용자 계정 정보 테이블의 접근 권한이 적절한 사용자에게 부여되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ mysql.user 테이블 접근이 가능한 사용자 조회
mysql> SELECT host, user, select_priv FROM mysql.user;</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 일반 사용자로부터 mysql.user 테이블 모든 접근 권한 제거
mysql> revoke all on mysql.user from '[user name]'@'[hosts]';
mysql> flush privileges
■ 일반 사용자로부터 mysql.user 테이블 접근 권한 제거
mysql> revoke [권한] on mysql.user from [user name] ;
mysql> flush privileges</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DY-05. root 권한으로 서버 구동 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">root 권한은 데이터베이스의 최고 상위 권한으로 소수의 관리자만이 제한적으로 사용되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DBMS가 root 계정 또는 root 권한으로 구동되고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">DBMS가 root 계정 또는 root 권한으로 구동되고 있을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ mysql 데몬이 root 계정 또는 root 권한으로 구동되고 있는지 확인
- 실행중인 프로세스를 통해 확인
ps -ef | grep mysql
- "my.cnf" 파일에서 [mysqld] 그룹의 'user' 지시자의 설정 값 확인
cat /etc/my.cnf | grep user</td></tr>
<tr><td>조치방법</td><td colspan="4">■ “my.cnf” 파일에서 [mysqld] 그룹의 ‘user’ 지시자 설정
- vi /etc/my.cnf
[mysqld]
user=<mysql 데몬을 구동할 시스템의 일반 사용자 계정명></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	DY-06. 환경설정 파일 접근 권한		취약도	중
항목설명	MY-SQL 중요 파일 중에 하나인 환경설정 파일의 변경으로 인한 시스템 장애 발생이 가능하므로, 환경설정 파일에 대한 접근 권한을 제한해야한다.			
진단기준	양호	환경설정 파일 접근 권한이 640(rw-r-----) 이하인 경우		
	취약	환경설정 파일 접근 권한이 640(rw-r-----) 초과인 경우		
진단방법	■ "my.cnf" 파일의 접근 권한 확인 # ls -alL /etc/my.cnf			
조치방법	■ 초기화 파일(my.cnf, my.ini)의 접근 권한을 초기화 파일에 대한 보호를 위하여 600 또는, 640으로 설정 my.cnf 파일 디폴트 위치: /etc/my.cnf, <각 홈 디렉터리>/my.cnf # chmod 600 [my.cnf 파일의 위치]			
비고				

진단항목	DY-07. 안전한 암호화 알고리즘 사용		취약도	상
항목설명	SHA-1의 취약점이 발견됨에 따라 SHA-1은 더 이상 안전한 알고리즘이 아니다. 따라서 SHA-256 이상의 암호화 알고리즘을 사용해야 한다.			
진단기준	양호	해시 알고리즘 SHA-256 이상을 사용하고 있는 경우		
	취약	해시 알고리즘 SHA-256 미만을 사용하고 있는 경우		
진단방법	▪ 수동 점검 1. 패스워드 저장 시 사용하는 해시 알고리즘 확인			
조치방법	▪ 수동 조치 1. 패스워드 저장 시 SHA-256 이상의 해시 알고리즘으로 암호화하여 저장			
비고				

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">DY-08. 로그 활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">로그 기능을 수행할 수 있게 설정함으로써 사용자에 의한 문장에 대한 감사, 권한에 대한 감사, 객체에 대한 감사를 수행할 수 있다. 또한, 침해사고 및 장애 시 로그 자료를 분석하여 정확한 분석을 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로그 기능이 활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로그 기능이 비활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ General log 설정 확인
mysql> show variables like ‘general_log%’;
▪ Slow Query 설정 확인
mysql> show variables like ‘slow%’;
mysql> show variables like ‘log%’;</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ General log 설정
mysql> set global general_log = ON;
mysql> set global general_log = 1;
▪ Slow Query 설정
mysql> set global slow_query_log = ON;
vi /etc/my.cnf
slow_query_log_file= /datadir/serverhostname-slow.log</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	DY-09. 최신 패치 적용		취약도	상
항목설명	버그 또는 알려진 취약점으로 인한 침해사고가 발생할 수 있다. 따라서 주기적으로 최신 패치를 적용하여 취약점을 제거해야 한다.			
진단기준	양호	최신 버전 패치가 되어있는 경우		
	취약	최신 버전 패치가 되어있지 않은 경우		
진단방법	▪ MYSQL 버전 확인 후 최신 패치 적용 여부 확인 mysql> use mysql; mysql> SELECT @@version;			
조치방법	▪ 데이터베이스에 대한 최신의 버전을 확인 후 업그레이드 및 패치 수행 버그 패치 릴리즈 사이트 : http://downloads.mysql.com/archives/ 버그 현황 사이트 : http://bugs.mysql.com/bugstats.php			
비고	시스템 업데이트는 영향도를 산정하여 진행하여야 함			

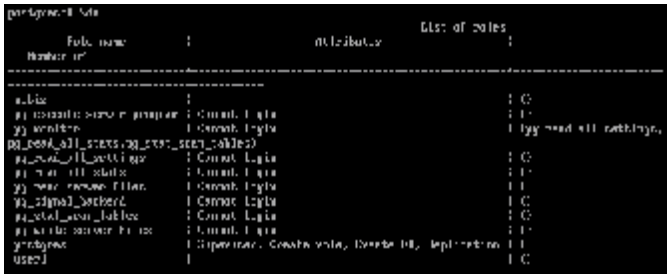
2.10. Postgres-SQL

보안 설정(7개 항목), 디렉토리 및 파일권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 11개 항목으로 구성된다.

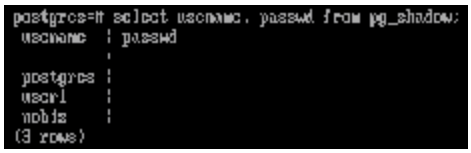
구분	진단코드	진단 항목	취약도
가. 보안 설정	DP-01	불필요한 계정 제거	중
	DP-02	취약한 패스워드 사용 제한	상
	DP-03	불필요한 권한 제거	상
	DP-04	public schema 사용 제한	상
	DP-05	IP 접근 제한 설정	상
	DP-06	안전한 인증 방식 설정	상
	DP-07	안전한 암호화 알고리즘 사용	상
나. 디렉토리 및 파일권한 관리	DP-08	데이터 디렉토리 권한 설정	상
	DP-09	환경 설정파일 권한 설정	상
다. 패치 및 로그 관리	DP-10	로그 활성화	하
	DP-11	최신 패치 적용	상

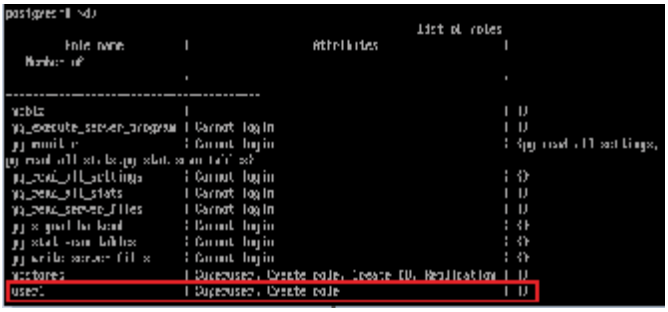
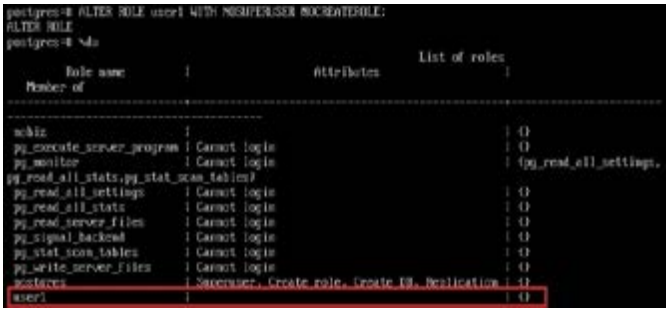
[표 10 PostgreSQL 진단 체크리스트

가. 보안 설정

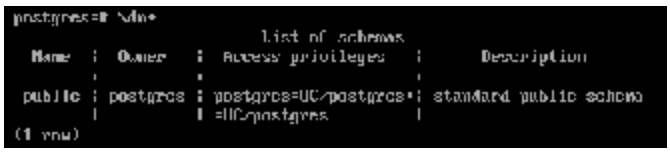
<table>
<tr><td>진단항목</td><td colspan="2">DP-01. 불필요한 계정 제거</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">데이터베이스의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 없는 경우</td></tr>
<tr><td>취약</td><td colspan="3">DB 설치 시 Default로 생성되는 계정 및 테스트 계정, 의심스러운 계정, 불필요한 계정이 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 사용자 계정 목록 조회
PGSQL 접속 후 ₩du 명령어로 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ NOLOGIN 설정
postgres=# ALTER ROLE 계정명 WITH NOLOGIN;
▪ 계정 삭제
postgres=# DROP USER 계정명;

※ LOGIN 가능한 계정 목록 중 불필요한 계정(인가되지 않은 계정, 퇴직자 계정 등 담당자가 실질적인 업무에 필요 없다고 판단하는 계정)은 삭제 또는 NOLOGIN 설정
※ PostgreSQL 접속 후 변경</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

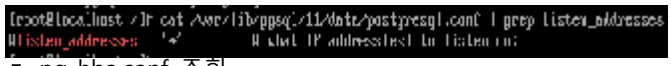
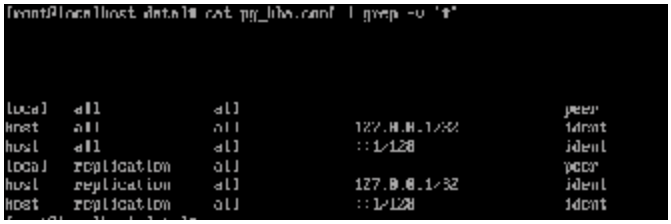
<table>
<tr><td>진단항목</td><td colspan="2">DP-02. 취약한 패스워드 사용제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드 복잡성 설정이 되어 있지 않은 패스워드나 null인 패스워드를 사용하는 경우 비인가자가 쉽게 데이터베이스에 접근할 위험이 있으며 이 경우 데이터베이스 삭제, 변경 등의 심각한 침해사고를 일으킬 가능성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 복잡성 설정이 되어 있거나 null인 패스워드 사용하고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 복잡성 설정이 되어 있지 않거나 null인 패스워드를 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ PGSQL 접속 후 사용자 계정, 패스워드 조회
postgres=# select usename, passwd from pg_shadow;
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 취약하게 설정된 사용자 계정 패스워드를 영어/숫자/특수문자를 혼용하여 8자리 이상으로 변경
▪ PostgreSQL 접속 후 변경
postgres=# ALTER ROLE 계정명 WITH PASSWORD ‘설정할 비밀번호’;
 
</td></tr>
<tr><td>비고</td><td colspan="4">패스워드 복잡성 설정 : 영어/숫자/특수문자를 혼용하여 8자리 이상</td></tr>
</table>

진단항목	DP-03. 불필요한 권한 제거	취약도	상
항목설명	PostgreSQL은 계정에 권한을 설정할 수 있으며 그 중 Superuser가 설정되어 있는 경우 모든 권한을 무시하고 작업을 수행할 수 있으며 Create Role이 설정되어 있는 경우 계정을 생성하고 권한을 부여할 수 있게 한다. 만약 불필요한 계정에 Superuser, Create Role이 설정되어 있는 경우 비인가자가 데이터베이스에 접속하여 계정 생성 및 삭제, 데이터 열람, 삭제, 수정 등의 위험이 있다.		
진단기준	양호	사용하고 있는 계정에 불필요한 권한이 존재하지 않는 경우	
	취약	사용하고 있는 계정에 불필요한 권한이 존재하는 경우	
진단방법	▪ 사용자 계정 목록 조회 PGSQL 접속 후 ₩du 명령어로 확인 		
조치방법	▪ PostgreSQL 접속 후 명령어로 불필요한 권한 제거 postgres=# ALTER ROLE 사용자 계정 WITH NOSUPERUSER NOCREATEROLE; 		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">DP-04. public schema 사용 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">PostgreSQL에서 DB를 생성할 경우 Default로 public schema가 생성된다. 다른 schema를 생성하지 않고 table을 생성할 경우 기본적으로 public schema 안에 생성이 되며 public schema는 모든 개체에서 접근이 가능하므로 정보유출, 자원고갈 등의 위험성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">public schema에 소유주와 특정 계정만이 접근 가능한 경우</td></tr>
<tr><td>취약</td><td colspan="3">public schema에 모든 계정이 접근 가능할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ public schema에 접근 가능한 계정 조회(DB 접속 후 명령어로 확인)

postgre=# ₩dn+
 

※ postgres+=UC가 존재할 경우 DB에 접근 가능한 모든 계정이 public schema에 테이블 생성 및 데이터 저장을 할 수 있음
※ "+"는 각 접근권한 스키마 목록을 구분하기 위한 구분자이며 "+"앞에 명시된 postgres는 상황에 따라 존재할 수도 있고 없을 수도 있음</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ public schema 사용 시 public 권한 REVOKE 적용
1) DB별 접속
2) REVOKE all on schema public from public;
▪ 추후 생성될 DB에 public 권한 REVOKE 적용
1) template1 DB 접속
2) revoke all on schema public from public;</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DP-05. IP 접근 제한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비인가된 사용자가 해당 데이터베이스에 접근할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인가된 IP만 접근 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">비인가된 IP의 접근이 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ postgresql.conf 조회
cat postgresql.conf | grep listen_addresses
 
▪ pg_hba.conf 조회
cat pg_hba.conf | grep –v '#'
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ postgresql.conf 수정
vi postgresql.conf
...
listen_addresses = '허용 IP'
...
 
▪ vi pg_hba.conf
IPv4 local connections: 부분에서
ADDRESS를 허용 IP로 수정
  </td></tr>
<tr><td>비고</td><td colspan="4">※ IP 접근 제한 설정 시 postgresql.conf, pg_hba.conf 두 설정파일이 연계되어 있으므로 한 설정이 잘못될 시 DB 접속이 불가할 수 있음
※ PostgreSQL 사이트에서는 iptables 등을 통해 ip 접근 제한을 설정할 것을 권장함</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DP-06. 안전한 인증 방식 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">PostgreSQL에서는 다양한 인증 방식을 지원하지만 trust, password 등 안전하지 않은 인증 방식도 존재한다. trust 설정 시 암호나 다른 인증 없이 바로 접속이 가능하며 password 설정 시 password가 평문으로 전송되어 스니핑 등의 공격을 통해 password가 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인증 방식이 trust, password, MD5 외 다른 방식으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">인증 방식이 trust, password, MD5 등 안전하지 않은 방식으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ pg_hba.conf에서 인증 방식 설정 조회
cat pg_hba.conf 명령어를 통해 설정 조회
 
'"local" is for Linux domain socket connections only 부분에서 METHOD를 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ pg_hba.conf에서 안전한 인증 방식으로 설정
vi pg_hba.conf 명령어를 통해 수정

ex) '"local" is for Linux domain socket connections only 부분에서
METHOD를 scram-sha-256으로 수정
 
※ 인증 방식 정보
<table><tr><th>인증 방식</th><th>설명</th></tr><tr><td>trust</td><td>무조건 연결을 허용하는 설정, 해당 설정을 적용하면 pgsql에 연결할 수 있는 모든 사용자가 암호나 다른 인증 없이 원하는 모든 pgsql 사용자로 로그인 가능</td></tr><tr><td>reject</td><td>무조건 연결을 거부하는 설정, 해당 설정은 그룹에서 특정 호스트를 필터링하는데 유용</td></tr></table></td></tr>
</table>

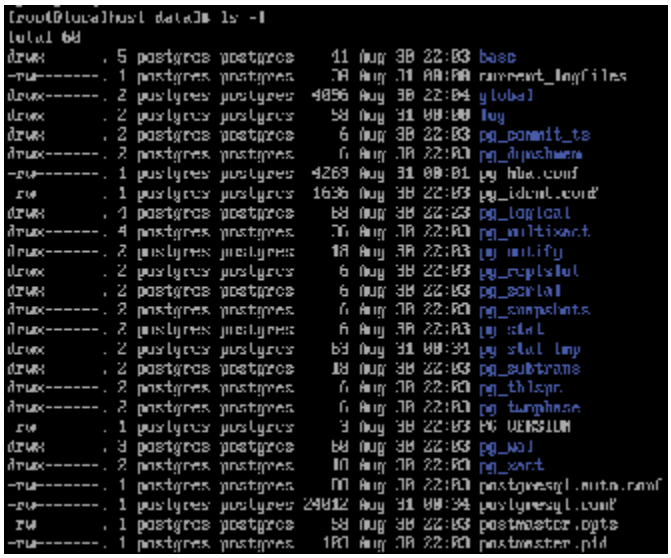
md5	클라이언트가 인증을 위해 MD5로 암호화된 암호를 제공하도록 요구
password	클라이언트가 인증을 위해 암호화되지 않은 암호를 제공, 해당 설정을 적용할 경우 암호가 평문으로 전송
sspi	SSPI를 사용하여 사용자를 인증, Windows에서만 사용 가능
gss	GSSAPI를 사용하여 사용자를 인증, TCP/IP 연결에만 사용 가능
krb5	SSPI를 사용하여 사용자를 인증, Windows에서만 사용 가능
peer	운영 체제에서 클라이언트의 운영 체제 사용자 이름을 얻고 요청한 데이터베이스 사용자 이름과 일치하는지 확인, 로컬 연결에만 사용할 수 있음
ldap	LDAP 서버를 사용하여 인증
radius	RADIUS 서버를 사용하여 인증
cert	SSL 클라이언트 인증서를 사용하여 인증
pam	운영 체제에서 제공하는 PAM(Pluggable Authentication Modules) 서비스를 사용하여 인증
scram-sha-s56	클라이언트가 인증을 위해 SHA256으로 암호화된 암호를 제공하도록 요구

비고	

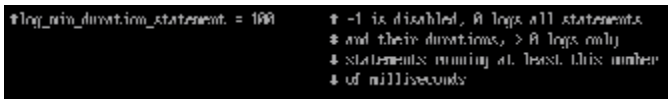
진단항목	DP-07. 안전한 암호화 알고리즘 사용		취약도	상
항목설명	SHA-1의 취약점이 발견됨에 따라 SHA-1이하의 알고리즘은 더 이상 안전한 알고리즘이 아니다. 따라서 SHA-256이상의 암호화 알고리즘을 사용해야 한다.			
진단기준	양호	해시 알고리즘 SHA-256 이상을 사용하고 있는 경우		
	취약	해시 알고리즘 SHA-256 미만을 사용하고 있는 경우		
진단방법	▪ 수동점검 1) 패스워드 저장 시 사용하는 해시 알고리즘 확인			
조치방법	▪ 수동조치 1) 패스워드 저장 SHA-256 이상의 해시 알고리즘으로 암호화 저장			
비고	※ PostgreSQL SHA-256 적용은 10버전 이상부터 가능함			

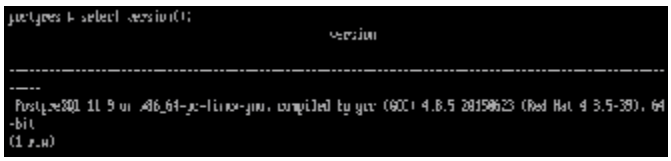
나. 디렉토리 및 파일권한 관리

진단항목	DP-08. 데이터 디렉토리 권한 설정		취약도	상
항목설명	일반 사용자가 PostgreSQL 데이터 디렉토리에 임의의 파일을 생성, 삭제 및 변경할 수 있으면 중요파일 삭제, 백도어 삽입등의 피해가 발생할 수 있다.			
진단기준	양호	데이터 디렉토리 권한이 700 이하인 경우		
	취약	데이터 디렉토리 권한이 700 초과인 경우		
진단방법	1. 데이터 디렉토리 확인 ex) # ls –ld /var/lib/pgsql/11/data 			
조치방법	1. 데이터 디렉토리 권한을 700으로 수정 # chmod 700 [PostgreSQL 데이터 디렉토리]			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">DP-09. 환경 설정파일 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">PostreSQL 중요 파일 중의 하나인 환경설정 파일이 비인가자에 의해 변경된다면 시스템 장애 발생이 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">해당 설정파일의 소유자 및 그룹이 별도의 계정 소유이면서 권한이 600 이하일 경우</td></tr>
<tr><td>취약</td><td colspan="3">해당 설정파일의 소유자 및 그룹이 별도의 계정 소유가 아니거나 권한이 600 초과일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"># ls –l [postgreSQL 설치 경로]
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 설정파일 권한을 600으로 수정
chmod 600 [postgreSQL 설정 파일]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 패치 및 로그 관리

진단항목	DP-10. 로그 활성화	취약도	하
항목설명	로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.		
진단기준	양호	로그가 활성화되어 있는 경우	
	취약	로그가 비활성화되어 있는 경우	
진단방법	▪ postgresql 설정파일을 통해 확인 1) log_statement 설정 ex) # cat /var/lib/pgsql/11/data/postgresql.conf | grep log_statement  2) log_min_duration_statement 설정 ex) # cat /var/lib/pgsql/11/data/postgresql.conf | grep log_min_duration_statement 		
조치방법	▪ postgresql 설정파일 수정 1) log_statement 로그 설정 # vi [postgresql 설치 경로]/postgresql.conf … log_statement = 'all'  2) log_min_duration_statement 로그 설정 # vi [postgresql 설치 경로]/postgresql.conf … log_min_duration_statement = 100 		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">DP-11. 최신 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 패치가 적용되어 있지 않을 경우, 잘 알려진 취약점에 데이터베이스가 노출될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 버전 패치가 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 버전 패치가 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ PostgreSQL 버전 확인 후 최신 패치 적용 여부 확인
postgres=# select version();
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 데이터베이스에 대한 최신의 버전을 확인 후 업그레이드 및 패치 수행

※ PostgreSQL 공식사이트에서 최신 버전 확인 가능
https://www.postgresql.org/download/</td></tr>
<tr><td>비고</td><td colspan="4">▪ 시스템 업데이트는 영향도를 산정하여 진행하여야 함
<table><tr><td>버전</td><td>지원 종료 날짜</td></tr><tr><td>13.0</td><td>2025.11.13</td></tr><tr><td>12.4</td><td>2024.11.14</td></tr><tr><td>11.9</td><td>2023.11.9</td></tr><tr><td>10.14</td><td>2022.11.10</td></tr><tr><td>9.6.19</td><td>2021.11.11</td></tr><tr><td>9.5.23</td><td>2021.2.11</td></tr><tr><td>9.4.26</td><td>20.2.13(종료)</td></tr></table></td></tr>
</table>

2.11. Redis

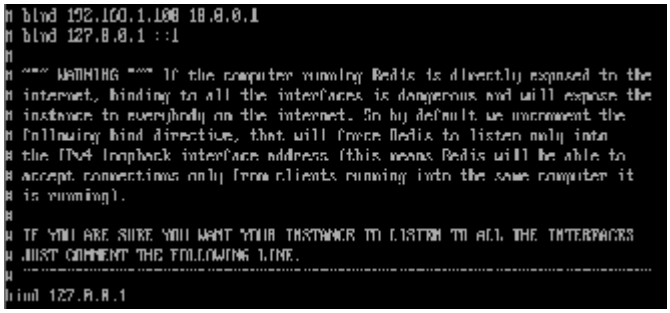
보안 설정(4개 항목), 디렉토리 및 파일권한 관리(2개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 8개 항목으로 구성된다.

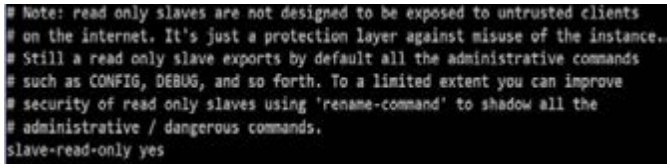
구분	진단코드	진단 항목	취약도
가. 보안 설정	DR-01	Redis 인증 패스워드 설정	중
	DR-02	Binding 설정	상
	DR-03	Slave 읽기 전용 모드 설정	상
	DR-04	rename-command 설정	중
나. 디렉토리 및 파일권한 관리	DR-05	데이터 디렉토리 접근권한 설정	중
	DR-06	설정파일 접근권한 설정	상
다. 패치 및 로그 관리	DR-07	로그 활성화	하
	DR-08	최신 패치 적용	상

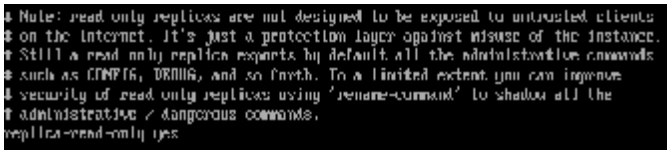
[표 11]Redis 점검 체크리스트

가. 보안 설정

진단항목	DR-01. Redis 인증 패스워드 설정		취약도	중
항목설명	Redis 패스워드 설정이 되어 있지 않은 경우, 서버에 접근하는 사용자 모두 데이터베이스에 접근이 가능하게 되어 데이터베이스 장악 및 정보 유출의 위험이 존재한다.			
진단기준	양호	인증패스워드가 설정되어 있는 경우		
	취약	인증패스워드가 설정되어 있지 않은 경우		
진단방법	▪ redis 디렉토리 > redis.conf 파일 안의 requirepass 설정 확인 # cat [redis 디렉토리]/redis.conf | grep –i requirepass 			
조치방법	▪ redis.conf 파일 안의 requirepass 설정 # vi [redis 디렉토리]/redis.conf에서 requirepass 설정 (주석 처리 되어있으면 주석 해제) 			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">DR-02. Binding 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비인가된 사용자가 해당 데이터베이스에 접근할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인가된 IP만 접근 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">비인가된 IP의 접근이 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 디렉토리 > redis.conf 파일 안의 bind 설정 확인
cat [redis 디렉토리]/redis.conf | grep –i bind
 
※ default 설정 : 127.0.0.1 (로컬호스트에서만 접근 가능)</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ redis 디렉토리 > redis.conf 파일 안의 bind 설정
vi [redis 디렉토리]/redis.conf
(인가된 IP만 접근 가능하도록 설정)</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

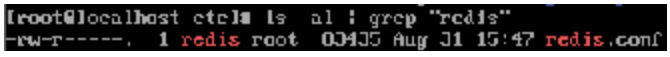
<table>
<tr><td>진단항목</td><td colspan="2">RE-03. Slave 읽기 전용 모드 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">master와 slave 환경에서 slave에 read only 기능만을 설정하여 master에 있는 자원을 변경할 수 없도록 해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">slave에 읽기 권한만 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">slave에 쓰기 설정이 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 4.x 이하일 경우 redis 설정파일에서 slave-read-only 설정 확인
cat [redis 디렉토리]/redis.conf | grep –i slave-read-only
 
※ default 설정 : slave-read-only yes

▪ redis 5.x 이상일 경우 redis 설정파일에서 replica-read-only 설정 확인
cat [redis 디렉토리]/redis.conf | grep –i replica-read-only
 
※ default 설정 : replica-read-only yes</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ redis 5.x 이상일 경우 redis 설정파일에서 replica-read-only 설정
vi [redis 디렉토리]/redis.conf
replica-read-only를 yes로 변경</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

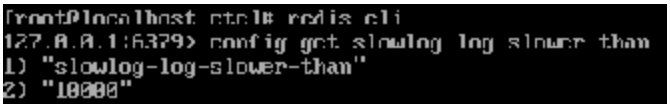
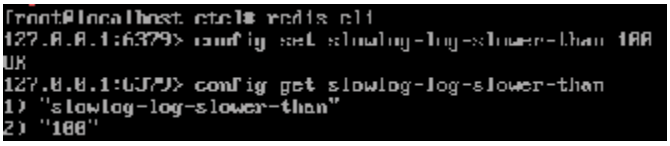
<table>
<tr><td>진단항목</td><td colspan="2">RE-04. rename-command 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">공유되는 환경에서는 위험한 command들의 이름을 변경할 수 없다. 비인가된 사용자가 환경을 변경하거나 데이터를 가져오는 위험한 command를 사용할 수 없도록 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">rename-command CONFIG를 빈칸으로 설정하고 있거나 운영상 필요한 command외 나머지 command의 이름을 변경하여 사용하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">rename-command CONFIG 설정이 되어 있지 않은 경우(주석 처리 되어 있는 경우)</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 디렉토리 > redis.conf 파일 안의 rename-command CONFIG 확인
cat [redis 디렉토리]/redis.conf | grep –i rename-config CONFIG
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ redis 디렉토리 > redis.conf 파일 안의 rename-command CONFIG 설정
vi [redis 디렉토리]/redis.conf
rename-command CONFIG 설정
예시)
rename-command CONFIG ""
또는
rename-command CONFIG b840fc02d624045429941cc15f59e41cb7be6c52</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

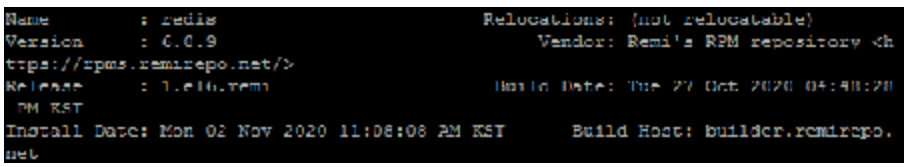
나. 디렉토리 및 파일권한 관리

<table>
<tr><td>진단항목</td><td colspan="2">RE-05. 데이터 디렉토리 접근권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자가 redis 설치 디렉토리에 임의의 파일을 생성, 삭제 및 변경할 수 있으면, 중요파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">데이터 디렉토리의 other 권한이 부여되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">데이터 디렉토리의 other 권한이 부여되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 데이터 디렉토리 권한 확인
1) 데이터 디렉토리 경로 확인
cat [redis 설정 파일] | grep –v "^#" | grep "^dir"
 
2) 데이터 디렉토리 권한 확인
ls –ld [데이터 디렉토리]
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ redis 데이터 디렉토리 권한을 750으로 변경
chmod 750 [redis 데이터 디렉토리]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">RE-06. 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일에 others 권한이 존재할 경우, 비인가된 사용자가 설정파일에 접근하여 설정 변경을 통해 서비스 장애를 일으킬 위험이 존재하며 또한 설정 파일을 통해 정보를 획득하여 2차 공격의 정보로 사용할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">설정 파일에 소유자에게만 권한이 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">설정 파일에 소유자 외에 권한이 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 디렉토리안에 redis.conf 권한 확인
ls –al [redis 디렉토리]/redis.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ redis 데이터 디렉토리 권한을 600 이하로 변경
chmod 600 [redis 디렉토리]/redis.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">RE-07. 로그 활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로그가 활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로그가 비활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 슬로우 쿼리 로그 확인
1) 127.0.0.1:6379> config get slowlog-log-slower-than
2) “slowlog-log-slower-than”
3) “100”
 
▪ 로그 레벨 설정 확인
1) # cat /etc/redis.conf | grep loglevel
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 슬로우 쿼리 로그 설정
1) 127.0.0.1:6379> config get slowlog-log-slower-than 100
2) “slowlog-log-slower-than”
3) “100”
 
▪ 로그 레벨 설정 변경
1) # vi /etc/redis.conf
loglevel notice</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">RE-08. 최신 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 패치가 적용되어 있지 않을 경우, 잘 알려진 취약점에 데이터베이스가 노출될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 버전 패치가 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 버전 패치가 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ redis 디렉토리에서 확인
[redis 디렉토리]/redis-cli –v
 

[redis 디렉토리]/redis-server –v
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 수동 조치
잘 알려진 취약점이 없는 버전으로 업그레이드 해야함.

https://redis.io/download</td></tr>
<tr><td>비고</td><td colspan="4">▪ 시스템 업데이트는 영향도를 산정하여 진행하여야 함
<table><tr><td>버전</td><td>지원 종료 날짜</td></tr><tr><td>6.0</td><td>2021.11.30</td></tr><tr><td>5.6</td><td>2021.10.31</td></tr><tr><td>5.4</td><td>2020.12.31</td></tr></table></td></tr>
</table>

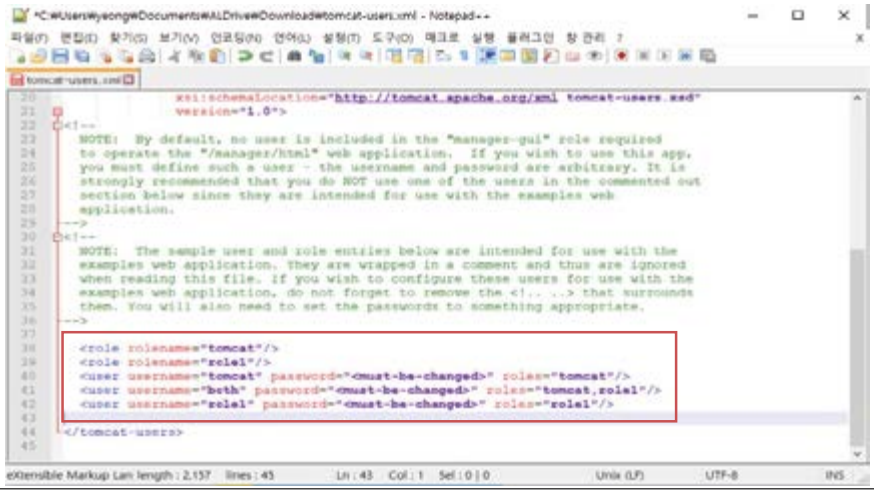
2.12. Tomcat

계정 관리(2개 항목), 보안 설정(5개 항목), 패치 및 로그관리(2개 항목) 총 3개 영역에서 9개 항목으로 구성된다.

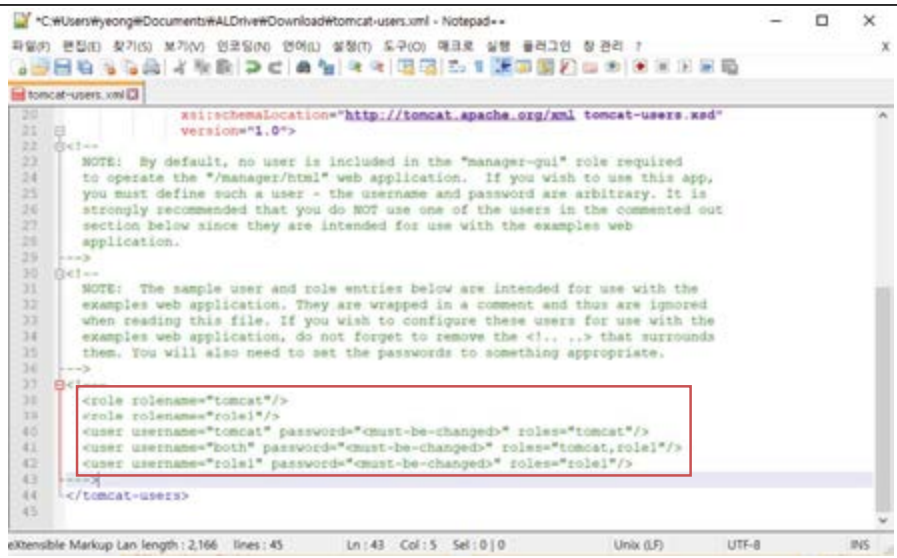
구분	진단코드	진단 항목	취약도
가. 계정 관리	TO-01	Default 관리자 계정명 변경	하
	TO-02	취약한 패스워드 사용제한	중
나. 보안 설정	TO-03	패스워드 파일 권한 관리	상
	TO-04	홈디렉터리 쓰기 권한 관리	상
	TO-05	환경설정 파일 권한 관리	상
	TO-06	디렉터리 리스팅 설정 제한	하
	TO-07	에러 메시지 관리	중
다. 패치 및 로그관리	TO-08	로그 파일 주기적 백업	중
	TO-09	최신 패치 적용	중

[표 12] Tomcat 진단 체크리스트

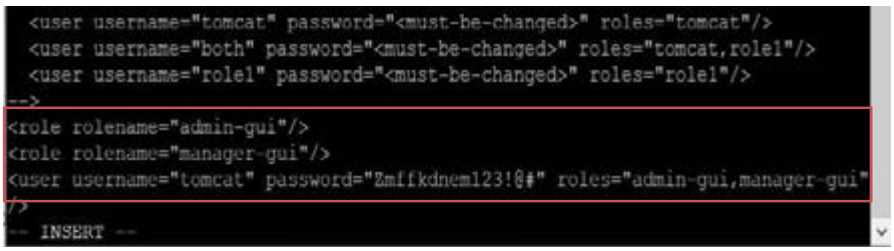
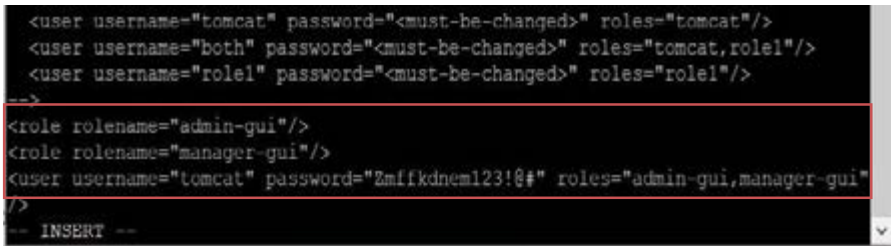
가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">TO-01. Default 관리자 계정명 변경</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">비인가 사용자에 의한 계정, 패스워드 유추 방지로서, WAS 설치지 Web 관리자 콘솔 계정으로 Default 값인 각각 Jeus[administrator], Tomcat[tomcat], WebLogic[weblogic]을 사용한다. Default값을 그대로 사용하는 경우 패스워드 유추 공격의 위험에 노출되므로, 유추하기 불가능한 계정명으로 변경해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">계정명이 Default 계정명으로 설정되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">계정명이 Default 계정명으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 계정 사용 여부 확인
1) tomcat-user.xml 파일에서 role 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 추가적인 보안을 위해, 시스템 관리자 계정으로 “system", "admin", 또는 ”administrator"와 같은 유추 가능한 쉬운 계정명 사용금지

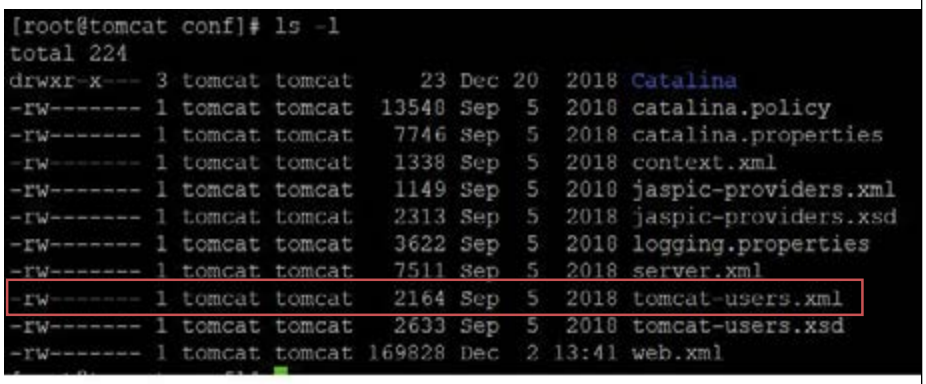
▪ Default 계정명 변경
1) /[Tomcat Dir]/conf/server.xml 파일 수정</td></tr>
</table>

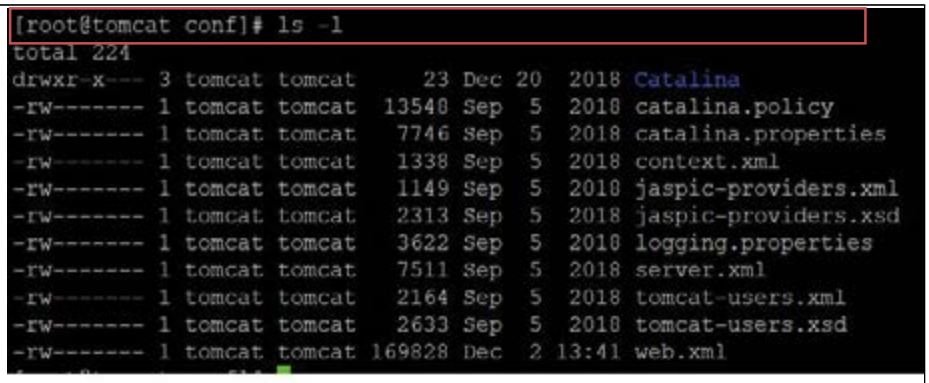
	
비고	

*C:₩Users₩yeong₩Documents₩ALDrive₩Download₩tomcat-users.xml - Notepad++
tomcat-users.xml
xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
version="1.0">
<!--
NOTE: By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application. If you wish to use this app,
you must define such a user - the username and password are arbitrary. It is
strongly recommended that you do NOT use one of the users in the commented out
section below since they are intended for use with the examples web
application.
-->
<!--
NOTE: The sample user and role entries below are intended for use with the
examples web application. They are wrapped in a comment and thus are ignored
when reading this file. If you wish to configure these users for use with the
examples web application, do not forget to remove the <!.. ..> that surrounds
them. You will also need to set the passwords to something appropriate.
-->
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
</tomcat-users>
eXtensible Markup Lan length : 2,166 lines : 45 Ln : 43 Col : 5 Sel : 0 | 0 Unix (LF) UTF-8 INS

<table>
<tr><td>진단항목</td><td colspan="2">TO-02. 취약한 패스워드 사용제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자 계정의 패스워드를 취약하게 설정하여 사용하는 경우, 비인가 사용자가 패스워드 유추 공격을 시도하여, 관리자 권한을 획득할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">관리자 패스워드가 암호화 되어 있거나, 유추하기 쉬운 패스워드로 설정되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">관리자 패스워드가 암호화 되어 있지 않거나, 유추하기 쉬운 패스워드로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 패스워드 암호화 설정 확인
1) /[Tomcat Dir]/conf/server.xml 파일에서 default password 사용여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 패스워드 암호화 설정 변경
1) 관리자가 패스워드 선정 시 다음 규칙에 따라 설정해야 함
2) 규칙 : 영문 대/소문자, 특수문자 포함 8자 이상, 동일문자 연속 4회 이상 사용 금지, 계정명과 동일하거나 패스워드 설정이 되어있지 않은 경우
3) 설정 파일 : /[Tomcat Dir]/conf/tomcat-users.xml
4) 예시 : <user username="tomcat" password="Zmffkdnem123!@" roles="admin, manager,tomcat"/>
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

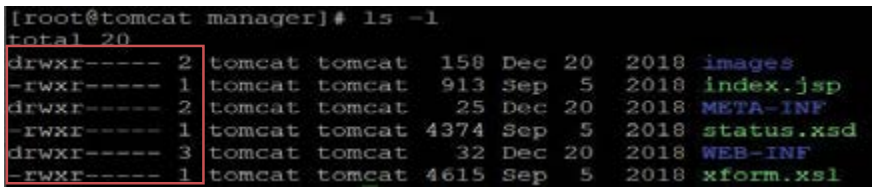
나. 보안 설정

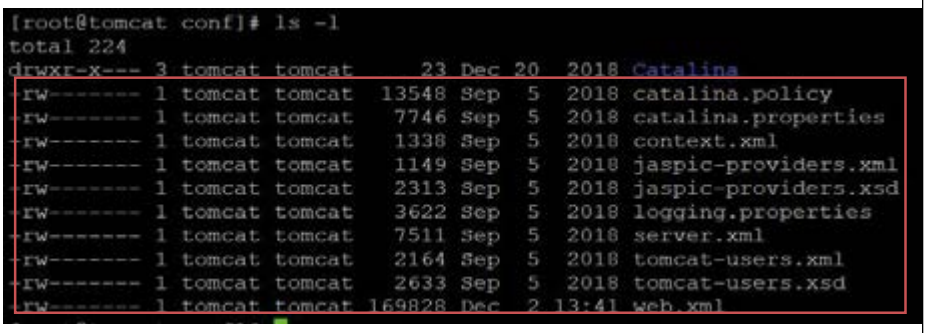
<table>
<tr><td>진단항목</td><td colspan="2">TO-03. 패스워드 파일 권한 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자 콘솔용 패스워드 파일, Role 파일의 default 퍼미션이 644(rw-r--r--)로 설정되어 있다면 일반 사용자에게 패스워드가 노출될 수 있다. 이 파일 내에는 계정과 패스워드가 평문으로 저장되어 있어 일반계정이 읽을 경우, 관리 콘솔용 패스워드가 쉽게 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 파일에 권한이 600(rw-------) 이하로 설정되어 있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 파일에 권한이 600(rw-------) 이하로 설정되어 있지 않을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 패스워드 권한 설정 확인
1) /[Tomcat Dir]/conf/tomcat-users.xml 파일 접근 권한 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 패스워드 권한 변경
[Lnix 환경]
chmod 600 file_name</td></tr>
</table>

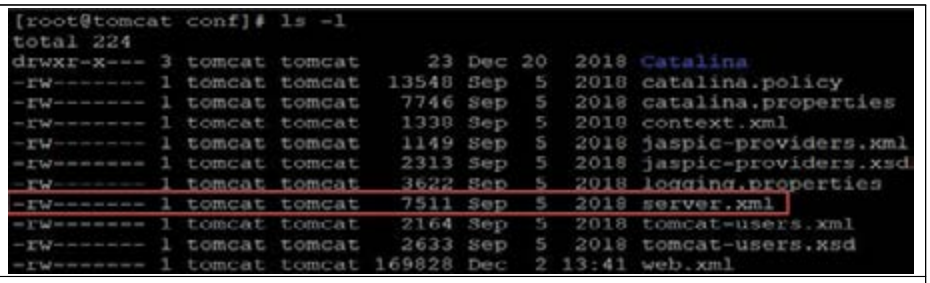
	
비고	적용시 개발자 및 운영자 협의필요

<table>
<tr><td>진단항목</td><td colspan="2">TO-04. 홈디렉터리 쓰기 권한 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자가 웹 서버 홈 디렉터리 또는 설정관리 서버 디렉터리 및 매니지드 구동서버 디렉터리에 임의의 파일을 생성, 삭제 및 변경 할 수 있으면, 홈페이지 변조, 중요파일 삭제, 백도어 삽입 등의 피해가 발생 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">홈 디렉터리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(drwxr-xr-x)로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">홈 디렉터리 또는 웹 서버, 관리 서버 디렉터리 권한이 755(drwxr-xr-x)로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 디렉터리 권한 설정 확인
1) 웹서버 홈 : /[Tomcat 설치 디렉터리]/conf/server.xml 파일 -> appBase="webapps"
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="true"
xmlValidation="false" xmlNamespaceAware="false">
2) 관리서버 홈 : /[Tomcat Dir]/webapps/ROOT 또는 /[Tomcat Dir]/webapps/manage
group 쓰기권한 및 others 쓰기 권한 제거 여부 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">※ 파일 업로드 폴더가 있다면 쓰기 권한 부여

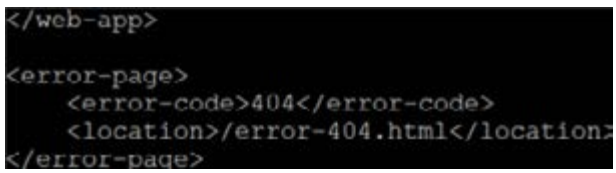
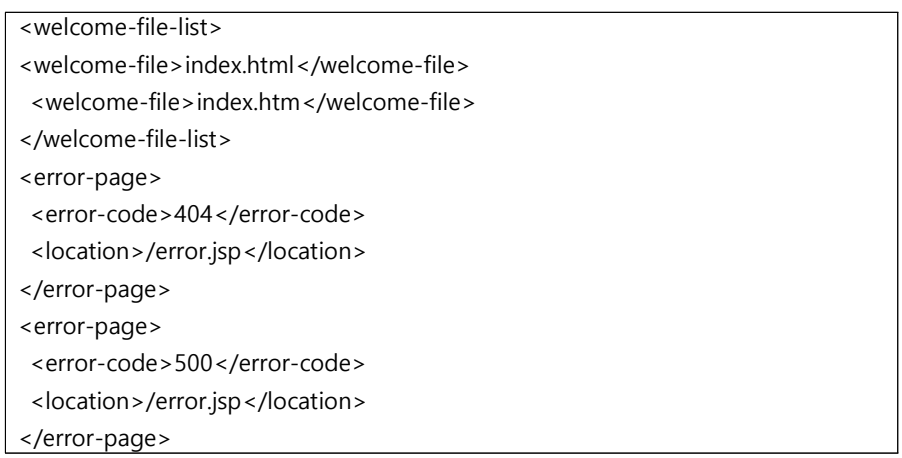
■ 디렉터리 권한 변경
chmod 755 dir_name

 
</td></tr>
<tr><td>비고</td><td colspan="4">※ tomcat server.xml 파일 설정에 Context path 설정이 존재할 경우 docBase에 설정된 경로가 웹서버 홈디렉터리로 설정됨</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">TO-05. 환경설정 파일 권한 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일반 사용자가 웹 사이트 소스 파일을 삭제, 변경할 수 있으면, 홈페이지 변조, 작업 실수로 인한 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다. 이로 인해 시스템이 오작동하여 사용 불능 상태에 빠질 우려가 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">WAS 전용계정 소유이고 소스파일 퍼미션 644, 설정파일 퍼미션 600으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">WAS 전용계정 소유이고 소스파일 퍼미션 644, 설정파일 퍼미션 600으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">1. 파일의 쓰기 권한 점검 확인
2. 소스 파일 : /[Tomcat 설치 디렉터리]/conf/server.xml(appBase 확인)
3. 설정 파일 : /[Tomcat 설치 디렉터리]/conf/ (해당파일: *.xml, *.properties, *.policy)</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 디렉터리 권한 변경
Tomcat
1) 설정 관련 파일 권한 변경
chmod 600 file_name
 
2) 소스 파일 권한 변경
chmod 644 file_name</td></tr>
</table>

	
비고	적용 시 개발자 및 운영자 협의필요

<table>
<tr><td>진단항목</td><td colspan="2">TO-06. 디렉터리 리스팅 설정 제한</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">디렉터리 검색 기능(Directory Indexing 또는 Directory Listing)이 설정되어 있는 경우, Web 서버 구조 노출 및 설치 파일의 유출 가능성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">디렉터리 리스팅이 설정되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">디렉터리 리스팅이 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 디렉터리 리스팅 설정유무 확인
1) /[Tomcat Dir]/conf/web.xml 파일에서 <param-value> 값 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[Tomcat]
■ /[Tomcat Dir]/conf/web.xml 파일에서 false 설정
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">TO-07. 에러 메시지 관리</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 돌아오는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">에러코드를 유추 불가능하도록 일원화된 에러메시지를 생성한 경우</td></tr>
<tr><td>취약</td><td colspan="3">에러코드를 유추 불가능하도록 일원화된 에러메시지를 생성하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /[Tomcat Dir]/conf/web.xml 파일에서 error-page 설정 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">[Tomcat]
■ 설정파일에서 에러 메시지 설정 확인 (필수 설정 : 400, 401, 403, 404, 500)
■ 설정 파일 : /[Tomcat Dir]/conf/web.xml (error 메시지 처리 확인)
 
</td></tr>
<tr><td>비고</td><td colspan="4">적용 시 개발자 및 운영자 협의 필요</td></tr>
</table>

다. 패치 및 로그관리

진단항목	TO-08. 로그 파일 주기적 백업		취약도	중
항목설명	Backup을 통해 고의/비고의적 사고로 인한 서비스 중단 시간을 최소화하여 복구할 수 있으며, Backup 파일의 퍼미션이 잘못 설정되어 있을 경우 비인가자가 Backup파일을 절취함으로써 중요 데이터가 누출될 수 있으므로 Backup은 적절한 정책에 의해 실행되어야 하며 생성된 Backup 파일의 관리가 철저히 이루어져야 한다. 주기적인 백업이 수행되어야 하며 특히 유지보수 및 Upgrade 작업에는 전체 Full 백업을 실시하여 장애 및 외부 침입 등에 대한 변조가 발생할 경우를 대비해야 한다.			
진단기준	양호	로그 파일을 주기적으로 백업하고 있는 경우		
	취약	로그 파일을 주기적으로 백업하고 있지 않은 경우		
진단방법	■ 백업설정에 대하여 해당 WEB서버 담당자와 인터뷰 실시 ■ 담당자와 인터뷰하여 주기적인 백업 수행 여부 점검 ■ 백업 및 복구 수행 이력을 점검하여 백업이 정책에 따라 수행되고 있는지 점검			
조치방법	■ 백업 정책을 바탕으로 주기적인 백업 절차를 수립 ■ 유지보수 및 Upgrade 작업 시에는 전체 Full 백업 절차를 수립(권고사항) ■ 주기적인 백업정책 설정을 하고, 백업내용의 복사본이 안전한 off-site에 보관되어야 함			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">TO-09. 최신 패치 적용</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">주기적으로 보안 패치를 적용하지 않으면 서버 침해가 발생할 수 있다. 따라서 최신의 버전과 패치를 확인 후 업그레이드 및 패치 수행해야 한다. Jeus는 Alternate Data Streams 취약점으로 소스 파일 노출이 가능하기 때문에 패치 조치가 필요하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 패치를 적용 하였을 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 패치를 적용 하지 않았을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 최신 패치 적용 확인

1) 소스 파일 설치 시 : # /[Tomcat Dir]/bin/version.sh
2) rpm 또는 yum 설치 시 : # rpm –qa | grep webapps</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 최신 패치를 확인 후 업그레이드 및 패치 수행</td></tr>
<tr><td>비고</td><td colspan="4">적용 시 개발자 및 운영자 협의 필요</td></tr>
</table>

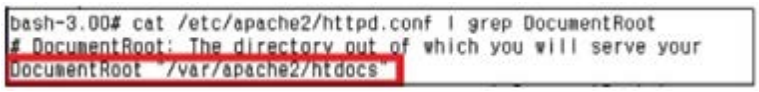
2.13. Apache

보안 설정(4개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

구분	항목 코드	점검 항목	취약도
가. 보안 설정	AP-01	웹 서비스 영역의 분리	상
	AP-02	불필요한 파일 제거	상
	AP-03	링크 사용금지	상
	AP-04	파일 업로드 및 다운로드 제한	상
나. 접근 관리	AP-05	디렉터리 리스팅 제거	상
	AP-06	웹 프로세스 권한 제한	상
다. 패치 관리	AP-07	안정화 버전 및 패치 적용	상

[표 13] Apache 점검 체크리스트

가. 보안 설정

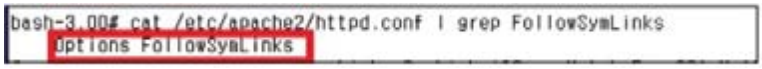
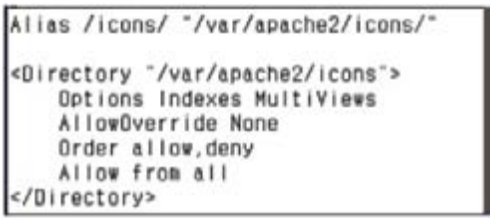
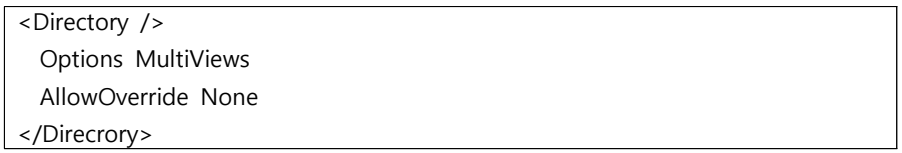
<table>
<tr><td>점검 항목</td><td colspan="2">AP-01. 웹 서비스 영역의 분리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">Apache 설치 시 htdocs 디렉터리를 DocumentRoot로 사용하고 있는데 htdocs 디렉터리는 공개되어서는 안 될(또는, 공개될 필요가 없는) Apache 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 변경하여야 한다. 또한, 대량의 업로드와 다운로드 시 서비스 불능 상태가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">DocumentRoot를 별도의 디렉터리로 지정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">DocumentRoot를 기본 디렉터리로 지정한 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 기본 디렉터리 확인
1) /etc/apache2/httpd.conf 파일에서 DocumentRoot 디렉터리 확인
2) # cat [Apache2 설정 디렉터리]/httpd.conf | grep DocumentRoot
 
</td></tr>
<tr><td>조치
방법</td><td colspan="4">1. 기본 디렉터리 변경
1) DocumentRoot 위치 변경
2) # vi [Apache2 설정 디렉터리]/httpd.conf
#DocumentRoot "/var/apache2/htdocs"
DocumentRoot "/export/userid/www"</td></tr>
<tr><td>비고</td><td colspan="4">※ 웹서버 데몬은 chroot에 설치하는 것이 안전하다. 만약 웹 서버 데몬이 공격당했다고 하더라도 공격자는 chroot 디렉터리 이외로는 접근할 수 없어 피해를 최소화할 수 있음</td></tr>
</table>

<table>
<tr><td>점검 항목</td><td colspan="2">AP-02. 불필요한 파일 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 외부 침입자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거하여야 한다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">매뉴얼, cgi-bin 파일 및 디렉터리가 제거되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">매뉴얼, cgi-bin 파일 및 디렉터리가 제거되지 않은 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 매뉴얼 디렉터리와 cgi-bin 디렉터리 존재여부 확인
1) manual 디렉터리와 cgi-bin 디렉터리 조회
2) # cd [Apache2 설치 디렉터리]
3) # find . -name manual 명령어
fine . -name cgi-bin 명령어
 
4) httpd.conf 파일에 manual과 cgi-bin에 관한 설정 존재여부 확인
5) # vi [Apache2 설정 디렉터리]/httpd.conf
  </td></tr>
<tr><td>조치
방법</td><td colspan="4">※ 웹 서버를 정기적으로 검사하여 임시 파일들을 삭제하도록 한다. 특히 웹 서비스의 업데이트나 유지보수 시 생성되는 백업파일이나 중요한 파일 등은 작업이 끝난 후 반드시 삭제하도록 한다. 아파치를 설치하면 기본적으로 설치되는 cgi-bin은 공격에 이용 될 수 있으므로 삭제하고, manual 파일은 시스템에 대한 정보를 포함하고 있어서 해킹에 도움이 될 수 있기 때문에 웹 서버에서 삭제한다. 정확한 관리를 위해 폴더와 파일의 이름과 위치, 개수 등이 적혀있는 별도의 문서를 관리하는 것이 좋다. 문서에 등록되지 않은 불필요한 파일들을 점검해서 삭제하도록 한다.

1. 매뉴얼 디렉터리와 cgi-bin 디렉터리 삭제
1) manual 디렉터리와 cgi-bin 디렉터리 삭제
2) # rm -rf [Apache2 설치 디렉터리]/manual
rm -rf [Apache2 설치 디렉터리]/cgi-bin
3) httpd.conf 에서 매뉴얼과 cgi-bin에 관한 설정이 존재할 경우 삭제 또는 주석처리
4) # vi [Apache2 설정 디렉터리]/httpd.conf</td></tr>
</table>

	 #AliasMatch ^/manual(?:/(?:de|en|es|fr|ja|ko|ru))?(/.*)?$ /usr/apache2/manual$1 # #<Directory "/usr/apache2/manual"> # Options Indexes # AllowOverride None # Order allow,deny # Allow from all # # <Files *.html> # SetHandler type-map # </Files> # # SetEnvIf Request_URI ^/manual/(de|en|es|fr|ja|ko|ru)/ prefer-language=$1 # RedirectMatch 301 ^/manual(?:/(de\|en\|es\|fr\|ja\|ko\|ru)){2,}(/.*)?$ /manual/$1$2 #</Directory>
비고	

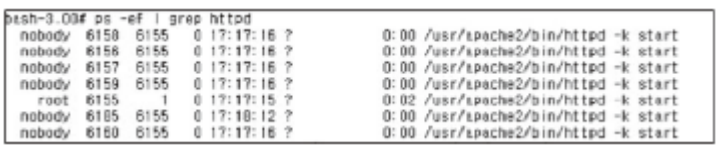
<table>
<tr><td>점검 항목</td><td colspan="2">AP-03. 링크 사용금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">일부 서버는 "심볼릭 링크(Symbolic link)를 이용하여 기존의 웹 문서 이외의 파일시스템 접근이 가능하도록 하고 있음. 이러한 방법은 편의성을 제공하는 반면, 일반사용자들도 시스템 중요 파일에 접근할 수 있게 하는 보안 문제를 발생시킨다.
가령 시스템 자체의 root 디렉터리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한(nobody)으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 "/etc/passwd" 파일과 같은 민감한 파일을 누구나 열람할 수 있게 된다.

* 심볼릭 링크(Symbolic link, 소프트 링크) : 윈도우 운영체제의 바로가기 아이콘과 비슷하다. 링크 생성 시 파일 내용은 존재하지 않으나 사용자가 파일을 요청하면 링크가 가리키고 있는 원본 데이터에서 데이터를 가져와서 전달한다. 직접 원본을 가리키지 않고 원본 데이터를 가리키는 포인터를 참조함으로써 원본데이터가 삭제, 이동, 수정이 되면 사용 불가능 하다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">심볼릭 링크, aliases 사용을 제한한 경우</td></tr>
<tr><td>취약</td><td colspan="3">심볼릭 링크, aliases 사용을 제한하지 않은 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 심볼릭 링크, aliases 사용을 제한여부 확인
1) httpd.conf 파일에서 FollowSymLinks 옵션이 설정되어 있는지 확인
2) # cat [Apache2 설정 디렉터리]/httpd.conf | grep FollowSymLinks
 
3) httpd.conf 파일에서 불필요한 alias설정이 존재하는지 확인
4) # vi [Apache2 설정 디렉터리]/httpd.conf
  </td></tr>
<tr><td>조치
방법</td><td colspan="4">1. 심볼릭 링크, aliases 사용을 제한 설정
1) httpd.conf 파일에 설정된 디렉터리별로 Options 항목에 설정된 FollowSymLinks 옵션을 제거하거나 –FollowSymLinks 옵션 설정
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

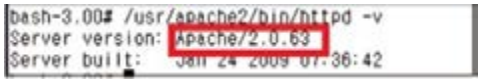
<table>
<tr><td>점검 항목</td><td colspan="2">AP-04. 파일 업로드 및 다운로드 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드로 인한 서비스 불능 상태가 발생할 수 있다. 따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹 서버에 의해 처리되지 못하게 하고, 자동이나 수동으로 파일의 보안성 검토를 수행한다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">파일 업로드 및 다운로드 용량을 제한한 경우</td></tr>
<tr><td>취약</td><td colspan="3">파일 업로드 및 다운로드 용량을 제한하지 않은 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 파일 업로드 및 다운로드 용량을 제한 설정 확인
1) httpd.conf 파일에 용량이 적절히 설정되어 있는지 확인
2) # vi [Apache2 설정 디렉터리]/httpd.conf
<Directory />
LimitRequestBody 10240000
</Directory>
<Directory /home/userdir/>
LimitRequestBody 20480000
</Directory></td></tr>
<tr><td>조치
방법</td><td colspan="4">1. 파일 업로드 및 다운로드 용량을 제한 설정
1) httpd.conf 파일에 용량을 시스템에 따라 적절하게 설정
2) vi [Apache2 설정 디렉터리]/httpd.conf
<Directory />
LimitRequestBody 5000000
</Directory>
<Directory /home/userdir/>
LimitRequestBody 10240000
</Directory>
3) 위와 같이 LimitRequestBody를 설정하면 아파치 웹 서버를 이용하여 (/)는 모든 파일의 사이즈를 5M로 제한하고 /home/userdir/ 폴더에 대해서는 10M로 제한하게 됨</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

나. 접근 관리

<table>
<tr><td>점검 항목</td><td colspan="2">AP-05. 디렉터리 리스팅 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">디렉터리 검색은 디렉터리 요청 시 해당 디렉터리에 기본 문서가 존재하지 않을 경우 디렉터리 내 모든 파일의 목록을 보여주는 기능임. 디렉터리 검색 기능이 활성화 되어 있는 경우 외부에서 디렉터리 내의 모든 파일에 대한 접근이 가능하여 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스 파일 등 공개되어서는 안 되는 중요 파일 노출이 가능하다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">디렉터리 검색 기능을 사용하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">디렉터리 검색 기능을 사용하는 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 디렉터리 검색 기능을 사용여부 확인
1) httpd.conf 파일에서 indexes 옵션이 설정되어 있는지 확인
2) # vi [Apache2 설정 디렉터리]/httpd.conf 파일 확인</td></tr>
<tr><td>조치
방법</td><td colspan="4">1. httpd.conf 파일에 설정된 Options 항목에 indexes를 제거하거나, -indexes 옵션 설정을 통해 디렉터리 리스팅을 제한한다.
2. httpd,conf 파일에서 indexes 지시자 삭제
3. # vi [Apache2 설정 디렉터리]/httpd.conf
<pre><Directory "/var/apache2/htdocs">
Options Indexes FollowSymLinks
Order allow,deny
Allow from all
</Directory></pre>4. httpd.conf 파일에서 -indexes 지시자 설정
5. # vi [Apache2 설정 디렉터리]/httpd.conf
<pre><Directory "/var/apache2/htdocs">
Options FollowSymLinks
Order allow,deny
Allow from all
</Directory></pre></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>점검 항목</td><td colspan="2">AP-06. 웹 프로세스 권한 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">Linux 시스템의 경우 Web 서버 데몬이 root 권한으로 운영될 경우 Web Application의 취약점 또는, 버퍼 오버플로우(Buffer Overflow)로 인하여 root 권한을 획득할 수 있으므로 서버 데몬이 root 권한으로 운영되지 않도록 관리하여야 한다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">Apache 데몬이 root 권한으로 구동되지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Apache 데몬이 root 권한으로 구동되는 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 웹 서버 프로세스 소유자의 권한을 확인
ps -ef | grep httpd
 
</td></tr>
<tr><td>조치
방법</td><td colspan="4">1. httpd.conf 파일에서 Root 권한으로 구동되고 있을 경우, Apache 데몬 User/Group 변경
2. # vi [Apache2 설정 디렉터리]/httpd.conf
User apache
Group apache
3. /etc/passwd 파일에서 Nobody나 Apache와 같이 변경하여 구동 중일 경우, 변경된 계정이 로그인이 되지 않도록 제한(예, 위에 변경된 Apache 계정)
4. # vi /etc/passwd
Apache:x:48:48:Apache:/home/Apache/www:/sbin/nologin
5. 다음 설정을 통해 로그인을 제한 할 수 있음
1. Nologin 설정 (apache:x:48:48:Apache:/home/Apache:/sbin/nologin)
2. False 설정 (apache:x:48:48:Apache:/home/Apache:/bin/false)
※ Shell부여가 되지 않는 경우도 로그인이 되지 않음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 패치 관리

<table>
<tr><td>점검 항목</td><td colspan="2">AP-07. 안정화 버전 및 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">주기적으로 보안 패치를 적용하지 않을 경우, 버전 취약점을 이용한 공격 또는 새로운 공격에 대한 침해 사고가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">판단기준</td><td>양호</td><td colspan="3">최신 패치를 적용하였을 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 패치를 적용하지 않았을 경우</td></tr>
<tr><td>점검
방법</td><td colspan="4">1. 웹 서버 버전과 최신 패치 버전을 비교하여 확인
/[Apache2 설치 디렉터리]/bin/httpd –v
 
</td></tr>
<tr><td>조치
방법</td><td colspan="4">1. Apache 사이트를 통해 주기적으로 버전 점검을 하도록 하며, 최신 버전 적용 시 충분한 테스트 후 적용할 것을 권고한다.

※ 참고 사이트 : http://httpd.apache.org/download.cgi</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

2.14. IIS

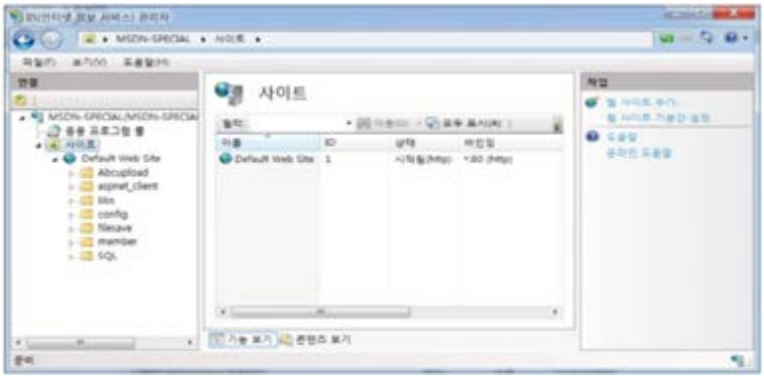
보안 설정(11개 항목), 접근 관리(2개 항목) 총 2개 영역에서 13개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 보안 설정	II-01	IIS 서비스 구동 점검	상
	II-02	IIS 불필요한 파일 제거	상
	II-03	IIS CGI 실행 제한	상
	II-04	IIS 링크 사용금지	상
	II-05	IIS 파일 업로드 및 다운로드 제한	상
	II-06	IIS DB 연결 취약점 점검	상
	II-07	IIS 가상 디렉터리 삭제	상
	II-08	IIS 데이터 파일 ACL 적용	상
	II-09	IIS 미사용 스크립트 매핑 제거	상
	II-10	IIS Exec 명령어 쉘 호출 점검	상
	II-11	IIS WebDAV 비활성화	상
나. 접근 관리	II-12	IIS 디렉터리 리스팅 제거	상
	II-13	IIS 상위 디렉터리 접근 금지	상

[표 14] IIS 진단 체크리스트

가. 보안 설정

<table>
<tr><td>진단항목</td><td colspan="2">II-01. IIS 서비스 구동 점검</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">IIS 서비스는 Web, FTP 등의 서비스를 제공해주는 유용한 서비스이지만 프로파일링, 서비스 거부, 불법적인 접근, 임의의 코드실행, 정보 공개, 바이러스, 웜, 트로이목마 등의 위협에 노출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 웹사이트가 구동 중이지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 웹사이트가 구동 중일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 불필요한 웹사이트 및 기본 웹사이트가 구동 되고 있는지 점검

■ 인터넷 정보 서비스 관리자에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0) Win2019(IIS10.0)]
1) 시작 > Win + R > inetmgr 명령어 입력
2) “기본 웹 사이트”와 “불필요한 웹 사이트” 구동 여부 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 불필요한 웹사이트가 구동 중일 경우 구동 중지 할 것을 권고

[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 윈도우 키 + R > services.msc
2) World Wide Web Publishing Service > 속성 > 일반 탭
3) 시작 유형 : 사용 안함, 서비스 상태 : 중지로 변경</td></tr>
</table>

■ 서비스를 사용하는 경우 인터넷 정보 서비스 관리자에서 변경

[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]

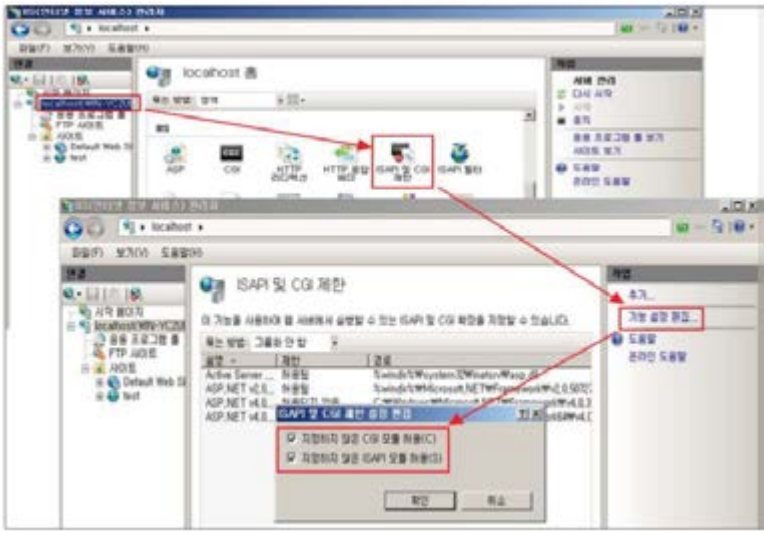
1) 시작 > Win + R > inetmgr 명령어 입력

2) "기본 웹 사이트"와 "불필요한 웹 사이트" 구동 중지

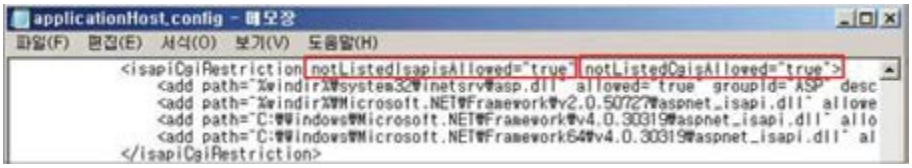
비고	

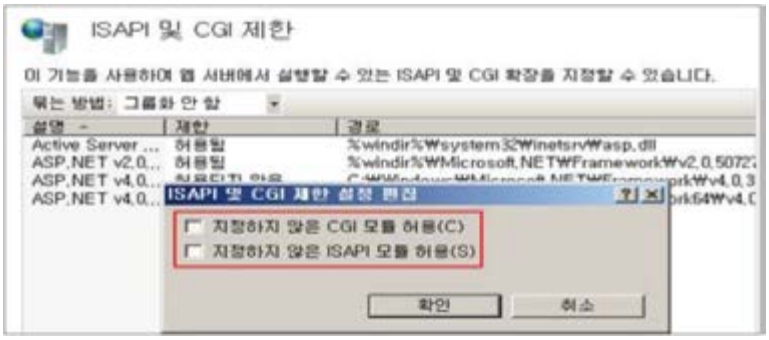
진단항목	II-02. 불필요한 파일 제거		취약도	상
항목설명	샘플 파일들은 IIS 서비스 설치 시 디폴트로 설치되는 예제 스크립트로 제거하는 것이 안전하다. IIS를 설치하면 기본적으로 예제와 설명서 등이 같이 설치되는데, 해당 폴더들은 불필요한 공격 대상으로 이용될 수 있으므로 제거하여야 한다.			
진단기준	양호	해당 웹사이트에 IISSamples, IISHelp 가상 디렉터리가 존재하지 않을 경우		
	취약	해당 웹사이트에 IISSamples, IISHelp 가상 디렉터리가 존재 할 경우		
진단방법	※ 운영 중인 웹사이트에 샘플 디렉터리 (IISHelp, IISSamples)가 존재하고 있는지 점검 ※ IIS 7.0 이상 버전은 해당 사항 없음			
조치방법	[Win2012(IIS8.0), Win2016(IIS10.0), Wind2019(IIS10.0)] IIS7.0 이상 버전은 가상디렉토리가 존재하지 않으므로 해당사항 없음			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">II-03. IIS CGI 실행 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">CGI 스크립트는 정해진 디렉터리에서만 실행되도록 해야 하며, 게시판이나 자료실과 같이 업로드 되는 파일이 저장되는 디렉터리에 CGI 스크립트가 실행 가능하다면 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고로 이어질 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">지정하지 않은 CGI 모듈 허용 및 지정하지 않은 ISAPI 모듈 허용을 사용하지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">지정하지 않은 CGI 모듈 허용 및 지정하지 않은 ISAPI 모듈 허용을 사용할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ CGI 디렉터리(기본값 C:₩inetpub₩scripts)에 Everyone의 모든 권한, 수정 권한, 쓰기 권한이 부여되어 있는지 점검

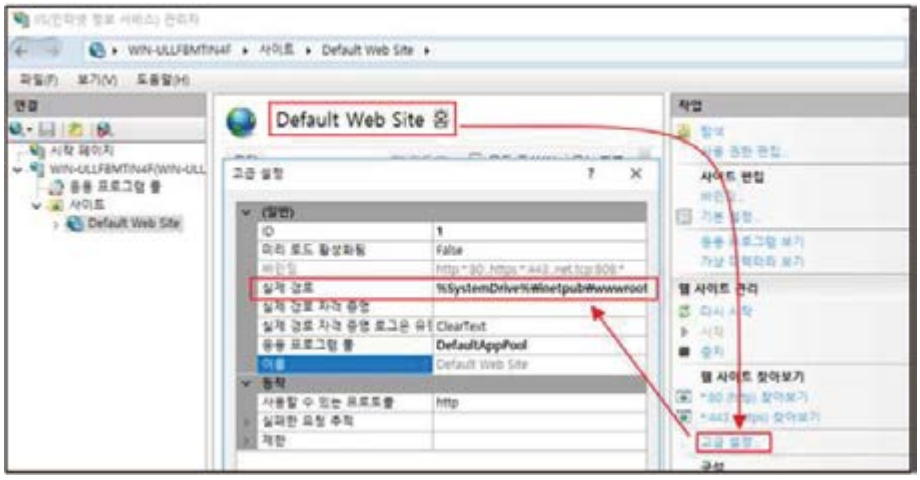
■ IIS 관리자에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019]
1) IIS 관리자 > 서버 선택 > ISAPI 및 CGI 제한 > 기능 설정 편집
2) “지정하지 않은 CGI 모듈 허용” 및 “지정하지 않은 ISAPI 모듈 허용”에 체크 해제되어 있는지 확인
 

■ 설정 파일에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 탐색기 > C:₩Windows₩System32₩inetsrv₩config > applicationHost.config 파일 Open
2) “notListedIsapisAllowed” 값과 “notListedCgisAllowed” 값이 모두 “false”로 되어 있는지 확인</td></tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>조치방법</td><td>※ 지정하지 않은 CGI 모듈 허용 또는 지정하지 않은 ISAPI 모듈 허용을 사용하면 서버가 CGI 또는 ISAPI 기술을 악용하는 컴퓨터 바이러스나 웜에 감염될 수 있으므로 보안상 위험

▪ IIS 관리자에서 설정 변경
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) IIS 관리자 > 서버 선택 > ISAPI 및 CGI 제한 > 기능 설정 편집
2) "지정하지 않은 CGI 모듈 허용" 및 "지정하지 않은 ISAPI 모듈 허용"에 체크 해제
 
</td></tr>
<tr><td>비고</td><td>적용 시 벤더 및 개발자 협의 필요</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">II-04. IIS 링크 사용금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">공개적인 웹 콘텐츠 디렉터리 안에서 서버의 다른 디렉터리나 파일들에 접근할 수 있는 심볼릭 링크, aliases, 바로가기 등을 사용하지 않도록 해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">홈 디렉터리에 바로가기 등의 링크 파일이 존재하지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">홈 디렉터리에 바로가기 등의 링크 파일이 존재 할 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 해당 디렉터리에 바로가기 파일 있는지 점검

▪ 홈 디렉터리에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > 작업 > 고급 설정 > 실제 경로 확인
3) 홈 디렉터리로 이동 후 바로가기 파일이 존재하는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">※ 홈 디렉터리로 이동하여 바로가기 파일 삭제

[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > 작업 > 고급 설정 > 실제 경로 확인
3) 홈 디렉터리로 이동 후 바로가기 파일 삭제</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	II-05. IIS 파일 업로드 및 다운로드 제한	취약도	상
항목설명	불필요한 파일 업로드, 다운로드 시에, 대량의 업로드, 다운로드로 인한 서비스 불능 상태가 발생한다. 불필요한 업로드와 다운로드는 허용하지 않으며, 웹서버에 의해 처리되지 못하게 해야 하며, 자동이나 수동으로 파일의 보안성 검토를 하도록 해야 한다.		
진단기준	양호	웹서비스 서버의 업로드, 다운로드 용량을 제한한 경우	
	취약	웹서비스 서버의 업로드, 다운로드 용량을 제한하지 않은 경우	
진단방법	※ ASP의 경우 업로드 기능을 제공하지 않으므로 특정 컴포넌트를 이용하여 업로드 기능을 구현. 이때 컴포넌트별로 업로드 용량 설정 방법이 다르나 공통적으로 요청 필터링에서 설정하는 "허용되는 최대 콘텐츠 길이" 설정에서 적용할 수 있음 ■ 탐색기에서 파일 다운로드 용량 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) C:₩windows₩system32₩inetsrv₩config₩applicationHost.config를 찾아서 편집기로 Open 2) maxRequestEntityAllowd 및 buffringLimit 값이 적절히 설정되어 있는지 확인 ■ 탐색기에서 파일 업로드 용량 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) C:₩windows₩system32₩inetsrv₩config₩applicationHost.config를 찾아서 편집기로 Open 2) maxAllowedContentLength 값이 적절히 설정되어 있는지 확인 인터넷 정보 서비스 관리에서 파일 다운로드 용량 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) Win + R > inetmgr 명령어 입력 2) 운영 중인 웹사이트 > ASP > 제한속성 3) "응답 버퍼링 제한"과 "최대 요청 엔터티 본문 제한"에 적절한 설정이 되어 있는지 확인 ■ 인터넷 정보 서비스 관리에서 파일 업로드 용량 확인 [Win2008(IIS7,0), Win2012(IIS8.0), Win2016(IIS10.0)] 1) Win + R > inetmgr 명령어 입력 2) 운영 중인 웹 사이트 > 요청 필터링 > 기능 설정 편집 3) "허용되는 최대 콘텐츠 길이"에 적절한 설정이 되어 있는지 확인		

조치방법

※ 파일 업로드 및 다운로드 용량을 허용할 수 있는 최소 범위로 설정

■ 탐색기에서 파일 다운로드 용량 설정 변경

[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]

1) 시작 > 실행 > services.msc > IIS Admin Service > 속성 > 정지 > 사용 안함
2) C:₩windows₩system32₩inetsrv₩config₩applicationHost.config를 찾아서 편집기로 Open
3) <system.webServer> 부분에 아래와 같이 추가 또는 변경

```
<location path="웹 사이트 이름">
  <system.webServer>
    <asp>
      <cache diskTemplateCacheDirectory="%SystemDrive%₩inetpub₩temp₩ASP Compiled Templates" />
      <limits buffringLimit="파일크기" maxRequestEntityAllowed="파일크기"/>
    </asp>
  </system.webServer>
```

■ 탐색기에서 파일 업로드 용량 설정 변경

[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]

1) 시작 > 실행 > services.msc > IIS Admin Service > 속성 > 정지 > 사용안함

	2) C:₩windows₩system32₩inetsrv₩config₩applicationHost.config를 찾아서 편집기로 Open 3) <system.webServer> 부분에 아래와 같이 추가 또는 변경 <location path="웹 사이트 이름"> <system.webServer> <security> <requestFiltering> <requestLimits masAllowedContentLength="파일크기" /> </requestFiltering> </security> </system.webServer> ■ 인터넷 정보 서비스 관리에서 파일 다운로드 용량 설정 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) Win + R > services.msc > IIS Admin Service > 속성 > 중지 2) Win + R > inetmgr 명령어 입력 3) 운영 중인 웹사이트 > ASP > 제한속성 4) "응답 버퍼링 제한"과 "최대 요청 엔터티 본문 제한"에 적절한 설정 5) Win + R > services.msc > World Wide Web Publishing Service > 속성 > 시작 ■ 인터넷 정보 서비스 관리에서 파일 업로드 용량 설정 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) Win + R > services.msc > IIS Admin Service > 속성 > 중지 2) Win + R > inetmgr 명령어 입력 3) 운영 중인 웹사이트 > 요청 필터링 > 기능 설정 편집 4) "허용되는 최대 콘텐츠 길이"에 적절한 설정 5) Win + R > services.msc > World Wide Web Publishing Service > 속성 > 시작
비고	■ IIS 7.0 이상은 별도의 설정을 하지 않을 경우 IIS.schema.xml의 Default 설정이 적용됨 - 파일 위치 : C:₩windows₩system32₩inetsrv₩config₩schema₩IIS_schema.틔 - Default 다운로드 제한 = 4194304바이트 업로드 제한 = 200000바이트 ■ IIS 7.0 이상 콘텐츠 용량 제한 30M - 콘텐츠 용량 = 콘텐츠 내용 + 이미지 + 첨부파일

진단항목	II-06. IIS DB 연결 취약점 점검		취약도	상
항목설명	Global.asa 파일에는 데이터베이스 관련 정보(IP 주소, DB명, 패스워드), 내부 IP 주소, 웹 애플리케이션 환경설정 정보 및 기타 정보 등 보안상 민감한 내용이 포함되어 있으므로 해당 파일이 악의적인 사용자에게 노출될 경우 침해사고로 이어질 수 있다.			
진단기준	양호	.asa 매핑이 존재 할 경우		
	취약	.asa 매핑이 존재하지 않을 경우		
진단방법	▪ 인터넷 정보 서비스 관리에서 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] ※ IIS 6.0 이상 버전은 해당 취약점에 대한 패치가 되어 있으므로 해당사항 없음(N/A)			
조치방법	[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] ※ IIS 6.0 이상 버전은 해당 취약점에 대한 패치가 되어 있으므로 해당사항 없음(N/A)			
비고	※ 해당 취약점에 영향을 받는 플랫폼 - Microsoft Internet Information Services 4.0 - Microsoft Internet Information Services 5.0 - Microsoft Active Server Pages 4.0			

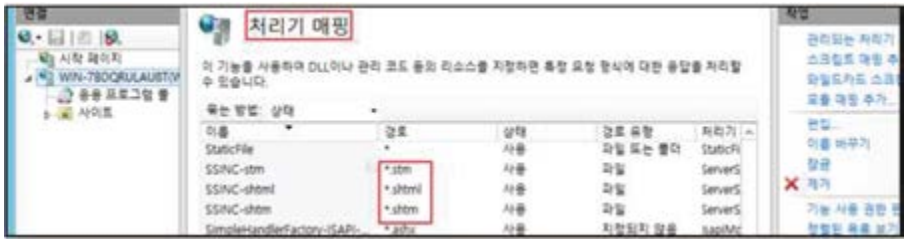
진단항목	II-07. IIS 가상 디렉터리 삭제	취약도	상
항목설명	IIS 설치 시 기본적으로 /iisadmpwd라는 가상 디렉터리를 생성하는데, 이 디렉터리에는 웹 서버를 통하여 패스워드를 변경시켜주는 기능 등을 하는 .HTR 파일이 존재한다. 이러한 기능들이 필요하지 않을 경우 /issadmpwd를 제거한다. 이 외 존재할 수 있는 취약점을 줄이기 위해서 IISADMIN에 관계되는 모든 파일 및 디렉터리를 삭제한다.		
진단기준	양호	IIS Admin, IIS Adminpwd 가상 디렉터리가 존재하지 않을 경우	
	취약	IIS Admin, IIS Adminpwd 가상 디렉터리가 존재할 경우	
진단방법	※ 보안상 취약한 가상 디렉터리(IIS Admin, IIS Adminpwd)를 사용하고 있는지 점검한다. ※ IIS 7.0 이상 버전은 해당 사항 없음		
조치방법	※ 보안상 취약한 가상 디렉터리(IIS Admin, IIS Adminpwd)를 사용하고 있는지 점검한다. ※ IIS 7.0 이상 버전은 해당 사항 없음		
비고			

<table>
<tr><td>진단항목</td><td colspan="2">II-08. IIS 데이터 파일 ACL 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">웹 데이터 파일에 ACL을 부여함으로서 권한 없는 사용자로부터의 실행 및 읽기 제한을 설정 할 수 있다. 향후 필요에 의하여 IIS를 설치하여 운용한다면 웹 데이터 파일에 대한 ACL을 부여하는 것이 바람직하며 ACL을 설정할 때에는 다음과 같은 사항을 참고하여 설정해야 한다.
1. 가능한 파일의 종류끼리 분류하여 폴더에 저장하는 것이 좋음
2. 홈 디렉터리(기본: C:₩inetpub₩wwwroot)내에 적절한 ACL 권한을 부여함</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않는 경우(정적 콘텐츠 파일은 Read 권한만)</td></tr>
<tr><td>취약</td><td colspan="3">홈 디렉터리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하는 경우(정적 콘텐츠 파일은 Read 권한 제외)</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 부적절한 파일 접근, 열람 및 삭제 가능 여부를 점검

■ 인터넷 정보 서비스 관리에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > 기본 설정 > 실제 경로 확인
3) 아래와 같은 파일들에 대한 불필요한 Everyone 권한이 존재하는지 확인
<table>
<tr><th>파일 형식</th><th>액세스 제어 목록</th></tr>
<tr><td>CGI(*.exe, *.dll, *.cmd, *pl)</td><td>모든 사람(X), 관리자/시스템(전체 제어)</td></tr>
<tr><td>스크립트 파일(*.asp)</td><td>모든 사람(X), 관리자/시스템(전체 제어)</td></tr>
</table></td></tr>
<tr><td>조치방법</td><td colspan="4">※ C:₩Inetpub₩wwwroot 디렉터리에 Administrators, System 추가(모든권한), Everyone Read만 설정 후 하위 디렉터리에 존재하는 CGI, 스크립트 파일, 포함파일에 Everyone 권한 모두 제거

■ 인터넷 정보 서비스 관리에서 변경
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > 기본 설정 > 실제 경로 확인
3) 상단과 같은 파일들에 대한 불필요한 Everyone 권한 제거</td></tr>
<tr><td>비고</td><td colspan="4">조치 시 마스터 속성과 모든 사이트에 적용함</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">II-09 미사용 스크립트 매핑 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용하지 않는 스크립트 매핑은 보안에 위협이 될 수 있으므로 개발자와 협의하여 불필요한 매핑인지 확인한 후에 제거하여야 하며, .asp나 .shtm과 같은 확장자들은 특정 DLL 파일과 매핑되어 있어, 이러한 파일들에 대한 요청이 들어오면 해당 DLL에 의해 처리되어진다. 이러한 매핑 가운데는 사용되지 않는 것들이 있어서 이를 제거해주는 것이 보안에 도움이 된다.
.ida, .idc, .idq, .printer, .htr, .htw 확장자는 Buffer overflow 공격 위험이 존재 하므로 삭제를 권고한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 불필요한 매핑확인 및 제거 점검한다.

▪ 인터넷 정보 서비스 관리에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 시작 > Win + R >inetmgr 명령어 입력
2) 해당 웹사이트 > 처리기 매핑 선택
3) 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하는지 확인
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 인터넷 정보 서비스 관리에서 변경
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 시작 > Win + R >inetmgr 명령어 입력
2) 해당 웹사이트 > 처리기 매핑 선택
3) 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq) 삭제</td></tr>
<tr><td>비고</td><td colspan="4">※ 조치 시 마스터 속성과 모든 사이트에 적용함
※ 취약한 매핑</td></tr>
</table>

확장자명	기능	취약점
asp	Active Server Pages 기능 지원	Buffer Overflow s02-018 • Win 2000 SP3 이상 양호
htr	Web-based password reset: Outlook Web Access등에서 웹기반 응용 프로그램으로 자신의 사용자 계정 암호 변경	+.htr 소스 공개 취약점 MS01-004 • Win 2000 SP3 이상 양호
idc	Internet Database Connector: SQL 서버에 연결하기 위한 정보 등을 관리함. asp를 통해 같은 작업을 수행 가능	Web 디렉터리패스 공개 Q 193689 • NT4.0, NT SP6a이상 양호
stm, shtm, shtml	Server-Side Includes	Buffer Overflow MS01-044 • Win 2000 SP3 이상 양호
printer	Internet Printing : URL을 사용하여 페이지를 프린터로 인쇄할 수 있도록 함. IIS가 인터넷이나 인트라넷을 통해 인쇄 서버 기능 수행	Buffer Overflow MS01-023 • Win 2000 SP2 이상 양호
ida, idq	Index Server : idq.dll에 매핑되며 인덱스 서버를 쿼리할 때 사용	Buffer Overflow MS01-033 • Win 2000 SP3 이상 양호
htw	Index Server : webhits.dll에 매핑되며 인덱스 서버를 쿼리할 때 사용	Webhit 소스 공개취약점 MS00-006 • Win 2000 SP1 이상 양호

※ IIS 7.0부터 .idc, .printer와 같은 불필요한 매핑이 제거되어 있음

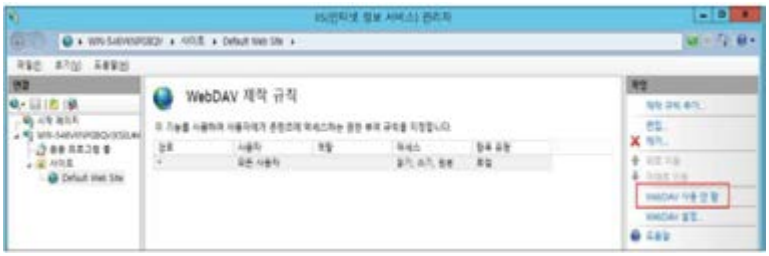
진단항목	II-10 IIS Exec 명령어 쉘 호출 점검	취약도	상
항목설명	명령어가 Web 서버에서 임의의 명령을 호출 하도록 사용될 수 있다. 임의의 명령을 호출 하도록 설정되어 있다면 아래의 조치 방법에 따라서 설정을 변경하여 주는 것이 안전하다. HTML 페이지에서 웹 서버에 명령어 실행은 # exec 명령어를 통해 활용이 가능하다. 기본 값으로 IIS 4.0에서는 이 명령어가 사용 가능하지만, IIS 5.0 에서는 기본 값으로 사용이 불가능하다. 기본 값은 서버 측의 허가되지 않은 실행구의 동작을 방지하기 위해 변경되었다.		
진단기준	양호	IIS 5.0 버전에서 해당 레지스트리 값이 0 이거나, IIS 6.0 이상일 경우 양호	
	취약	IIS 5.0 버전에서 해당 레지스트리 값이 1인 경우, IIS 6.0이후 해당 항목에 대해 패치가 적용되어 있으므로 양호함	
진단방법	■ 레지스트리에서 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) 시작 > 실행 > regedit 2) HKLM₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters 3) SSIEnableCmdDirective 값이 존재하는지 확인 ※ IIS 버전 5.0부터 SSIEnableCmdDirective 레지스트리 속성의 기본 값은 false임 (즉 레지스트리 값이 존재하지 않을 경우 false임)		
조치방법	■ 레지스트리 값 설정 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) 시작 > 실행 > regedit > HKLM₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters 2) 새로 만들기 > DWORD > SSIEnableCmdDirective 라는 값을 찾아 오른쪽 버튼을 눌러 값을 0으로 입력(없을 경우 새로 생성)		
비고	■ 변경사항 적용을 위해 웹 서비스 정지 후 재시작 ■ 명령을 통한 정지, 시작은 다음과 같이 실행 1) 시작 > 실행 > 층* 2) C:> net stop w3svc 3) C:> net start w3svc		

<table>
<tr><td>진단항목</td><td colspan="2">II-11 IIS WebDAV 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">악의적으로 작성된 요청을 이용하여 특별한 방식으로 인증을 우회할 경우 패스워드로 보호된 *WebDAV에 의해 호출된 구성 요소 중 하나에 결함이 존재하며, 이로 인해 버퍼 오버런이 일어날 수 있다.

* WebDAV(Web Distributed Authoring and Versioning): 웹상의 공동개발을 지원하기 위한 IETF 표준안(RFC 2518)으로서, 원격지 사용자들 간에 인터넷상에서 파일을 공동 편집하고 관리 할 수 있도록 해준다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">다음 중 한 가지라도 해당하는 경우
- IIS 서비스를 사용하지 않는 경우
- DisableWebDAV 값이 1로 설정되어 있는 경우
- Windows NT, 2000은 서비스팩 4 이상이 설치되어 있는 경우
- Win2003, Win2008, Win2012에서 WebDAV가 금지 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">양호기준에 한가지라도 해당되지 않을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ WebDAV항목이 금지되어 있는지 점검 (IIS 6.0 이상은 Default로 금지됨)
※ WevDAV 레지스트리 경로
HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Service₩W3SVC₩Parameters

■ 서비스에서 IIS 구동 상태 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > services.msc > World Wide Web Publishing Service > 속성
2) 시작 유형 : 사용 안함 / 서비스 상태 : 중지로 설정되어 있는지 확인

■ 인터넷 정보 서비스 관리에서 WebDAV 상태 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr
2) 해당 웹 사이트 > WebDAV 제작 규칙 > WebDAV 활성화 여부 확인
  </td></tr>
</table>

	
조치방법	■ 서비스에서 IIS 구동 상태 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) Win + R > services.msc > World Wide Web Publishing Service > 속성 2) 시작 유형 : 사용 안 함 / 서비스 상태 : 중지로 변경 ■ 인터넷 정보 서비스 관리에서 WebDAV 상태 확인 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) Win + R > inetmgr 2) 해당 웹 사이트 > WebDAV 제작 규칙 > WebDAV 사용 안 함 클릭 
비고	■ 인증 우회 취약점에 영향받는 플랫폼 - Microsoft Internet Information Services 5.0 - Microsoft Internet Information Services 6.0 ※ 익명 파일 업로드가 가능한 IIS 6.0의 WevDAV와는 다르게, IIS 7.0에서의 WebDAV는 강화된 보안설계 변경으로 인해 WebDAV를 허용한 후에도 익명 사용자가 WebDAV를 통해 쓰기를 시도하는 경우, 'HTTP 401.0 Access is denied. (0x80070005)' 또는 'HTTP 401 Unauthorized' 에러가 발생 ■ 원격 코드 실행에 영향받는 플랫폼 - Microsoft Internet Information Services 6.0

나. 접근 관리

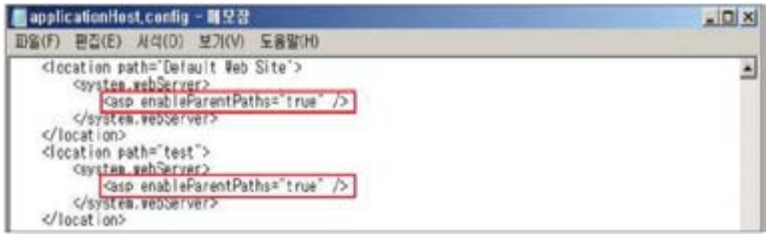
<table>
<tr><td>진단항목</td><td colspan="2">II-12 IIS 디렉터리 리스팅 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">디렉터리 검색 기능이 활성화되어 있으면 IIS 기본파일(default.asp, default.htm)이 서버에 없는 경우 해당 디렉터리에 존재하는 모든 파일의 리스트를 보여주어, Web 서버 구조 노출 및 주요 설정 파일의 내용이 유출될 가능성이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">"디렉터리 검색"이 체크되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">"디렉터리 검색"이 체크되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 운영 중인 웹사이트의 디렉터리 검색 기능이 설정되어 있는지 점검

▪ 인터넷 정보 서비스 관리자에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 시작 > Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > IIS > 디렉터리 검색 > 작업 > 디렉터리 검색 옵션이 활성화 되어있는지 확인
  </td></tr>
<tr><td>조치방법</td><td colspan="4">※ 운영 중인 웹사이트의 디렉터리 검색 기능을 제한(체크해제)

▪ 인터넷 정보 서비스 관리자에서 변경
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > IIS > 디렉터리 검색 > 작업 > 사용 안 함 선택</td></tr>
<tr><td>비고</td><td colspan="4">조치 시 마스터 속성과 모든 사이트에 적용함</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">II-13 IIS 상위 디렉터리 접근 금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">상위경로로 이동하는 것이 가능할 때 하위경로에 접속하여 상위로 이동함으로써 해킹을 당할 위험이 있으며, Unicode 버그 및 서비스 거부 공격에 이용당하기 쉬우므로 되도록이면 “.” 와 같은 상위 경로를 사용하지 못하도록 설정하는 것이 바람직하다. “.”는 unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">상위 패스 기능을 제거한 경우</td></tr>
<tr><td>취약</td><td colspan="3">상위 패스 기능을 제거하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">※ 상위경로 사용 여부를 확인한다.

■ 인터넷 정보 서비스 관리자에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) Win + R > inetmgr 명령어 입력
2) 해당 웹사이트 > IIS > ASP > 부모 경로 사용 항목이 False로 되어있는지 확인
 

■ 설정 파일에서 확인
[Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)]
1) 탐색기 > C:₩Windows₩System32₩inetsrv₩config > 파일 Open
2) 사용 중인 웹사이트의 하위 설정에 “enableParentPaths”의 값이 “false”로 되어 있는지 확인
 
</td></tr>
</table>

조치방법	※ 상위경로 사용 안 함으로 설정 ▪ 인터넷 정보 서비스 관리자에서 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) 시작 > Win + R > inetmgr 명령어 입력 2) 해당 웹사이트 > IIS > ASP > 부모 경로 사용 항목이 False 로 변경 ▪ applicationHost.config 파일에서 설정 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 탐색기 > %Windir% > system32 > inetsrv > applicationHost.config 파일을 메모장으로 열어서 아래와 같이 설정 <location path="Default Web Site(웹 사이트 이름)"> <system.webServer> <asp enableParentPaths="false" /> </system.webServer> </location> ▪ appcmd 유틸리티를 이용하여 설정 변경 [Win2012(IIS8.0), Win2016(IIS10.0), Win2019(IIS10.0)] 1) 시작 > 실행 > cmd 2) cd %systemroot%₩System32₩inetsrv로 이동 후 아래의 명령어를 입력 3) appcmd.exe set config "Default Web Site(웹 사이트 이름)" -section:system.webServer/asp/enableParentPaths:"False"/commit:apphost
비고	▪ IIS 7.0 이상은 별도의 설정을 하지 않을 경우 IIS_schema.xml의 Default 설정이 적용됨. - 파일 위치 : C:₩windows₩system32₩inetsrv₩config₩schema₩IIS_schema.xml - Default 설정 : <attribute name="enableParentPaths" type="bool" defaultValue="false" /> ※ 애플리케이션에서 "../" 와 같이 상대경로를 사용하도록 코딩되어 있을 경우 영향 있음 ※ 조치 시 마스터 속성과 모든 사이트에 적용함

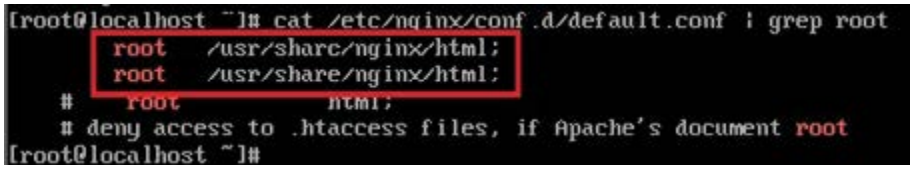
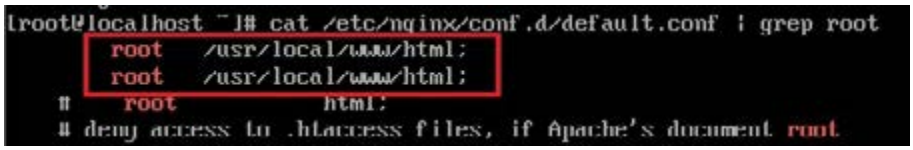
2.15. NginX

보안 설정(4개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목) 총 3개 영역에서 7개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 보안 설정	NG-01	웹 서비스 영역의 분리	상
	NG-02	불필요한 파일 제거	상
	NG-03	링크 사용금지	상
	NG-04	파일 업로드 및 다운로드 제한	상
나. 접근 관리	NG-05	디렉토리 리스팅 제거	상
	NG-06	웹 프로세스 권한 제한	상
다. 패치 관리	NG-07	안정화 버전 및 패치 적용	상

[표 15] NginX 진단 체크리스트

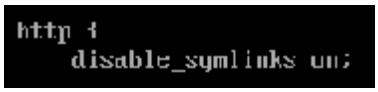
가. 보안 설정

<table>
<tr><td>진단항목</td><td colspan="2">NG-01. 웹 서비스 영역의 분리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Nginx 설치 시 html 디렉터리를 root로 사용하고 있는데 html 디렉터리는 공개되어서는 안 될(또는, 공개될 필요가 없는) Nginx 문서뿐만 아니라 공격에 이용될 수 있는 시스템 관련 정보도 포함하고 있으므로 이를 변경하여야 한다. 또한, 대량의 업로드와 다운로드 시 서비스 불능 상태가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">root를 별도의 디렉터리로 지정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">root를 기본 디렉터리로 지정한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 기본 디렉터리 확인
1) [설치위치]/conf.d/default.conf 파일에서 root 디렉터리 확인
cat [설치위치]/default.conf | grep root
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 기본 디렉터리 변경
1) root 위치 변경
2) # vi [설치위치]/default.conf // 별도의 디렉터리로 지정
3) # cat [설치위치]/default.conf
  </td></tr>
<tr><td>비고</td><td colspan="4">▪ Nginx의 default 디렉터리는 [설치위치]/html</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">NG-02. 불필요한 파일 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">웹 서버 설치 시 기본으로 생성되는 매뉴얼 파일은 외부 침입자에게 시스템 정보 및 웹 서버 정보를 제공할 수 있으므로 제거하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">매뉴얼 파일 및 디렉터리가 제거되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">매뉴얼 파일 및 디렉터리가 제거되지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 매뉴얼 디렉터리 존재여부 확인
1) 운영상 불필요한 파일이 존재하는지 확인(test, old, bak파일이 존재하는지 확인)
cd [설치 디렉터리]</td></tr>
<tr><td>조치방법</td><td colspan="4">※ 웹 서버를 정기적으로 검사하여 임시 파일들을 삭제하도록 해야함. 특히 웹 서비스의 업데이트나 유지보수 시 생성되는 백업파일이나 중요한 파일 등은 작업이 끝난 후 반드시 삭제 해야함. 정확한 관리를 위해 폴더와 파일의 이름과 위치, 개수 등이 적혀있는 별도의 문서를 관리하는 것이 좋으며 문서에 등록되지 않은 불필요한 파일들을 점검해서 삭제하도록 해야함

■ 매뉴얼 디렉터리 삭제
1) 운영상 불필요한 파일이 존재할 경우 제거
cd [설치 디렉터리]
rm -rf [해당 파일명]</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

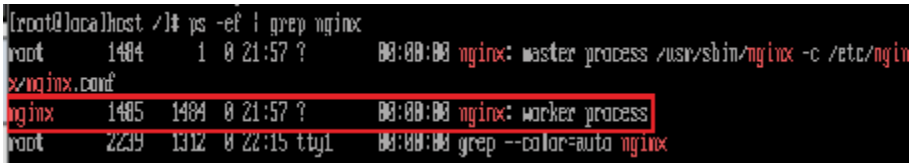
<table>
<tr><td>진단항목</td><td colspan="2">NG-03. 링크 사용금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">일부 서버는 “심볼릭 링크(Symbolic link)를 이용하여 기존의 웹 문서 이외의 파일 시스템 접근이 가능하도록 하고 있다. 이러한 방법은 편의성을 제공하는 반면, 일반 사용자들도 시스템 중요 파일에 접근할 수 있게 하는 보안 문제를 발생시킨다. 가령 시스템 자체의 root 디렉터리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한(nobody)으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 “/etc/passwd" 파일과 같은 민감한 파일을 누구나 열람할 수 있게 된다.

* 심볼릭 링크(Symbolic link, 소프트 링크) : 윈도우 운영체제의 바로가기 아이콘과 비슷하다. 링크 생성 시 파일 내용은 존재하지 않으나 사용자가 파일을 요청하면 링크가 가리키고 있는 원본 데이터에서 데이터를 가져와서 전달한다. 직접 원본을 가리키지 않고 원본 데이터를 가리키는 포인터를 참조함으로써 원본데이터가 삭제, 이동, 수정이 되면 사용 불가능 하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">심볼릭 링크 사용을 제한한 경우</td></tr>
<tr><td>취약</td><td colspan="3">심볼릭 링크 사용을 제한하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 심볼릭 링크 사용을 제한여부 확인
1) nginx.conf 파일에서 disable_symlinks 확인
2) # cat [설치위치]/nginx.conf | grep disable_symlinks</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 심볼릭 링크 사용을 제한 설정
1) nginx.conf 파일에서 disable_symlinks 적용
 
2) # vi [설치위치]/nginx.conf</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">NG-04. 파일 업로드 및 다운로드 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">불필요한 파일 업로드, 다운로드 시에 대량의 업로드, 다운로드로 인한 서비스 불능상태가 발생할 수 있다. 따라서 불필요한 업로드와 다운로드는 허용하지 않으며, 웹 서버에 의해 처리되지 못하게 하고, 자동이나 수동으로 파일의 보안성 검토를 수행한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">파일 업로드 및 다운로드 용량을 제한한 경우</td></tr>
<tr><td>취약</td><td colspan="3">파일 업로드 및 다운로드 용량을 제한하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 파일 업로드 및 다운로드 용량을 제한 설정 확인
1) nginx.conf 파일에 용량이 적절히 설정되어 있는지 확인
cat [설치위치]/nginx.conf | grep client_max_body_size</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 파일 업로드 및 다운로드 용량을 제한 설정
1) nginx.conf 파일에 용량을 시스템에 따라 적절하게 설정
(예시)
vi [설치위치]/nginx.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

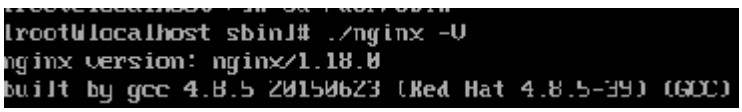
나. 접근 관리

<table>
<tr><td>진단항목</td><td colspan="2">NG-05. 디렉터리 리스팅 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">디렉터리 검색은 디렉터리 요청 시 해당 디렉터리에 기본 문서가 존재하지 않을 경우 디렉터리 내 모든 파일의 목록을 보여주는 기능이다. 디렉터리 검색 기능이 활성화되어 있는 경우 외부에서 디렉터리 내의 모든 파일에 대한 접근이 가능하여 WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스 파일 등 공개되어서는 안 되는 중요 파일 노출이 가능하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">디렉터리 검색 기능을 사용하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">디렉터리 검색 기능을 사용하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 디렉터리 검색 기능을 사용여부 확인
1) nginx.conf 파일에 autoindex가 적절히 설정되어 있는지 확인
cat [설치 위치]/nginx.conf | grep autoindex</td></tr>
<tr><td>조치방법</td><td colspan="4">■ nginx.conf 파일에 autoindex 설정
vi [설치위치]/nginx.conf
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">NG-06. 웹 프로세스 권한 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Linux 시스템의 경우 Web 서버 데몬이 root 권한으로 운영될 경우 Web Application의 취약점 또는, 버퍼 오버플로우(Buffer Overflow)로 인하여 root 권한을 획득할 수 있으므로 서버 데몬이 root 권한으로 운영되지 않도록 관리하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">nginx 데몬이 root 권한으로 구동되지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">nginx 데몬이 root 권한으로 구동되는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 웹 서버 프로세스 소유자의 권한을 확인
ps -ef | grep nginx
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ nginx.conf 파일에서 Root 권한으로 구동되고 있을 경우, nginx 데몬 User/Group 변경
 

■ # vi [설치 위치]/nginx.conf
■ /etc/passwd 파일에서 Nobody나 그 외의 별도 계정을 생성하여 구동 중일 경우, 변경된 계정이 로그인이 되지 않도록 제한
■ # vi /etc/passwd
- /sbin/nologin 설정 또는 /bin/false 설정
 
</td></tr>
<tr><td>비고</td><td colspan="4">■ 디폴트가 nobody로 설정되어 있으며 아무런 설정이 존재하지 않는 경우 nobody로 설정됨</td></tr>
</table>

다. 패치 관리

<table>
<tr><td>진단항목</td><td colspan="2">NG-07. 안정화 버전 및 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">주기적으로 보안 패치를 적용하지 않을 경우, 버전 취약점을 이용한 공격 또는 새로운 공격에 대한 침해 사고가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 패치를 적용하였을 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 패치를 적용하지 않았을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 웹 서버 버전과 최신 패치 버전을 비교하여 확인
cd /usr/sbin
./nginx -V
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Nginx 사이트를 통해 주기적으로 버전 점검을 하도록 하며, 최신 버전 적용 시 충분한 테스트 후 적용할 것을 권고

※ 참고 사이트 : https://nginx.org/</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

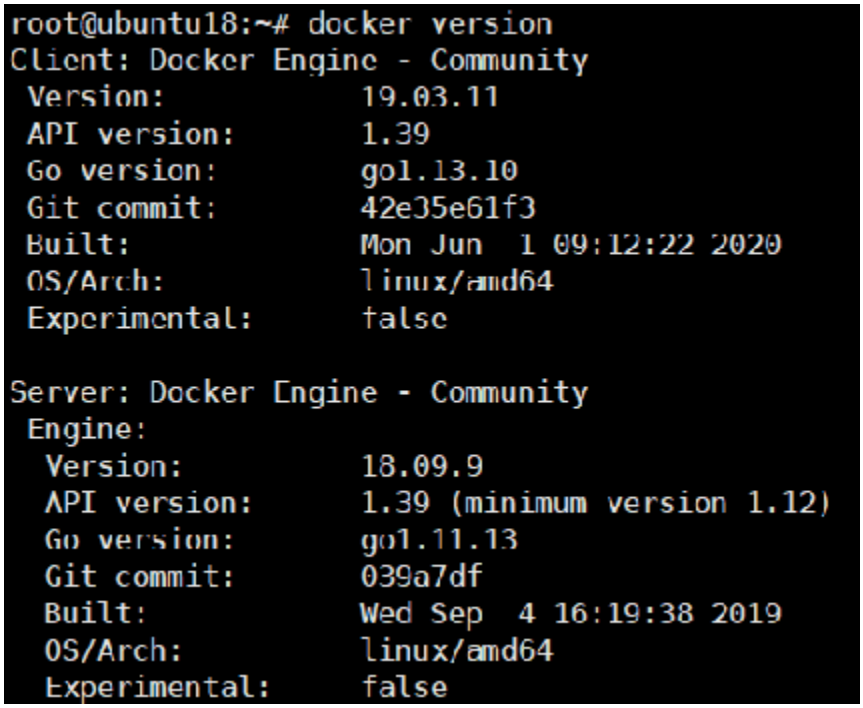
2.16. Docker

Host 설정(8개 항목), 도커 데몬 설정(4개 항목), 도커 데몬 설정 파일(12개 항목), 컨테이너 이미지 및 빌드 파일(2개 항목) 컨테이너 런타임(6개 항목) 총 5개 영역에서 32개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. Host 설정	DO-01	도커 최신 패치 적용	상
	DO-02	도커 그룹에 불필요한 사용자 제거	중
	DO-03	Docker daemon audit 설정	상
	DO-04	/var/lib/docker audit 설정	상
	DO-05	/etc/docker audit 설정	상
	DO-06	docker.service audit 설정	상
	DO-07	docker.socket audit 설정	상
	DO-08	/etc/default/docker audit 설정	상
나. 도커 데몬 설정	DO-09	default bridge를 통한 컨테이너 간 네트워크 트래픽 제한	상
	DO-10	도커 클라이언트 인증 활성화	상
	DO-11	legacy registry (v1) 비활성화	하
	DO-12	추가 권한 획득으로부터 컨테이너 제한	중
다. 도커 데몬 설정 파일	DO-13	docker.service 소유권 설정	상
	DO-14	docker.service 파일 접근권한 설정	상
	DO-15	docker.socket 소유권 설정	상
	DO-16	docker.socket 파일 접근권한 설정	상
	DO-17	/etc/docker 디렉터리 소유권 설정	상
	DO-18	/etc/docker 디렉터리 접근권한 설정	상
	DO-19	/var/run/docker.sock 파일 소유권 설정	상
	DO-20	/var/run/docker.sock 접근권한 설정	상
	DO-21	daemon.json 파일 소유권 설정	중
	DO-22	daemon.json 파일 접근권한 설정	중
	DO-23	/etc/default/docker 파일 소유권 설정	상
	DO-24	/etc/default/docker 파일 접근권한 설정	상
라. 컨테이너 이미지 및 빌드 파일	DO-25	root가 아닌 user로 컨테이너 실행	중
	DO-26	도커를 위한 컨텐츠 신뢰성 활성화	중
마. 컨테이너 런타임	DO-27	컨테이너 SELinux 보안 옵션 설정	중
	DO-28	컨테이너에서 ssh 사용 금지	상
	DO-29	컨테이너에 privileged 포트 매핑 금지	중
	DO-30	PIDs cgroup 제한	상
	DO-31	도커의 default bridge docker0 사용 제한	하
	DO-32	호스트의 user namespaces 공유 제한	하

[표 16] Docker 점검 체크리스트

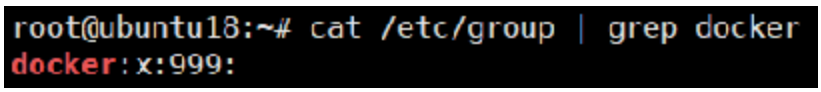
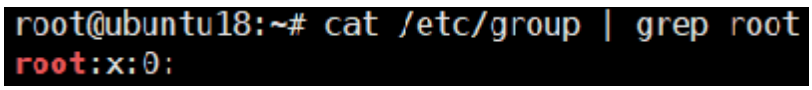
가. Host 설정

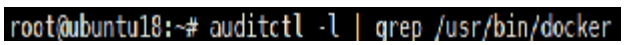
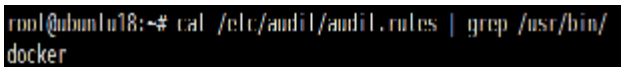
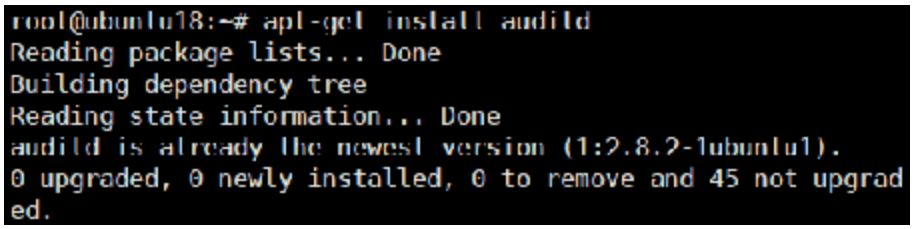
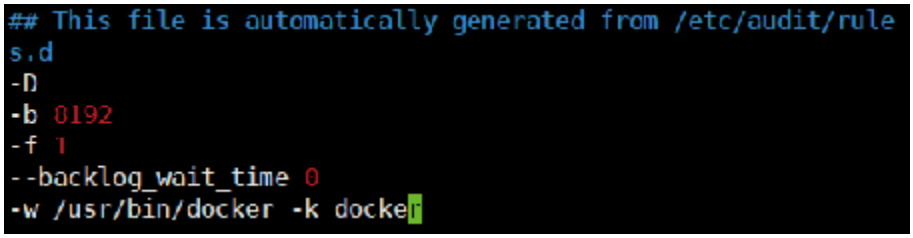
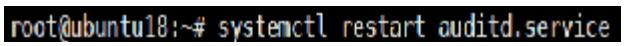
<table>
<tr><td>진단항목</td><td colspan="2">DO-01. 도커 최신 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 최신 업데이트 버전을 유지함으로써 Docker 소프트웨어의 취약점을 완화할 수 있다. 공격자는 권한을 획득하거나 권한 상승을 시도할 때 알려진 취약점을 악용할 수 있으며, Docker 최신 업데이트 버전을 설치하지 않으면 취약한 Docker 소프트웨어가 실행될 수 있다. 그에 따라 권한 상승, 비인가 접근, 또는 기타 보안 침해로 이어질 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">알려진 취약점이 없는 버전을 사용하는 경우</td></tr>
<tr><td>취약</td><td colspan="3">알려진 취약점이 존재하는 버전을 사용하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 버전 확인 방법
1) Docker 버전 확인
$ docker version
 
2) 우분투 또는 데비안의 경우 패키지 버전 확인
$ dpkg –l | grep docker.io
3) CentOS의 경우 패키지 버전 확인
$ rpm –qa | grep docker.io</td></tr>
</table>

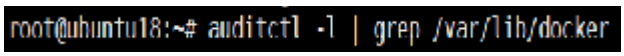
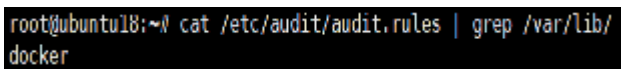
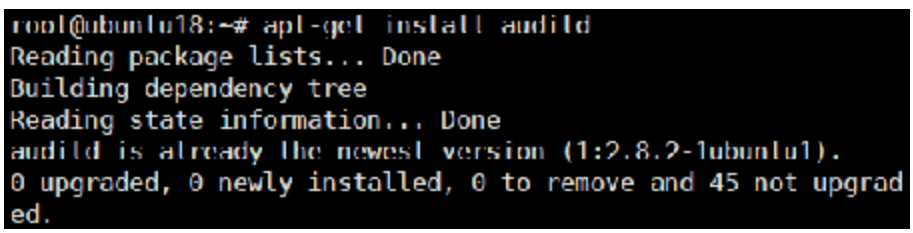
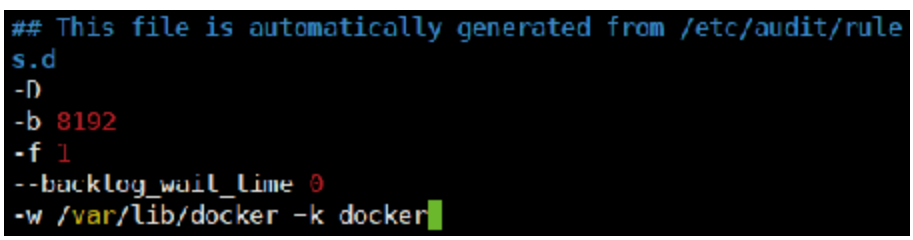
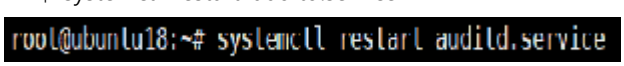
<table>
<tr><td></td><td></td></tr>
<tr><td>조치방법</td><td>
■ 수동 조치
1) Docker 사이트를 통해 주기적으로 버전 점검을 하도록 하며, 최신 버전 적용 시 충분한 테스트 후 적용

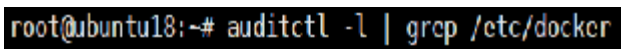
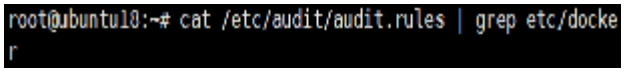
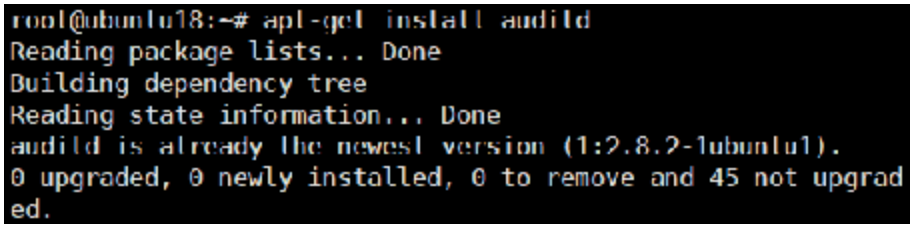
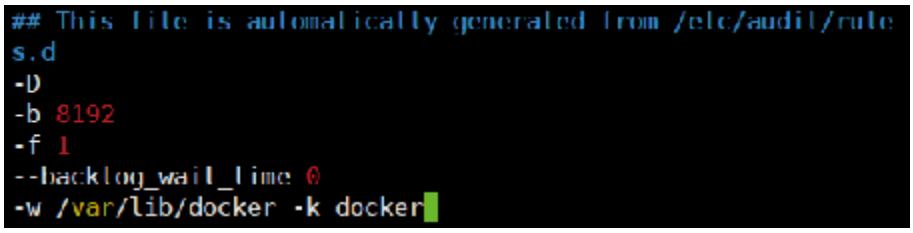
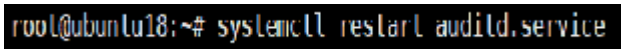
※ Docker와 통신이 필요한 타 어플리케이션의 경우 호환성 문제가 생길 수 있으므로 버전 업데이트에 대한 위험 평가를 수행한 후 업데이트 작업을 실시

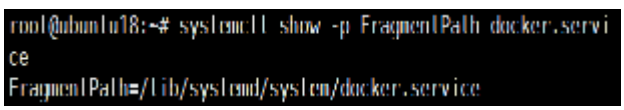
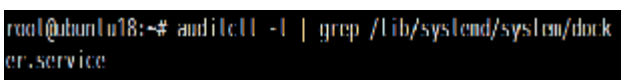
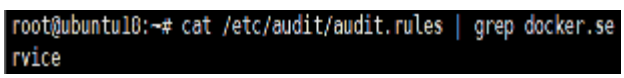
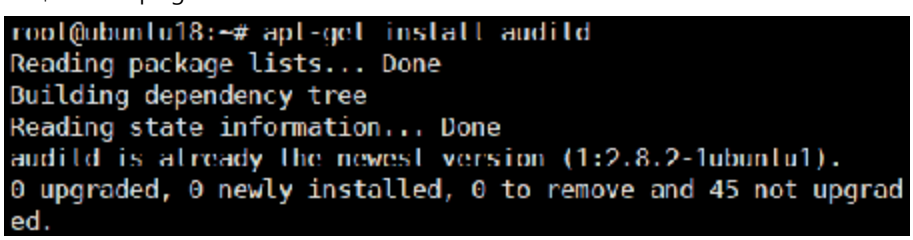
※ Docker Release date(2020.10.29 기준)
<table>
<tr><th>Docker 종류</th><th>최신 버전</th><th>릴리즈 날짜</th></tr>
<tr><td>Docker Engine</td><td>19.03.13</td><td>2020.09.16</td></tr>
<tr><td>Docker Desktop for MAC(Stable)</td><td>2.4.0.0</td><td>2020.09.30</td></tr>
<tr><td>Docker Desktop for MAC(Edge)</td><td>2.4.2.0</td><td>2020.10.19</td></tr>
<tr><td>Docker Desktop for Windows(Stable)</td><td>2.4.0.0</td><td>2020.09.30</td></tr>
<tr><td>Docker Desktop for Windows(Edge)</td><td>2.4.2.0</td><td>2020.10.19</td></tr>
<tr><td>Docker Compose</td><td>1.27.4</td><td>2020.09.24</td></tr>
</table>
</td></tr>
<tr><td>비고</td><td>
※ Docker Release Note 사이트
- https://docs.docker.com/release-notes/ (Docker 공식 홈페이지)
- https://launchpad.net/ubuntu/+source/docker.io (Ubuntu docker.io 패키지 릴리즈 정보)
</td></tr>
</table>

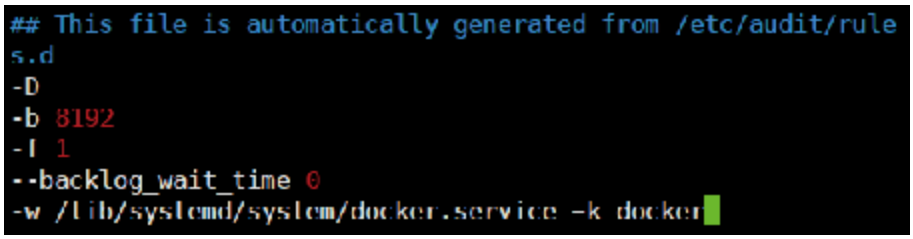
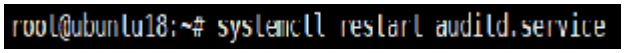
<table>
<tr><td>진단항목</td><td colspan="2">DO-02. 도커 그룹에 불필요한 사용자 제거</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 데몬은 루트 권한을 필요로 하며, Docker 그룹에 추가된 사용자는 루트 권한을 부여받게 된다. Docker는 Docker 호스트와 게스트 컨테이너 간의 접근 권한을 제한하지 않고 root 디렉터리(/)를 공유할 수 있다. 즉, 컨테이너를 실행하고 호스트의 root 디렉터리를 컨테이너에 매핑할 수 있어 컨테이너는 제한 없이 호스트 파일 시스템을 변경할 수 있는 위험이 존재한다. 도커 그룹에 속한 사용자는 상승된 권한을 얻을 수 있고 호스트의 root 디렉터리가 매핑된 컨테이너를 실행할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">도커 그룹에 불필요한 사용자가 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">도커 그룹에 불필요한 사용자가 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 도커 그룹에 속한 사용자 계정 조회
$ cat /etc/group | grep docker
 
▪ 도커 그룹 이름이 dockerroot일 경우 root 및 dockerroot 그룹에 속한 사용자 계정 동시 조회
$ cat /etc/group | grep root
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Docker 그룹에서 신뢰되지 않은 사용자 또는 불필요한 사용자 계정은 삭제
ex) $ vi /etc/group에서 삭제
▪ Docker 그룹 이름이 dockerroot일 경우 root 및 dockerroot 그룹에서 신뢰되지 않은 사용자 또는 불필요한 사용자 계정은 삭제
ex) $ vi /etc/group에서 삭제</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

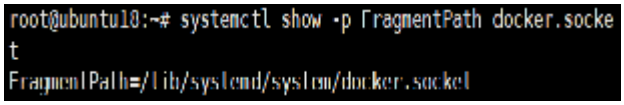
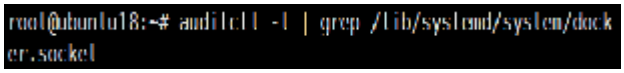
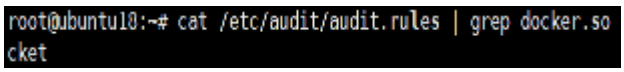
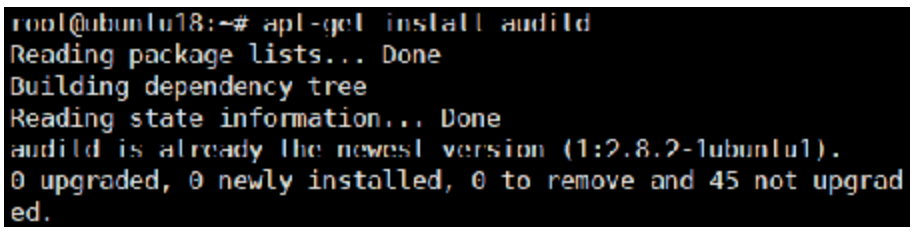
<table>
<tr><td>진단항목</td><td colspan="2">DO-03. Docker daemon audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 데몬은 root 권한으로 실행되기 때문에 그 활동과 용도를 감사하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/usr/bin/docker 파일의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/usr/bin/docker 파일의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령어를 통해 /usr/bin/docker 감사 설정 확인
$ auditctl –l | grep /usr/bin/docker
 
▪ 명령어를 통해 /etc/audit/audit.rules 파일의 내용 확인
$ cat /etc/audit/audit.rules | grep /usr/bin/docker
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 다음과 같은 절차로 설정 적용
1) auditd 설치
$ sudo apt-get install auditd
 
2) /etc/audit/audit.rules 파일에 다음 내용 추가
-w /usr/bin/docker –k docker
 
3) audit 데몬을 재시작
$ systemctl restart auditd.service
  </td></tr>
<tr><td>비고</td><td colspan="4">※ auditd가 설치되어 있어야 함
$ sudo apt-get install auditd</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-04. /var/lib/docker audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/var/lib/docker 디렉터리는 컨테이너에 대한 모든 정보를 보유하고 있는 디렉터리이므로 감사 설정을 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/var/lib/docker 디렉터리의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/var/lib/docker 디렉터리의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령어를 통해 /var/lib/docker 감사 설정 확인
$ auditctl –l | grep /var/lib/docker
 
▪ 명령어를 통해 /etc/audit/audit.rules 파일의 내용을 확인
$ cat /etc/audit/audit.rules | grep /var/lib/docker
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 다음과 같은 절차로 audit 설정 적용
1) auditd 설치
$ sudo apt-get install auditd
 
2) /etc/audit/audit.rules 파일에 다음 내용 추가
-w /var/lib/docker –k docker
 
3) audit 데몬을 재시작
$ systemctl restart auditd.service
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-05. /etc/docker audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/docker 디렉터리는 Docker 데몬과 Docker 클라이언트 간의 TLS 통신에 사용되는 다양한 인증서와 키를 보유하고 있으므로 감사 설정을 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/docker 디렉터리의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/docker 디렉터리의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령어를 통해 /etc/docker 감사 설정 확인
$ auditctl –l | grep /etc/docker
 
▪ 명령어를 통해 /etc/audit/audit.rules 파일의 내용을 확인
$ cat /etc/audit/audit.rules | grep etc/docker
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 다음과 같은 절차로 audit 설정 적용
1) auditd 설치
$ sudo apt-get install auditd
 
2) /etc/audit/audit.rules 파일에 다음 내용 추가
-w /var/lib/docker –k docker
 
3) audit 데몬을 재시작
$ systemctl restart auditd.service
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-06. docker.service audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">데몬 매개변수가 관리자에 의해 변경된 경우 docker.service 파일이 존재한다. docker.service 파일은 Docker 데몬을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.service 파일의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.service 파일의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 다음과 같은 절차로 docker.service 파일의 감사 설정 확인
1) docker.service 파일의 경로 확인
$ systemctl show –p FragmentPath docker.service
 
2) docker.service 파일의 감사 설정 확인
$ auditctl –l | grep /lib/systemd/system/docker.service
 
▪ /etc/audit/audit.rule 파일 내용 확인
$ cat /etc/audit/audit.rules | grep docker.service
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 다음과 같은 절차로 audit 설정 적용
1) auditd 설치
$ sudo apt-get install auditd
 
2) /etc/audit/audit.rules 파일에 다음 내용 추가
-w /lib/systemd/system/docker.service –k docker</td></tr>
</table>

	 3) audit 데몬을 재시작 $ systemctl restart auditd.service 
비고	※ 이 파일은 시스템에 존재하지 않을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음

<table>
<tr><td>진단항목</td><td colspan="2">DO-07. docker.socket audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">docker.socket 파일은 Docker 데몬 소켓을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.socket 파일의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.socket 파일의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 다음과 같은 절차로 docker.service 파일의 감사 설정 확인
1) docker.socket 파일의 경로 확인
$ systemctl show –p FragmentPath docker.socket
 
2) docker.socket 파일의 감사 설정 확인
$ auditctl –l | grep /lib/systemd/system/docker.socket
 
■ /etc/audit/audit.rule 파일 내용 확인
$ cat /etc/audit/audit.rules | grep docker.socket
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ 다음과 같은 절차로 audit 설정 적용
1) auditd 설치
$ sudo apt-get install auditd
 
2) /etc/audit/audit.rules 파일에 다음 내용 추가
-w /lib/systemd/system/docker.socket –k docker</td></tr>
</table>

<table>
<tr><td></td><td>

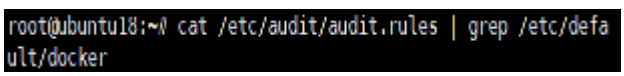
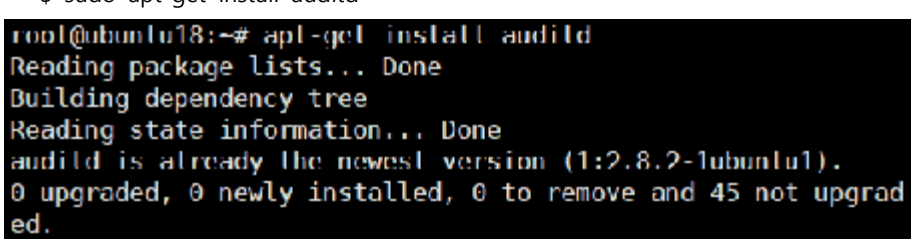
```
## This file is automatically generated from /etc/audit/rule
s.d
-D
-b 8192
-f 1
--backlog_wait_time 0
-w /lib/systemd/system/docker.socket -k docker
```

3) audit 데몬을 재시작

$ systemctl restart auditd.service

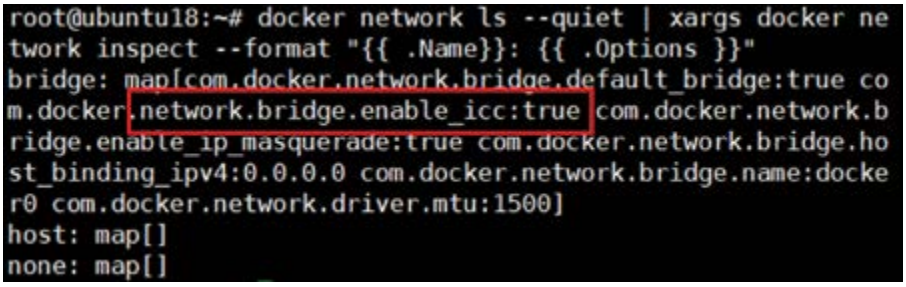
```
root@ubuntu18:~# systemctl restart auditd.service
```

</td></tr>
<tr><td>비고</td><td>※ 이 파일은 시스템에 존재하지 않을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음</td></tr>
</table>

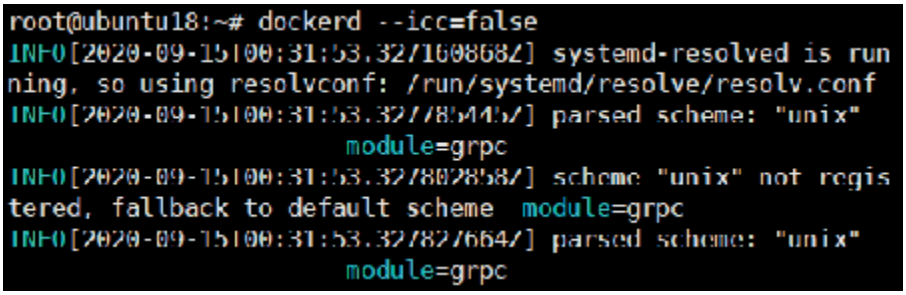
<table>
<tr><td>진단항목</td><td colspan="2">DO-08. /etc/default/docker audit 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/default/docker 파일은 Docker 데몬을 위한 다양한 파라미터를 보유하고 있으므로 감사 설정을 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/default/docker 파일의 감사 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/default/docker 파일의 감사 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ Debian 계열
1) /etc/default/docker 감사 설정 확인
$ auditctl –l | grep /etc/default/docker
 
2) /etc/audit/audit.rules 파일 내용 확인
$ cat /etc/audit/audit.rules | grep /etc/default/docker
 
■ RedHat 계열
1) /etc/sysconfig/docker 감사 설정 확인
$ auditctl –l | grep /etc/sysconfig/docker
2) /etc/audit/audit.rules 파일 내용 확인
$ cat /etc/audit/audit.rules | grep /etc/sysconfig/docker</td></tr>
<tr><td>조치방법</td><td colspan="4">■ auditd 설치
$ sudo apt-get install auditd
 
■ /etc/audit/audit.rules 파일에 다음 내용 추가
-w /etc/default/docker –k docker</td></tr>
</table>

	`` ## This file is automatically generated from /etc/audit/rules.d -D -b 8192 -f 1 --backlog_wait_time 0 -w /etc/default/docker -k docker ``` ▪ audit 데몬 재시작 $ systemctl restart auditd.service ``` root@ubuntu18:~# systemctl restart auditd.service ```
비고	

나. 도커 데몬 설정

<table>
<tr><td>진단항목</td><td colspan="2">DO-09. default bridge를 통한 컨테이너 간 네트워크 트래픽 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Default Network Bridge의 동일한 호스트에서 컨테이너 간의 네트워크 통신은 제한되지 않는다. 따라서 각 컨테이너는 호스트의 네트워크를 통해 다른 컨테이너 네트워크 패킷을 모두 볼 수 있다. 이로 인해 의도하지 않거나 원하지 않는 정보가 다른 컨테이너에 공개될 수 있으므로 Default Network Bridge에서 컨테이너 간 통신을 제한하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">컨테이너 간 네트워크 통신이 가능하지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">컨테이너 간 네트워크 통신이 가능한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 명령을 통해 컨테이너 간 제한 옵션이 적용되어 있는지 확인
$ docker network ls --quiet | xargs docker network inspect --format "{{ .Name}}: {{ .Options }}"
 

※ com.docker.network.bridge.enable_icc: true 값이 반환되면 제한되어 있지 않음

▪ 다음과 같은 옵션으로 데몬 재시작
$ dockerd --icc=false
 

▪ /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작
DOCKER_OPTS="--icc=false"</td></tr>
</table>

<table>
<tr><td></td><td rowspan="2"><pre>#export DOCKER_TMPDIR="/mnt/bigdrive/docker-tmp"

DOCKER_OPTS="--icc=false"</pre>
■ /etc/docker/daemon.json 파일에 아래와 같이 작성 후 데몬 재시작
{ "icc": false }
<pre>{
        "icc": false
}</pre></td></tr>
<tr><td>조치방법</td></tr>
<tr><td>비고</td><td>※ /etc/default/docker를 사용할 경우 Ubuntu docker.io 패키지를 제외한 docker를 사용 시 systemd를 사용하는 OS에서는 바로 적용되지 않으며 docker.service를 수정하여 사용해야 함
■ systemctl show –p FragmentPath docker.service 명령어를 통해 docker.service 경로 확인
FragmentPath=/lib/systemd/system/docker.service
<pre>root@ubuntu18:~# systemctl show -p FragmentPath docker.servi
ce
FragmentPath=/lib/systemd/system/docker.service</pre>
■ vi 편집기를 통해 docker.service를 연 후
■ 아래와 같이 수정 또는 추가
[Service]
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd –H fd:// $DOCKER_OPTS
<pre>[Service]
Type=notify
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd H fd:// $DOCKER OPTS</pre>
※ /etc/docker/daemon.json를 사용하는 경우 ps 명령어를 통한 옵션 확인을 할 수 없으며 docker 명령어를 통해 옵션 적용 여부를 확인할 수 있음</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-10. 도커 클라이언트 인증 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker는 기본적으로 인증 절차를 거치지 않기 때문에, 비인가 된 사용자가 Docker 데몬에 접근하여 명령을 실행할 수 있다. 그러므로 인증 플러그인을 설치하여 Docker 클라이언트 명령을 실행할 때 인증 절차를 거치도록 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Docker 인증 플러그인이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Docker 인증 플러그인이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">

아래와 같은 명령어를 통해 인증 플러그인 옵션이 적용되어 있는지 확인
$ ps –ef | grep docker

<pre>root@ubuntu18:~# ps -ef | grep docker
root   1118   1 0 05:38 ?   00:00:13 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
root   28881 1118 0 08:18 ?   00:00:00 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 1234 -container-ip 172.17.0.2 -container-port 6739
root   28889 1099 0 08:18 ?   00:00:00 containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1.linux/moby/07ee32159539dc8b41ab08a57ac9805016c304ddbea096f603cb45ecacd315d8 -address /run/containerd/containerd.sock -containerd-binary /usr/bin/containerd -runtime-root /var/run/docker/runtime-runc
root   29154 1118 0 08:21 ?   00:00:00 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 3306 -container-ip 172.17.0.3 -container-port 3306
root   29161 1099 0 08:21 ?   00:00:00 containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1.linux/moby/c192484c48053c05896902b741b0a88cdde9530fea20e90fb535c7aeac7f2b94 -address /run/containerd/containerd.sock -containerd-binary /usr/bin/containerd -runtime-root /var/run/docker/runtime-runc
root   29590 27011 0 08:28 pts/1   00:00:00 grep --color=auto docker</pre>

아래 명령어를 수행하는데 인증이 필요한지 확인
$ docker search hello-world

</td></tr>
</table>

<table>
<tr><td></td><td>

```
root@ubuntu18:~# docker search hello-world
NAME                                      DESCRIPTION
                                STARS               OFFICIAL
          AUTOMATED
hello-world                               Hello World! (an
example of minimal Dockeriz…   1290                [OK]

kitematic/hello-world-nginx               A light-weight ng
inx container that demonstr…   147

tutum/hello-world                         Image to test doc
ker deployments. Has Apache…   73
          [OK]
dockercloud/hello-world                   Hello World!
```

</td></tr>
<tr><td>조치방법</td><td>

▪ 다음과 같은 절차로 인증 설정
1) 인증 플러그인 설치
2) 인증 정책 설정
3) 아래와 같은 옵션으로 데몬 시작
(방법1) docker daemon --authorization-plugin=<PLUGIN_ID>
(방법2) /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작
DOCKER_OPTS=" --authorization-plugin-<PLUGIN_ID>"
(방법3) /etc/docker/daemon.json 파일에 아래와 같은 옵션 추가 후 데몬 재시작
{ "authorization-plugins": ["PLUGIN_ID"]}

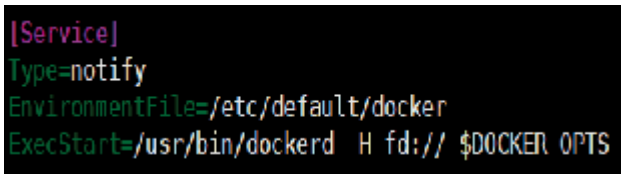
</td></tr>
<tr><td>비고</td><td>

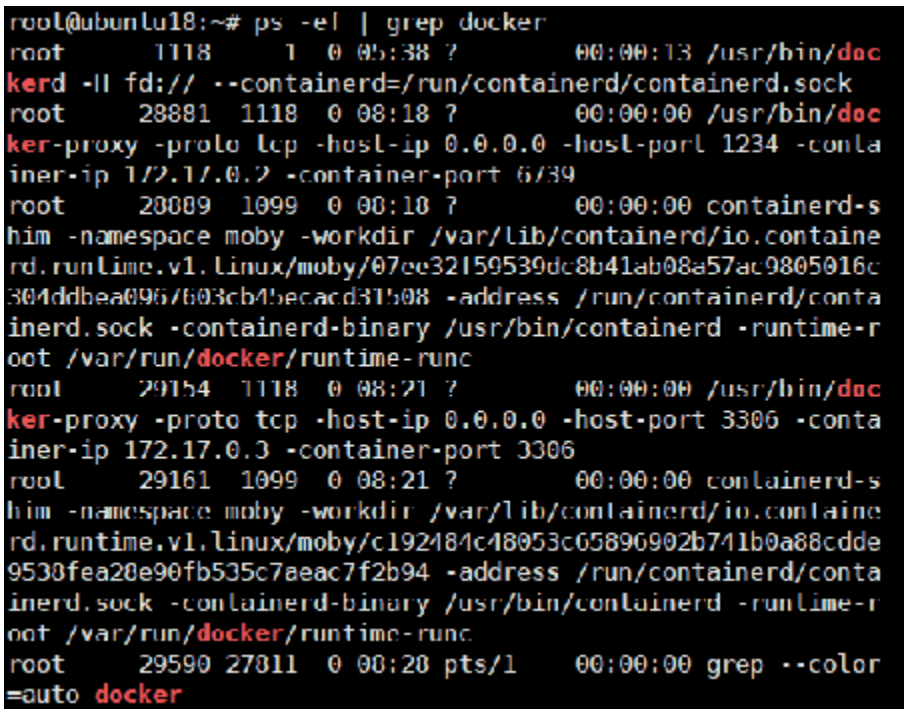
※ /etc/default/docker를 사용할 경우 Ubuntu docker.io 패키지를 제외한 docker를 사용 시 systemd를 사용하는 OS에서는 바로 적용되지 않으며 docker.service를 수정하여 사용해야 함
▪ systemctl show –p FragmentPath docker.service 명령어를 통해 docker.service 경로 확인
FragmentPath=/lib/systemd/system/docker.service

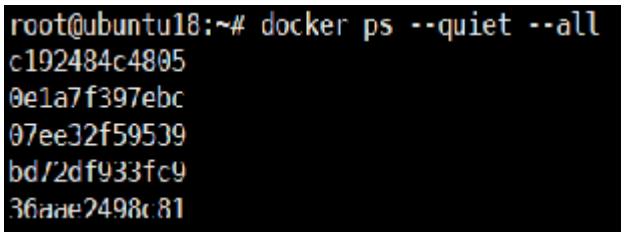
```
root@ubuntu18:~# systemctl show -p FragmentPath docker.servi
ce
FragmentPath=/lib/systemd/system/docker.service
```

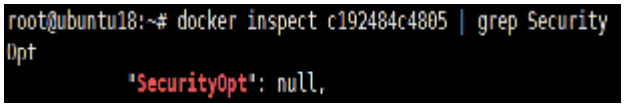
▪ vi 편집기를 통해 docker.service를 연 후
▪ 아래와 같이 수정 또는 추가
[Service]
EnvironmentFile=/etc/default/docker
ExecStart=/usr/bin/dockerd –H fd:// $DOCKER_OPTS

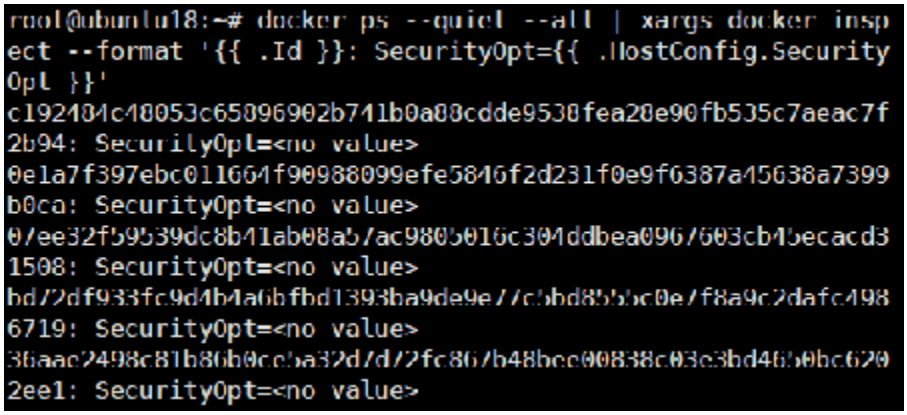
</td></tr>
</table>

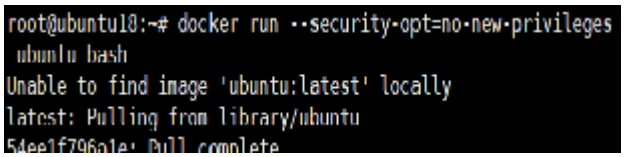
	 ※ /etc/docker/daemon.json를 사용하는 경우 ps 명령어를 통한 옵션 확인을 할 수 없으며 docker 명령어를 통해 옵션 적용 여부를 확인할 수 있음

<table>
<tr><td>진단항목</td><td colspan="2">DO-11. legacy registry (v1) 비활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 레지스트리 v2는 이미지 출처 및 이미지 서명 및 확인과 같은 보안 기능을 지원하는 등 레거시 레지스트리 v1보다 더 많은 성능 및 보안 향상 기능을 제공한다. 따라서 Docker 레거시 레지스트리는 사용이 제한되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">legacy registry v1이 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">legacy registry v1이 비활성화 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래와 같은 명령어를 통해 --disable-legacy-registry 옵션이 적용되어 있는지 확인
$ ps –ef | grep docker
 
▪ /etc/default/docker 파일에서 --disable-legacy-registry 옵션이 적용되어 있는지 확인
$ cat /etc/default/docker | grep --disable-legacy-registry</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 아래와 같은 옵션으로 데몬 시작
$ docker daemon --disable-legacy-registry
▪ /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작
DOCKER_OPTS="--disable-legacy-registry"</td></tr>
<tr><td>비고</td><td colspan="4">※ Docker v17.12(CE) 이상부터는 --disable-legacy-registry 옵션을 사용할 수 없으므로 legacy registry v1을 사용할 수 없음</td></tr>
</table>

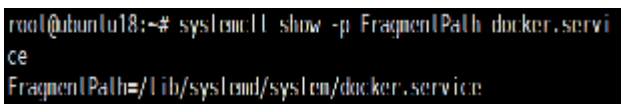
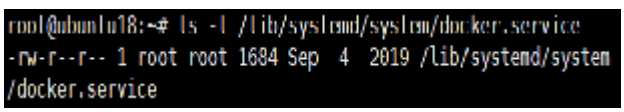
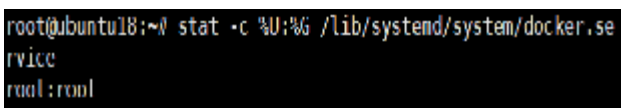
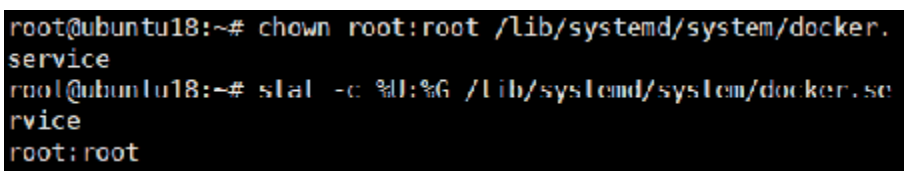
<table>
<tr><td>진단항목</td><td colspan="2">DO-12. 추가 권한 획득으로부터 컨테이너 제한</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">컨테이너가 suid 또는 sgid를 통해 추가 권한을 얻는 것을 제한하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">컨테이너 추가 권한 획득 제한 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">컨테이너 추가 권한 획득 제한 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래와 같은 명령어를 통해 컨테이너 추가 권한 획득 제한 설정이 적용되어 있는지 확인
1) 컨테이너 목록 확인
$ docker ps --quiet --all
 

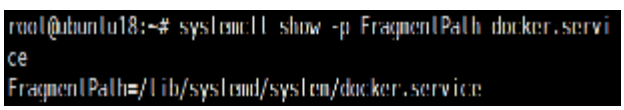
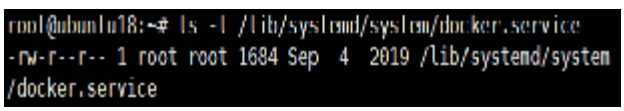
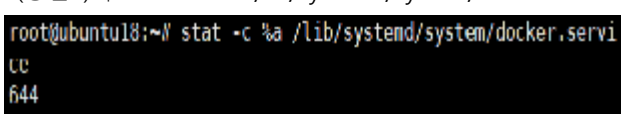
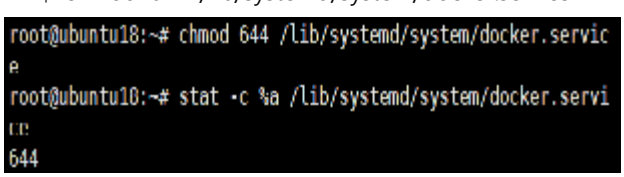
2) SecurityOpt 옵션 설정 확인
$ docker inspect <CONTAINER ID> | grep SecurityOpt
 

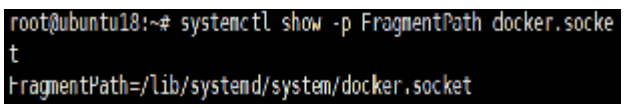
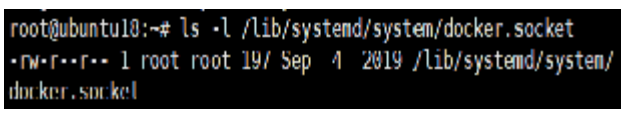
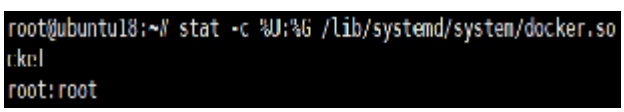
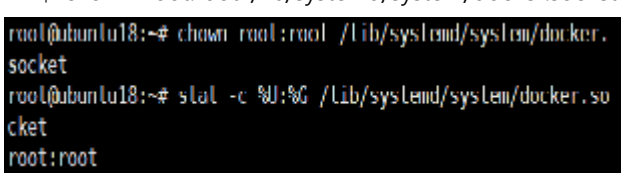
▪ 아래와 같은 명령어를 통해 컨테이너 추가 권한 획득 제한 설정이 적용되어 있는지 확인
$ docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: SecurityOpt={{ .HostConfig.SecurityOpt }}'
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 아래와 같은 옵션으로 컨테이너 실행</td></tr>
</table>

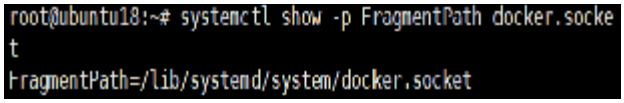
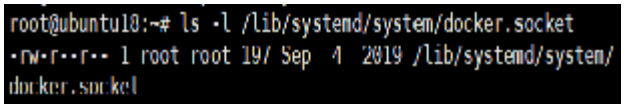
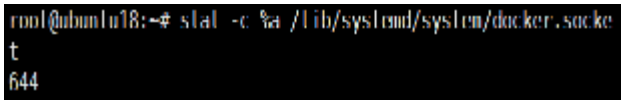
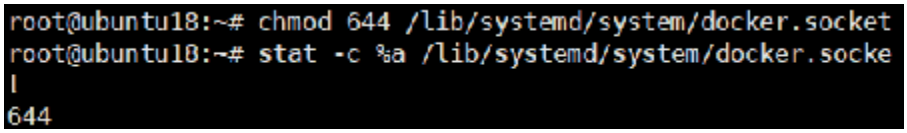
	$ docker run —security-opt=no-new-privileges ex) $ docker run —security-opt=no-new-privileges ubuntu bash 
비고	※ docker 1.11에 추가된 옵션

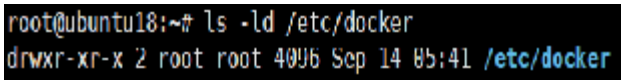
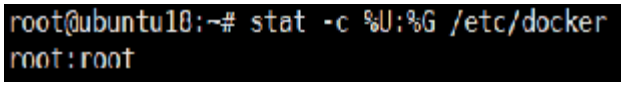
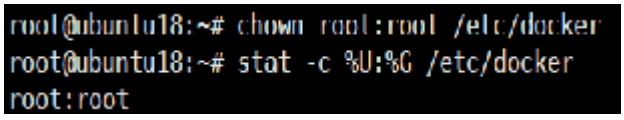
다. 도커 데몬 설정 파일

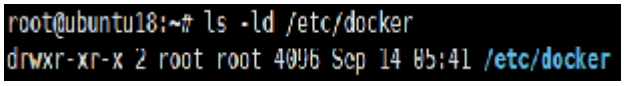
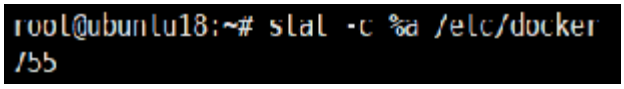
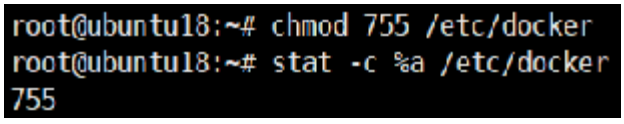
<table>
<tr><td>진단항목</td><td colspan="2">DO-13. docker.service 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">docker.service 파일에는 Docker 데몬의 동작을 변경할 수 있는 중요한 매개변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 파일의 소유자 및 소유그룹이 root:root이어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.service 파일의 소유자 및 소유그룹이 root:root인 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.service 파일의 소유자 및 소유그룹이 root:root가 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ docker.service 파일의 경로 확인
$ systemctl show -p FragmentPath docker.service
 
▪ docker.service 파일의 소유권 확인
(방법1) $ ls –l /lib/systemd/system/docker.service
 
(방법2) $ stat -c %U:%G /lib/systemd/system/docker.service
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ docker.service 파일의 소유자 및 소유그룹을 root:root로 설정
$ chown root:root /lib/systemd/system/docker.service
  </td></tr>
<tr><td>비고</td><td colspan="4">※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음</td></tr>
</table>

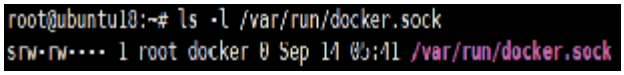
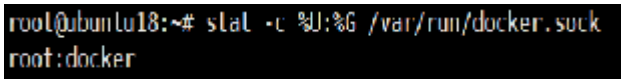
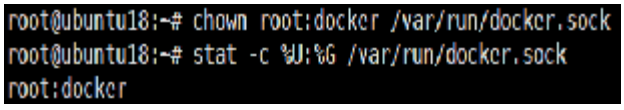
<table>
<tr><td>진단항목</td><td colspan="2">DO-14. docker.service 파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">docker.service 파일에는 Docker 데몬의 동작을 변경할 수 있는 중요한 매개변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 root 이외의 사용자는 쓰기 권한을 제거하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.service 파일의 접근권한이 644 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.service 파일의 접근권한이 644 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ docker.service 파일의 경로 확인
$ systemctl show –p FragmentPath docker.service
 
▪ docker.service 파일의 접근권한 확인
(방법1) $ ls –l /lib/systemd/system/docker.service
 
(방법2) $ stat –c %a /lib/systemd/system/docker.service
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ docker.service 파일의 접근권한을 644로 설정
$ chmod 644 /lib/systemd/system/docker.service
  </td></tr>
<tr><td>비고</td><td colspan="4">※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음</td></tr>
</table>

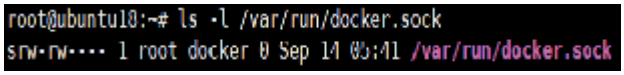
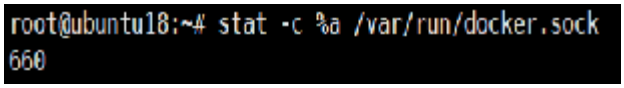
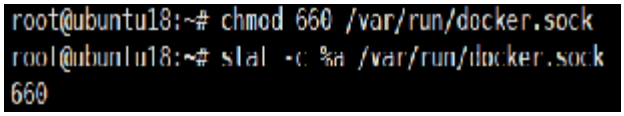
<table>
<tr><td>진단항목</td><td colspan="2">DO-15. docker.socket 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">docker.socket 파일에는 Docker API의 동작을 변경할 수 있는 중요한 매개변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 docker.socket 파일의 소유자 및 소유 그룹이 root:root 이어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.socket 파일의 소유자 및 소유그룹이 root:root인 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.socket 파일의 소유자 및 소유그룹이 root:root가 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ docker.socket 파일의 경로 확인
$ systemctl show -p FragmentPath docker.socket
 
▪ docker.socket 파일의 소유권 확인
(방법1) $ ls –l /lib/systemd/system/docker.socket
 
(방법2) $ stat -c %U:%G /lib/systemd/system/docker.socket
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ docker.service 파일의 소유자 및 소유그룹을 root:root로 설정
$ chown root:root /lib/systemd/system/docker.socket
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-16. docker.socket 파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">docker.socket 파일에는 Docker API의 동작을 변경할 수 있는 중요한 매개변수가 포함되어 있다. 따라서 무결성을 유지하기 위해서는 root 이외의 사용자는 쓰기 권한을 제거하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">docker.socket 파일의 접근권한이 644 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">docker.socket 파일의 접근권한이 644 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ docker.socket 파일의 경로 확인
$ systemctl show –p FragmentPath docker.socket
 
■ docker.socket 파일의 접근권한 확인
(방법1) $ ls –l /lib/systemd/systemd/docker.socket
 
(방법2) $ stat –c %a /lib/systemd/system/docker.socket
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ docker.socket 파일의 접근권한을 644로 설정
$ chmod 644 /lib/systemd/system/docker.socket
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-17. /etc/docker 디렉터리 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/docker 디렉터리에는 민감한 파일들 외에도 인증서 및 민감 데이터가 들어 있으므로 디렉터리의 무결성을 유지하기 위해서는 소유자 및 소유그룹이 root:root 이어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/docker 디렉터리의 소유자 및 소유그룹이 root:root인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/docker 디렉터리의 소유자 및 소유그룹이 root:root가 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/docker 디렉터리의 소유권 확인
(방법 1) $ ls –ld /etc/docker
 
(방법 2) $ stat -c %U%G /etc/docker
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/docker 디렉터리의 소유자:소유그룹을 root:root로 설정
$ chown root:root /etc/docker
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

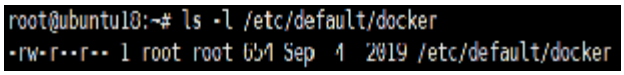
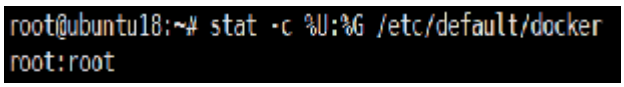
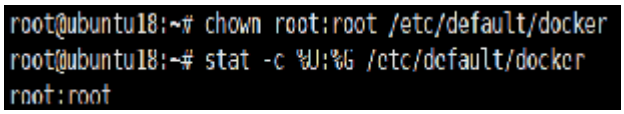
<table>
<tr><td>진단항목</td><td colspan="2">DO-18. /etc/docker 디렉터리 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/docker 디렉터리에는 민감한 파일들 외에도 인증서 및 민감 데이터가 들어 있으므로 디렉터리의 무결성을 유지하기 위해서는 root 이외의 사용자는 쓰기권한이 제거되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/docker 디렉터리의 접근권한이 755 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/docker 디렉터리의 접근권한이 755 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/docker 디렉터리의 접근권한 확인
(방법1) $ ls –ld /etc/docker
 
(방법2) $ stat –c %a /etc/docker
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/docker 디렉터리의 접근권한을 755로 설정
$ chmod 755 /etc/docker
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

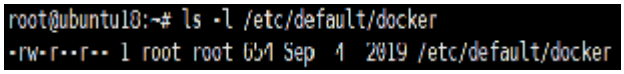
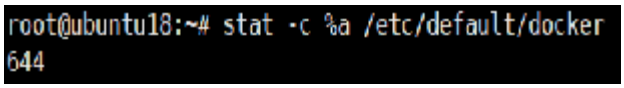
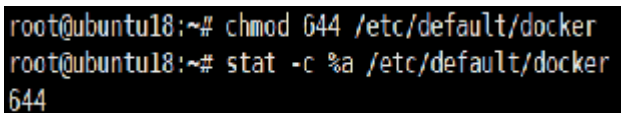
<table>
<tr><td>진단항목</td><td colspan="2">DO-19. /var/run/docker.sock 파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 데몬은 root로 구동된다. 그러므로 해당 소켓은 root가 소유하고 있어야 하며 root 및 Docker 그룹의 구성원만이 Docker Unix 소켓을 읽고 쓸 수 있어야 한다. 다른 사용자나 프로세스가 이 소켓을 소유하고 있는 경우 권한 없는 사용자나 프로세스가 Docker 데몬과 상호작용할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/var/run/docker.sock 파일의 소유자 및 소유그룹이 root:docker(root)인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/var/run/docker.sock 파일의 소유자 및 소유그룹이 root:docker(root)가 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /var/run/docker.sock 파일의 소유권 확인
(방법1) $ ls –l /var/run/docker.sock
 
(방법2) $ stat –c %U%G /var/run/docker.sock
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /var/run/docker.sock 파일의 소유자:소유그룹을 root:docker로 설정
$ chown root:docker /var/run/docker.sock
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-20. /var/run/docker.sock 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker 데몬은 root로 구동된다. 그러므로 root 및 Docker 그룹의 구성원만이 Docker Unix 소켓을 읽고 쓸 수 있어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/var/run/docker.sock 파일의 접근권한이 660 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/var/run/docker.sock 파일의 접근권한이 660 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /var/run/docker.sock 파일의 접근권한 확인
(방법1) $ ls –l /var/run/docker.sock
 
(방법2) $ stat –c %a /var/run/docker.sock
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ docker.sock 파일의 접근권한을 660으로 설정
$ chmod 660 /var/run/docker.sock
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

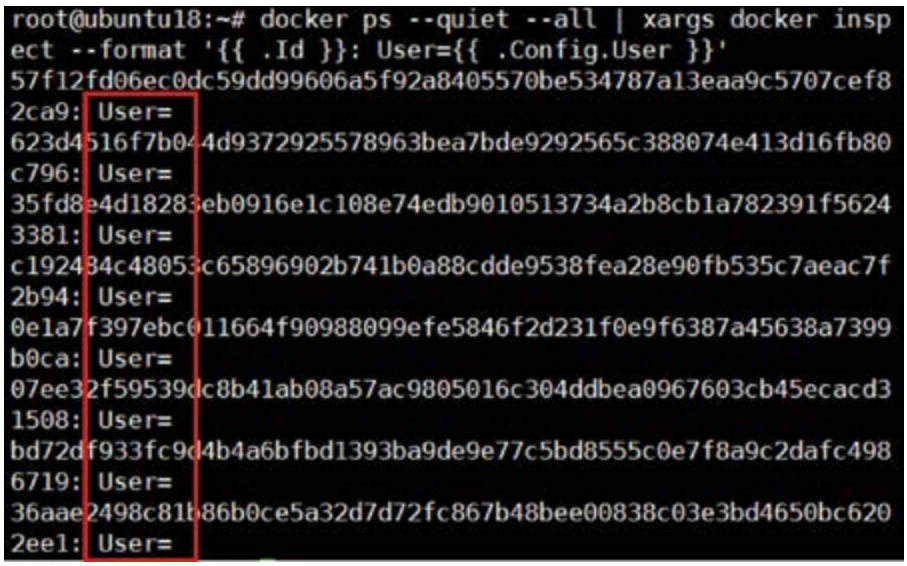
진단항목	DO-21. daemon.json 파일 소유권 설정	취약도	중
항목설명	daemon.json 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 소유자 및 소유그룹은 root가 되어야 한다.		
진단기준	양호	/etc/docker/daemon.json 파일의 소유자 및 소유그룹이 root인 경우	
	취약	/etc/docker/daemon.json 파일의 소유자 및 소유그룹이 root가 아닌 경우	
진단방법	▪ /etc/docker/daemon.json 파일의 소유권 확인 (방법1) ls -l /etc/docker/daemon.json (방법2) stat -c %U%G /etc/docker/daemon.json		
조치방법	▪ daemon.json 파일의 소유자:소유그룹을 root:root로 설정 $ chown root:root /etc/docker/daemon.json		
비고	※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음		

진단항목	DO-22. daemon.json 파일 접근권한 설정	취약도	중
항목설명	daemon.json 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 root 이외의 사용자는 쓰기권한이 제거되어야 한다.		
진단기준	양호	/etc/docker/daemon.json 파일의 접근권한이 644 이하인 경우	
	취약	/etc/docker/daemon.json 파일의 접근권한이 644 초과인 경우	
진단방법	▪ /etc/docker/daemon.json 파일의 접근권한 확인 (방법1) $ ls –l /etc/docker/daemon.json (방법2) $ stat –c %a /etc/docker/daemon.json		
조치방법	▪ daemon.json 파일의 접근권한을 644로 설정 $ chmod 644 /etc/docker/daemon.json		
비고	※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음		

<table>
<tr><td>진단항목</td><td colspan="2">DO-23. /etc/default/docker 파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/default/docker 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 소유자 및 소유그룹은 root가 되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/default/docker 파일의 소유자 및 소유그룹이 root:root인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/default/docker 파일의 소유자 및 소유그룹이 root:root 가 아닌 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Debian 계열
1) /etc/default/docker 파일의 소유권 확인
(방법1) $ ls –l /etc/default/docker
 
(방법2) $ stat –c %U:%G /etc/default/docker
 
▪ RedHat 계열
1)/etc/sysconfig/docker 파일의 소유권 확인
(방법1) $ ls -l /etc/sysconfig/docker
(방법2) $ stat –c %U:%G /etc/sysconfig/docker</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Debian 계열
1) /etc/default/docker 파일의 소유자:소유그룹을 root:root로 설정
$ chown root:root /etc/default/docker
 
▪ RedHat 계열
1) /etc/sysconfig/docker 파일의 소유자:소유그룹을 root:root로 설정
$ chown root:root /etc/sysconfig/docker</td></tr>
<tr><td>비고</td><td colspan="4">※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음</td></tr>
</table>

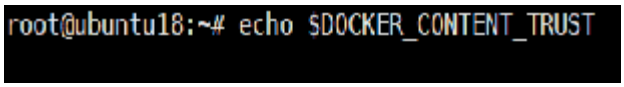
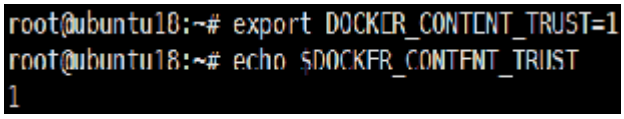
<table>
<tr><td>진단항목</td><td colspan="2">DO-24. /etc/default/docker 파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">/etc/default/docker 파일에는 Docker 데몬의 동작과 관련된 중요한 매개 변수가 포함되어 있다. 따라서 파일의 무결성을 유지하기 위해서 root 이외의 사용자는 쓰기권한이 제거되어야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/default/docker 파일의 접근권한이 644 이하인 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/default/docker 파일의 접근권한이 644 초과인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Debian 계열
1) /etc/default/docker 파일의 접근권한 확인
(방법1) $ ls –l /etc/default/docker
 
(방법2) $ stat –c %a /etc/default/docker
 
▪ RedHat 계열
1) /etc/sysconfig/docker 파일의 접근권한 확인
(방법1) $ ls –l /etc/sysconfig/docker
(방법2) $ stat –c %a /etc/sysconfig/docker</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Debian 계열
1) /etc/default/docker 파일의 접근권한을 644로 설정
$ chmod 644 /etc/default/docker
 
▪ RedHat 계열
1) /etc/sysconfig/docker 파일의 접근권한을 644로 설정
$ chmod 644 /etc/sysconfig/docker</td></tr>
<tr><td>비고</td><td colspan="4">※ 이 파일은 시스템에 없을 수 있다. 그런 경우에는 권장 사항이 적용되지 않음</td></tr>
</table>

라. 컨테이너 이미지 및 빌드 파일

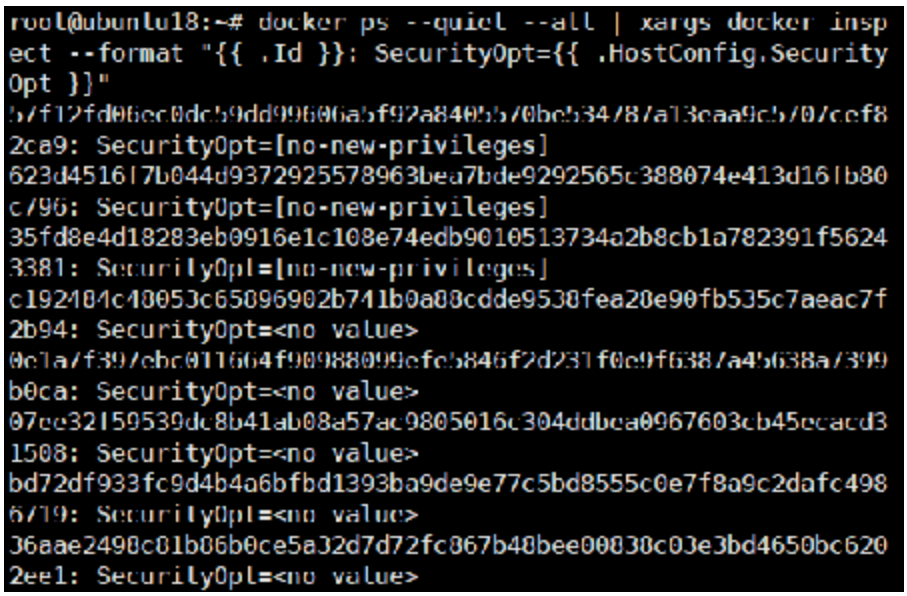
<table>
<tr><td>진단항목</td><td colspan="2">DO-25. root가 아닌 user로 컨테이너 실행</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">기본적으로 컨테이너의 user namespace는 호스트의 namespace와 동일하다. 즉, 컨테이너 내부의 root 사용자는 호스트 시스템의 root 사용자이며 root로 실행되는 컨테이너 프로세스의 손상은 Docker 호스트를 손상시킬 가능성이 있다. 일반적으로 컨테이너에는 root 권한이 필요하지 않으므로 컨테이너에 있는 애플리케이션은 root 권한으로 실행하지 않아야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">컨테이너가 root 계정으로 실행되지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">컨테이너가 root 계정으로 실행되고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 컨테이너가 root 계정으로 실행되고 있는지 확인
$ docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}: User={{ .Config.User }}'
 

※ 위 명령어 실행시 username 또는 user ID를 반환한다. 빈칸으로 나오는 경우는 root 계정으로 컨테이너가 실행되어 있다는 것을 의미한다.</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Dockerfile에 다음과 같은 내용을 추가
예시) RUN useradd -d /home/username -m -s /bin/bash username
USER username</td></tr>
</table>

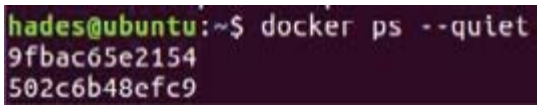
	`` # Dockcr Upstart and SysVinit configuration filc RUN useradd -d /home/username -m -s /bin/bash username USER username # ```
비고	

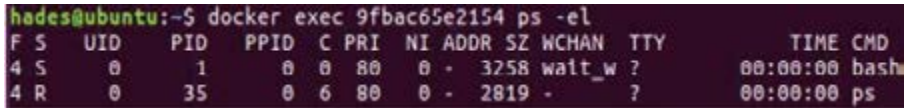
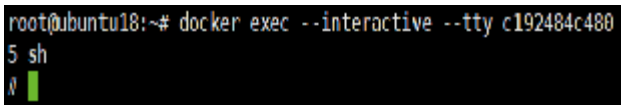
<table>
<tr><td>진단항목</td><td colspan="2">DO-26. 도커를 위한 컨텐츠 신뢰성 활성화</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Content Trust 설정은 원격 Docker 레지스트리와 주고받는 데이터에 디지털 서명을 허용할 수 있는 기능을 제공한다. 이미지 서명은 데이터 전송 도중에 발생할 수 있는 컨테이너 조작을 방지할 수 있기 때문에 컨텐츠 신뢰성 설정을 적용 하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Docker 컨텐츠 신뢰성 설정이 활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Docker 컨텐츠 신뢰성 설정이 비활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래와 같은 명령어를 입력했을 경우 "1"을 반환하는지 확인
$ echo $DOCKER_CONTENT_TRUST
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 사용하는 shell(예. bash shell)에 아래와 같은 내용을 추가
$ export DOCKER_CONTENT_TRUST=1
  </td></tr>
<tr><td>비고</td><td colspan="4">※ 기본 설정 값 : disabled
※ bash shell 전체 적용 시 /etc/bash.bashrc(Ubuntu 계열) 또는 /etc/bashrc(CentOS 계열)에 작성 후 적용
※ Docker Engine 1.8부터 추가된 기능</td></tr>
</table>

마. 컨테이너 런타임

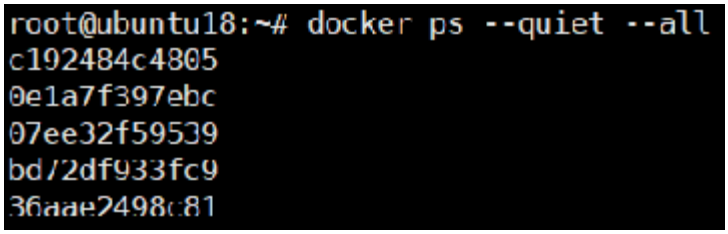
<table>
<tr><td>진단항목</td><td colspan="2">DO-27. 컨테이너 SELinux 보안 옵션 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">SELinux는 효과적인 Linux 애플리케이션 보안 시스템으로 MAC(Mandatory Access Control) 시스템을 제공한다. 때문에 네트워크의 보안 수준을 향상시키기 위해서는 SELinux를 사용하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SELinux 보안옵션이 활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SELinux 보안옵션이 비활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 프로세스 확인을 통해 SELinux 보안옵션이 적용되어 있는지 확인
$ ps -ef | grep docker | grep selinux-enabled
 
▪ 아래와 같은 명령어를 통해 SELinux 보안옵션이 적용되어 있는지 확인
$ docker ps --quiet --all | xargs docker inspect —format “{{ .Id }}: SecurityOpt={{ .HostConfig.SecurityOpt }}”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 아래와 같은 단계로 SELinux 옵션 설정
1) SELinux 상태 설정
2) SELinux 정책 설정
3) 도커 컨테이너를 위한 SELinux 정책 템플릿을 생성하거나 가져오기
4) SELinux가 활성화 되도록 도커 데몬 시작</td></tr>
</table>

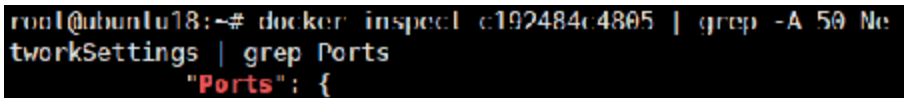
	(방법 1) docker daemon --selinux-enabled (방법 2) /etc/default/docker 파일에 아래와 같은 옵션 추가 후 데몬 재시작 DOCKER_OPTS="--selinux-enabled" 5) $ docker run --interactive --tty --security-opt label=level:TopSecret centos /bin/bash
비고	▪ 참고 사이트 1) https://docs.docker.com/engine/security/security/#other-kernel-security-features 2) https://docs.docker.com/engine/reference/run/#security-configuration 3) https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7

<table>
<tr><td>진단항목</td><td colspan="2">DO-28. 컨테이너에서 ssh 사용 금지</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">대부분 백업, 로그 확인, 프로세스 재시작, 설정 변경과 같은 작업을 위해 SSH를 사용한다. 하지만 Docker 컨테이너에서의 이러한 작업은 SSH가 없어도 가능하다. SSH 접속을 위해 사용하는 키와 패스워드는 이미지와 같이 생성하거나 불륨에 넣는다. 키와 패스워드를 갱신해야 할 때, 이미지 안에 넣은 경우 이미지를 다시 만들어 배포하고 컨테이너를 다시 시작해야 한다. 인증정보를 볼륨에 넣어두고 관리하는 경우에는 컨테이너에 쓰기 권한을 부여해서는 안 된다. 컨테이너가 인증정보를 파손시킬 수 있기 때문이다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">컨테이너에 SSH가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">컨테이너에 SSH가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래와 같은 절차로 컨테이너에 SSH가 활성화 되어 있는지 확인
1) 실행중인 컨테이너 목록을 확인
2) $ docker ps —quiet
 

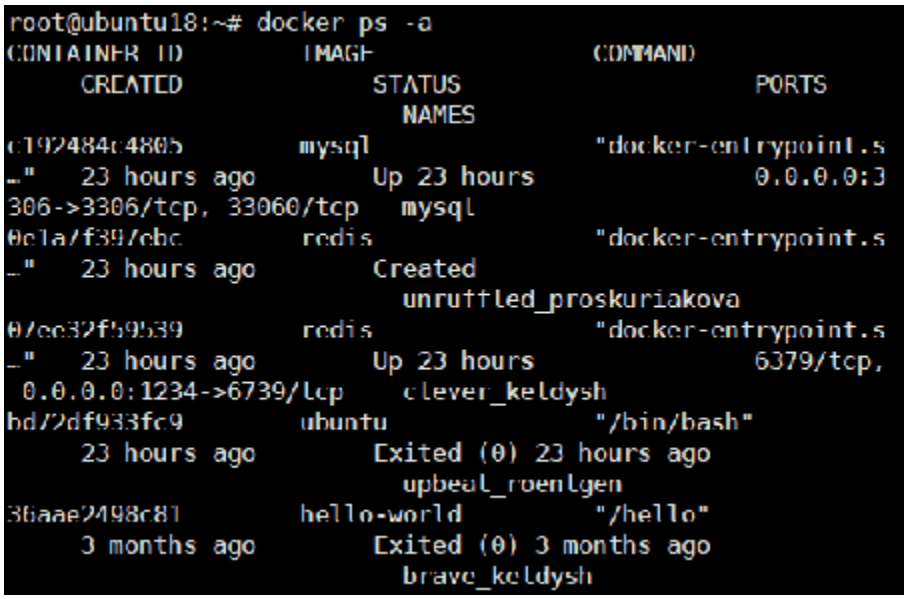
3) 실행중인 컨테이너의 활성화된 서비스 확인
4) $ docker exec $INSTANCE_ID ps –el
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 컨테이너에서 SSH를 제거하고 nsenter 또는 docker exec 및 docker attach와 같은 명령어를 통해 컨테이너에 접속
(방법 1) $ docker exec --interactive --tty $INSTANCE_ID sh
 

(방법 2) docker attach $INSTANCE_ID
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-29. 컨테이너에 privileged 포트 매핑 금지</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">TCP/IP 포트 중 1024 미만의 포트는 권한이 있는 포트로 특정한 쓰임새를 위해서 IANA에서 할당한 포트번호이다. 일반 사용자 및 프로세스는 다양한 보안상의 이유로 privileged 포트를 사용하지 않는 것이 좋다. Docker를 사용하면 컨테이너 포트를 privileged 포트에 매핑할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">컨테이너 포트가 privileged 포트에 매핑되어 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">컨테이너 포트가 privileged 포트에 매핑되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
■ 아래와 같은 절차로 privileged 포트가 매핑되어 있는지 확인
1) 컨테이너 목록 확인
2) $ docker ps --quiet --all


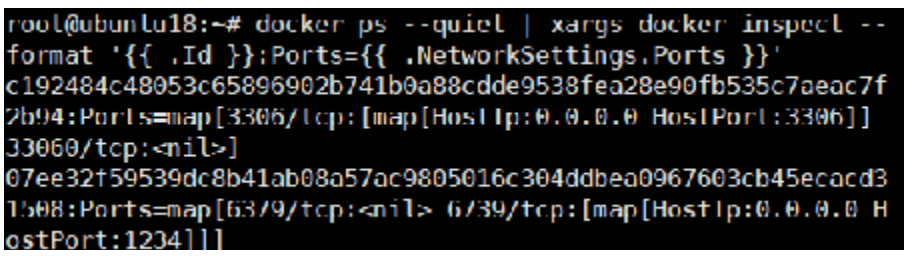
3) 각 컨테이너에 매핑된 포트 확인
4) $ docker inspect <CONTAINER ID> | grep -A 50 NetworkSettings | grep Ports


■ 컨테이너 전체 목록을 출력하는 옵션을 통해 매핑된 포트 확인
$ docker ps –a
</td></tr>
</table>

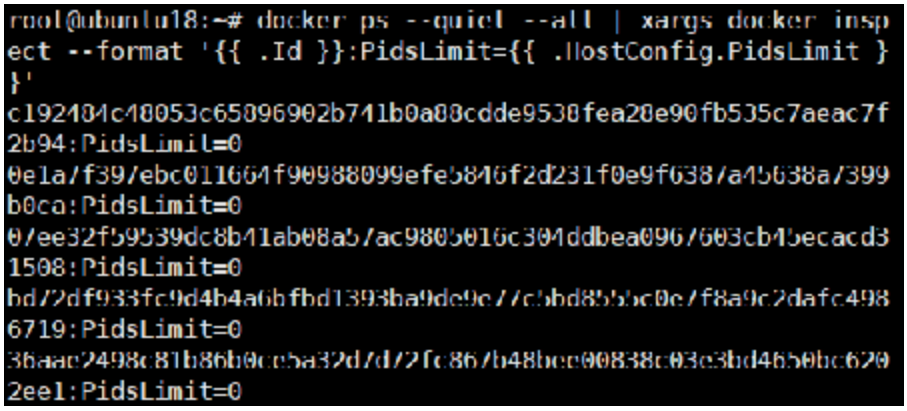


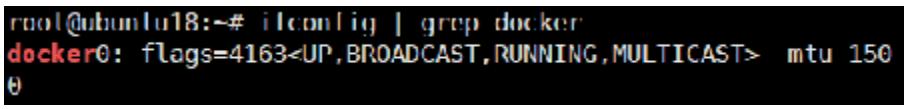
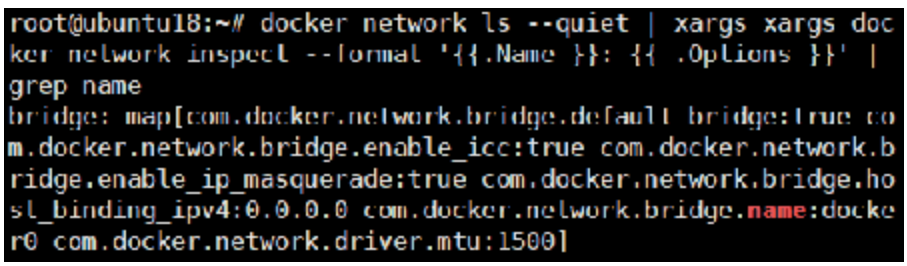
- 아래와 같은 명령어로 컨테이너에 매핑된 포트 확인

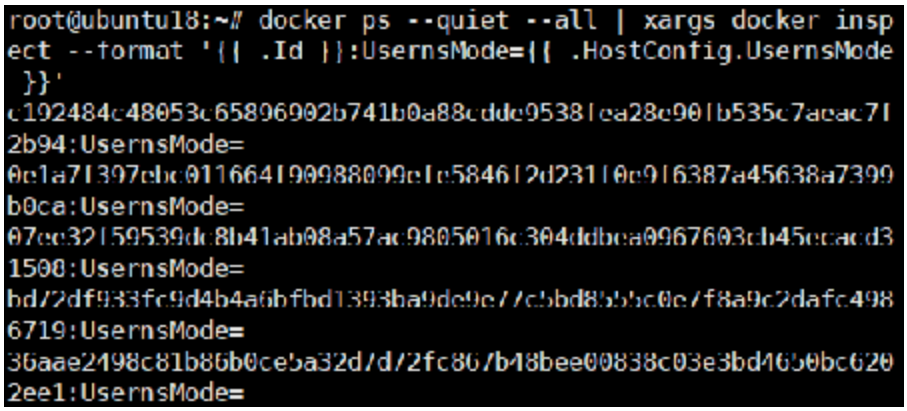
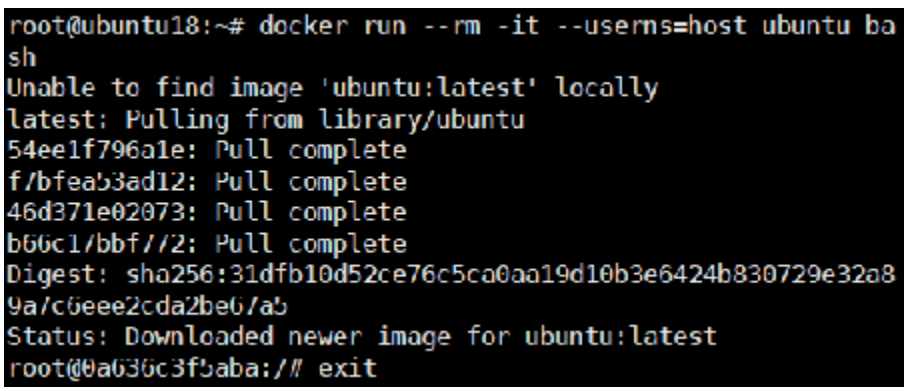
  $ docker ps --quiet | xargs docker inspect --format '{{ .Id }}:Ports={{ .NetworkSettings.Ports }}'

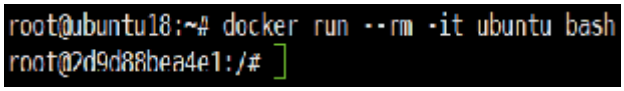


조치방법	▪ 컨테이너를 시작할 때 컨테이너 포트를 호스트의 privileged 포트가 아닌 포트에 매핑 ▪ Docker 파일에서 privileged 포트 매핑 선언을 호스팅 하는 컨테이너가 없는지 확인
비고	

<table>
<tr><td>진단항목</td><td colspan="2">DO-30. PIDs cgroup 제한</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">공격자는 컨테이너 내부에서 포크 폭탄을 실행할 수 있다. 이 포크 폭탄은 전체 시스템을 손상시킬 수 있으므로 컨테이너 내부에서 발생할 수 있는 포크의 수를 제한함으로써 이러한 공격을 방지하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">PIDs cgroup 제한 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">PIDs cgroup 제한 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ PIDs cgroup 제한 설정이 적용되어 있는지 확인
$ docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}:PidsLimit={{ .HostConfig.PidsLimit }}'
 
※ PidsLimit 값이 0 또는 -1로 되어있으면 컨테이너 내부에서 동시에 모든 수의 프로세스를 fork 할 수 있음</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 컨테이너 시작시--pids-limit 플래그를 사용
예시) $ docker run –it --pids-limit 100 <Image_ID></td></tr>
<tr><td>비고</td><td colspan="4">docker 1.11 버전에서 추가된 옵션</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-31. 도커의 default bridge docker0 사용 제한</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">Docker는 브리지 모드에서 생성된 가상 인터페이스를 docker0라는 공통 브리지에 연결한다. 이 네트워크 모델은 필터링이 적용되지 않기 때문에 ARP Spoofing 및 MAC Flooding 등의 공격에 취약하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Default bridge docker0를 사용하고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">Default bridge docker0를 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ ifconfig 명령어를 통해 Default bridge docker0를 사용하고 있는지 확인
$ ifconfig | grep docker
 
▪ Docker 명령어를 통해 Default bridge docker0를 사용하고 있는지 확인
$ docker network ls --quiet | xargs xargs docker network inspect --format '{{. Name }}: {{ .Options }}' | grep name
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 사용자 정의 네트워크를 설정하고, 정의된 네트워크에서 컨테이너를 실행하여야 함
예시) $ vi /etc/docker/daemon.json
{
“bip”: “192.168.1.5/24”,
“fixed-cidr”: “192.168.1.5/25”,
“fixed-cidr-v6”: “2001:db8::/64”,
“mtu”: 1500,
“default-gateway”: “10.20.1.1”,
“default-gateway-v6”: “2001:db8:abcd::89”,
“dns”:[“10.20.1.2”, “10.20.1.3”]
}</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">DO-32. 호스트의 user namespaces 공유 제한</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">user namespaces는 컨테이너 내부의 루트 프로세스가 컨테이너 외부의 루트가 아닌 프로세스에 매핑되도록 한다. 따라서 호스트의 use namespaces을 컨테이너와 공유하면 호스트의 사용자와 컨테이너의 사용자가 분리되지 않는다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">호스트의 user namespace를 컨테이너와 공유하고 있지 않은 경우</td></tr>
<tr><td>취약</td><td colspan="3">호스트의 user namespace를 컨테이너와 공유하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 아래 명령어를 통해 UsernsMode 값을 반환하는지 확인
$ docker ps --quiet --all | xargs docker inspect --format '{{ .Id }}:UsernsMode={{ .HostConfig.UsernsMode }}'
 
※ host 값을 반환하는 경우 호스트 user namespaces가 컨테이너와 공유되고 있음</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 호스트와 컨테이너 간에 user namespaces를 공유하지 않아야 함
예시) $ docker run --rm –it --userns=host ubuntu bash -> 취약
 
$ docker run --rm -it ubuntu bash -> 양호</td></tr>
</table>

	 root@ubuntu18:~# docker run --rm -it ubuntu bash root@2d9d88bea4e1:/#
비고	

2.17. OpenStack

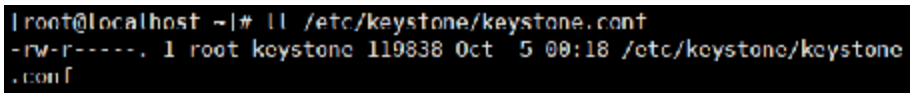
파일 권한 관리(14개 항목), 암호화(15개 항목), 보안 설정(18개 항목), 총 3개 영역에서 47개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 파일 권한 관리	OT-01	Identity 설정파일 소유권 설정	상
	OT-02	Identity 설정파일 접근권한 설정	상
	OT-03	Dashboard 설정파일 소유권 설정	상
	OT-04	Dashboard 설정파일 접근권한 설정	상
	OT-05	Compute 설정파일 소유권 설정	상
	OT-06	Compute 설정파일 접근권한 설정	상
	OT-07	블록 스토리지 서비스 설정파일 소유권 설정	상
	OT-08	블록 스토리지 서비스 설정파일 접근권한 설정	상
	OT-09	이미지 스토리지 설정파일 소유권 설정	상
	OT-10	이미지 스토리지 설정파일 접근권한 설정	상
	OT-11	공유파일 시스템 설정파일 소유권 설정	상
	OT-12	공유파일 시스템 설정파일 접근권한 설정	상
	OT-13	네트워킹 서비스 설정파일 소유권 설정	상
	OT-14	네트워킹 서비스 설정파일 접근권한 설정	상
나. 암호화	OT-15	Identity TLS 활성화	상
	OT-16	PKI토큰의 강력한 해시 알고리즘 사용	상
	OT-17	Dashboard의 SECURE_PROXY_SSL_HEADER 설정	상
	OT-18	Compute 인증을 위한 보안프로토콜 사용	상
	OT-19	Nova와 Glance의 안전한 통신	상
	OT-20	블록 스토리지 서비스 인증을 위한 TLS 활성화	상
	OT-21	cinder와 nova의 TLS 통신	상
	OT-22	cinder와 glance의 TLS 통신	상
	OT-23	이미지 스토리지 서비스 인증을 위한 TLS 활성화	상
	OT-24	공유 파일 시스템 인증을 위한 TLS 활성화	상
	OT-25	TLS를 이용한 공유 파일 시스템과 Compute의 통신	상
	OT-26	TLS를 이용한 공유 파일 시스템과 네트워킹과의 연결	상
	OT-27	TLS를 이용한 공유 파일 시스템과 블록 스토리지 서비스와의 연결	상
	OT-28	네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용	상
	OT-29	Neutron API 서버의 TLS 활성화	상

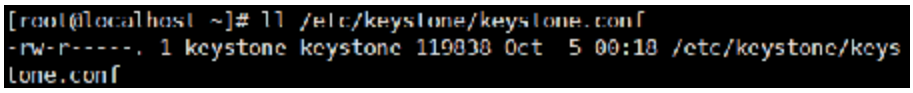
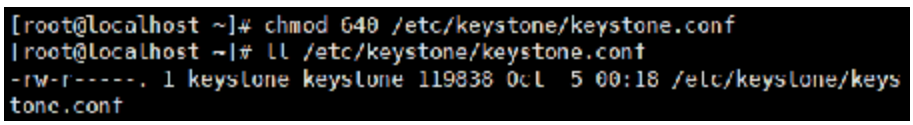
구분	진단코드	진단 항목	취약도
다. 보안 설정	OT-30	Identity 서비스 max_request_body_size 설정	상
	OT-31	admin 토큰 비활성화	상
	OT-32	Dashboard의 DISALLOW_IFRAME_EMBED 설정	상
	OT-33	Dashboard의 CSRF_COOKIE_SECURE 설정	상
	OT-34	Dashboard의 SESSION_COOKIE_SECURE 설정	상
	OT-35	Dashboard의 SESSION_COOKIE_HTTPONLY 설정	상
	OT-36	Dashboard의 PASSWORD_AUTOCOMPLETE 설정	상
	OT-37	Dashboard의 DISABLE_PASSWORD_REVEAL 설정	상
	OT-38	Dashboard의 ENFORCE_PASSWORD_CHECK 설정	상
	OT-39	Dashboard의 PASSWORD_VALIDATOR 설정	상
	OT-40	Compute의 인증을 위한 keystone 사용	상
	OT-41	블록 스토리지 서비스의 인증을 위한 keystone 사용	상
	OT-42	안전한 환경에서의 NAS 운영	상
	OT-43	블록 스토리지 서비스에서 요청 본문 최대 크기 설정	상
	OT-44	블록 스토리지 볼륨 암호화	상
	OT-45	이미지 스토리지 서비스 인증을 위한 keystone 설정	상
	OT-46	공유파일 시스템 인증을 위한 오픈스택 Identity 사용	상
	OT-47	공유파일 시스템에서 요청 본문 최대 사이즈 설정	상

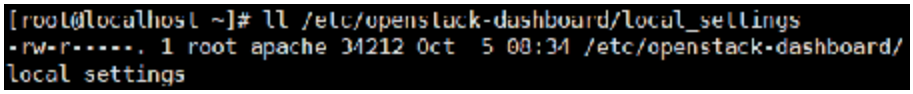
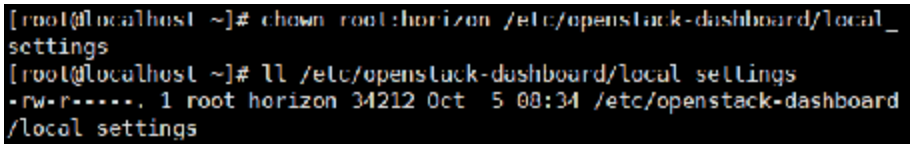
[표 17] OpenStack 진단 체크리스트

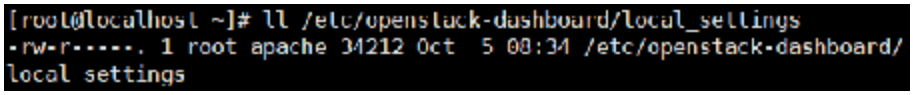
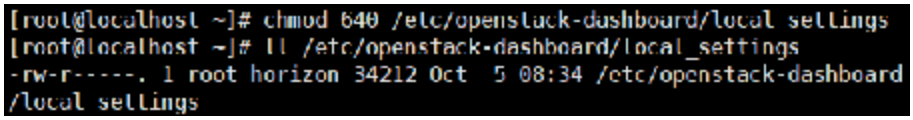
가. 파일 권한 관리

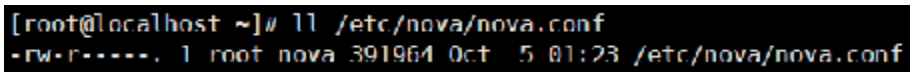
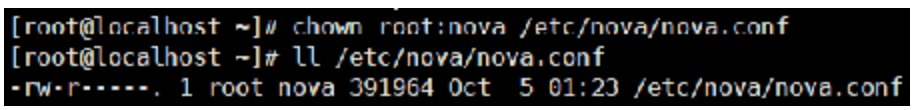
<table>
<tr><td>진단항목</td><td colspan="2">OT-01. Identity 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 해당 구성요소 소유자로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Identity 설정 파일의 소유자 및 소유그룹이 keystone으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Identity 설정 파일의 소유자 및 소유그룹이 keystone이 아닌 다른 소유자또는 소유그룹으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Identity 설정파일의 소유자 소유그룹이 keystone/keystone로 출력되는지 확인
ll /etc/keystone/keystone.conf
ll /etc/keystone/keystone-paste.ini
ll /etc/keystone/policy.json
ll /etc/keystone/logging.conf
ll /etc/keystone/ssl/certs/signing_cert.pem
ll /etc/keystone/ssl/private/signing_key.pem
ll /etc/keystone/ssl/certs/ca.pem
ex)
ll /etc/keystone/keystone.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Identity 설정파일의 소유자 소유그룹을 keystone/keystone로 변경
chown keystone:keystone /etc/keystone/keystone.conf
chown keystone:keystone /etc/keystone/keystone-paste.ini
chown keystone:keystone /etc/keystone/policy.json
chown keystone:keystone /etc/keystone/logging.conf
chown keystone:keystone /etc/keystone/ssl/certs/signing_cert.pem
chown keystone:keystone /etc/keystone/ssl/private/signing_key.pem
chown keystone:keystone /etc/keystone/ssl/certs/ca.pem
ex)
chown keystone:keystone /etc/keystone/keystone.conf</td></tr>
</table>

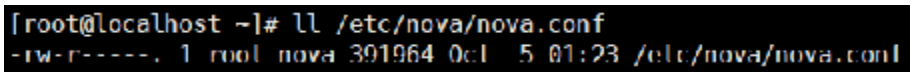
	[root@localhost ~]# chown keystone:keystone /etc/keystone/keystone.conf [root@localhost ~]# ll /etc/keystone/keystone.conf -rw-r-----. 1 keystone keystone 119838 Oct 5 00:18 /etc/keystone/keystone.conf
비고	

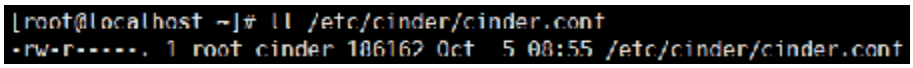
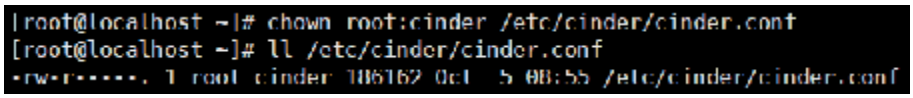
<table>
<tr><td>진단항목</td><td colspan="2">OT-02. Identity 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 설정 파일들에 엄격한 접근권한을 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Identity 설정 파일의 퍼미션이 640 또는 그보다 엄격하게 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Identity 설정 파일의 퍼미션이 최소 640으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Identity 설정파일의 퍼미션을 확인
ll /etc/keystone/keystone.conf
ll /etc/keystone/keystone-paste.ini
ll /etc/keystone/policy.json
ll /etc/keystone/logging.conf
ll /etc/keystone/ssl/certs/signing_cert.pem
ll /etc/keystone/ssl/private/signing_key.pem
ll /etc/keystone/ssl/certs/ca.pem
ex)
ll /etc/keystone/keystone.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Identity 설정파일의 퍼미션을 최소 640으로 설정
chmod 640 /etc/keystone/keystone.conf
chmod 640 /etc/keystone/keystone-paste.ini
chmod 640 /etc/keystone/policy.json
chmod 640 /etc/keystone/logging.conf
chmod 640 /etc/keystone/ssl/certs/signing_cert.pem
chmod 640 /etc/keystone/ssl/private/signing_key.pem
chmod 640 /etc/keystone/ssl/certs/ca.pem
ex)
chmod 640 /etc/keystone/keystone.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

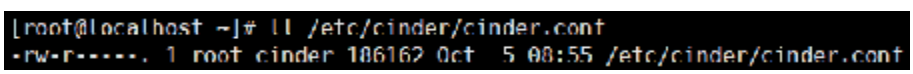
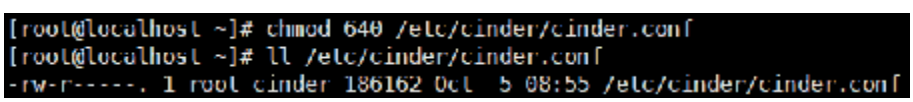
<table>
<tr><td>진단항목</td><td colspan="2">OT-03. Dashboard 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부될 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/horizon으로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Dashboard 설정 파일의 소유자 및 소유그룹이 root/horizon으로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Dashboard 설정 파일의 소유자 및 소유그룹이 root/horizon으로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Dashboard 설정파일의 소유자 소유그룹이 root/horizon으로 출력되는지 확인
ll /etc/openstack-dashboard/local_settings.py
또는
ll /etc/openstack-dashboard/local_settings
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Dashboard 설정파일의 소유자 소유그룹을 root/horizon로 변경
chown root:horizon /etc/openstack-dashboard/local_settings.py
또는
chown root:horizon /etc/openstack-dashboard/local_settings
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

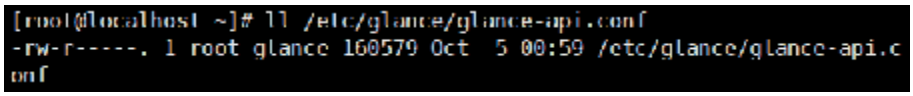
<table>
<tr><td>진단항목</td><td colspan="2">OT-04. Dashboard 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일의 접근권한을 엄격하게 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Dashboard 설정파일의 퍼미션이 640 또는 그보다 엄격하게 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Dashboard 설정 파일의 퍼미션이 최소 640으로 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Dashboard 설정파일 퍼미션을 확인
ll /etc/openstack-dashboard/local_settings.py
또는
ll /etc/openstack-dashboard/local_settings
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/openstack-dashboard/local_settings.py
또는
chmod 640 /etc/openstack-dashboard/local_settings
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

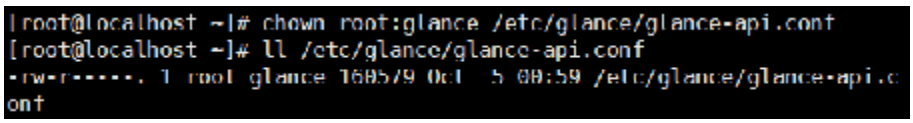
<table>
<tr><td>진단항목</td><td colspan="2">OT-05. Compute 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 의도적으로 또는 실수로 권한이 없는 사용자가 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 서비스 거부가 발생할 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/nova로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Compute 설정 파일의 소유자 및 소유그룹이 root/nova로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Compute 설정 파일의 소유자 및 소유그룹이 root/nova로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Compute 설정파일의 소유자 소유그룹이 root/nova으로 출력되는지 확인
ll /etc/nova/nova.conf
ll /etc/nova/api-paste.ini
ll /etc/nova/policy.json
ll /etc/nova/rootwrap.conf
ex)
ll /etc/nova/nova.conf
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Compute 설정파일의 소유자 소유그룹을 root/nova로 변경
chown root:nova /etc/nova/nova.conf
chown root:nova /etc/openstack-dashboard/local_settings
chown root:nova /etc/nova/policy.json
chown root:nova /etc/nova/rootwrap.conf
ex)
chown root:nova /etc/nova/nova.conf
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

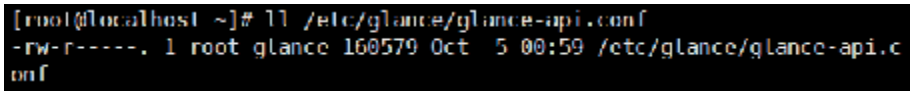
<table>
<tr><td>진단항목</td><td colspan="2">OT-06. Compute 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 의도적으로 또는 실수로 권한이 없는 사용자가 매개변수 또는 파일 자체를 수정하거나 삭제하면 심각한 서비스 거부가 발생할 수 있다. 따라서 중요한 설정 파일의 접근권한을 엄격하게 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Compute 설정 파일의 접근권한이 640이거나 그보다 엄격한 경우</td></tr>
<tr><td>취약</td><td colspan="3">Compute 설정 파일의 접근권한이 최소 640으로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Compute 설정파일의 소유자 소유그룹이 root/nova으로 출력되는지 확인
ll /etc/nova/nova.conf
ll /etc/nova/api-paste.ini
ll /etc/nova/policy.json
ll /etc/nova/rootwrap.conf
ex)
ll /etc/nova/nova.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Compute 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/nova/nova.conf
chmod 640 /etc/openstack-dashboard/local_settings
chmod 640 /etc/nova/policy.json
chmod 640 /etc/nova/rootwrap.conf
ex)
chmod 640 /etc/nova/nova.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-07. 블록 스토리지 서비스 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 만약에 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제가 발생한다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/cinder로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">블록 스토리지 서비스 설정 파일의 소유자 및 소유그룹이 root/cinder로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">블록 스토리지 서비스 설정 파일의 소유자 및 소유그룹이 root/cinder로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 블록 스토리지 서비스 설정파일의 소유자 소유그룹이 root/cinder로 출력되는지 확인
ll /etc/cinder/cinder.conf
ll /etc/cinder/api-paste.ini
ll /etc/cinder/policy.json
ll /etc/cinder/rootwrap.conf
ex)
ll /etc/cinder/cinder.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 블록 스토리지 서비스 설정파일의 소유자 소유그룹을 root/cinder로 변경
chown root:cinder /etc/cinder/cinder.conf
chown root:cinder /etc/cinder/api-paste.ini
chown root:cinder /etc/cinder/policy.json
chown root:cinder /etc/cinder/rootwrap.conf
ex)
chown root:cinder /etc/cinder/cinder.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

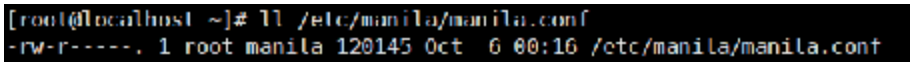
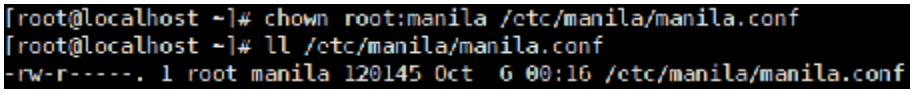
<table>
<tr><td>진단항목</td><td colspan="2">OT-08. 블록 스토리지 서비스 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 만약에 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제가 발생한다. 따라서 중요한 설정 파일은 엄격한 접근권한을 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">블록 스토리지 서비스 설정파일의 퍼미션이 640이거나 그보다 엄격한 경우</td></tr>
<tr><td>취약</td><td colspan="3">블록 스토리지 서비스 설정파일의 퍼미션이 최소 640으로 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 블록 스토리지 서비스 설정파일의 퍼미션을 확인
ll /etc/cinder/cinder.conf
ll /etc/cinder/api-paste.ini
ll /etc/cinder/policy.json
ll /etc/cinder/rootwrap.conf
ex)
ll /etc/cinder/cinder.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 블록 스토리지 서비스 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/cinder/cinder.conf
chmod 640 /etc/cinder/api-paste.ini
chmod 640 /etc/cinder/policy.json
chmod 640 /etc/cinder/rootwrap.conf
ex)
chmod 640 /etc/cinder/cinder.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

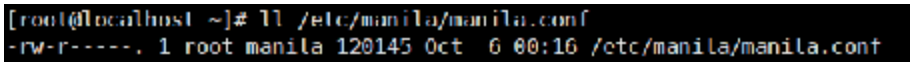
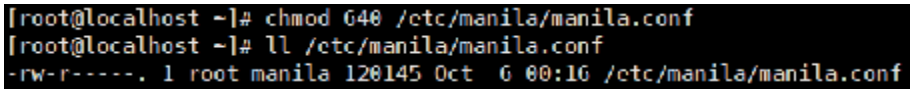
<table>
<tr><td>진단항목</td><td colspan="2">OT-09. 이미지 스토리지 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 root/glance로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">이미지 스토리지 설정 파일의 소유자 및 소유그룹이 root/glance로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">이미지 스토리지 설정 파일의 소유자 및 소유그룹이 root/glance로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 이미지 스토리지 설정파일의 소유자 소유그룹이 root/glance로 출력되는지 확인
ll /etc/glance/glance-api-paste.ini
ll /etc/glance/glance-api.conf
ll /etc/glance/glance-cache.conf
ll /etc/glance/glance-manage.conf
ll /etc/glance/glance-registry-paste.ini
ll /etc/glance/glance-registry.conf
ll /etc/glance/glance-scrubber.conf
ll /etc/glance/glance-swift-store.conf
ll /etc/glance/policy.json
ll /etc/glance/schema-image.json
ll /etc/glance/schema.json
ex)
ll /etc/glance/glance-api.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 이미지 스토리지 설정파일의 소유자 소유그룹을 root/glance로 변경
chown root:glance /etc/glance/glance-api-paste.ini
chown root:glance /etc/glance/glance-api.conf
chown rootglance /etc/glance/glance-cache.conf
chown root:glacne /etc/glance/glance-manage.conf
chown root:glacne /etc/glance/glance-registry-paste.ini
chown root:glacne /etc/glance/glance-registry.conf
chown root:glacne /etc/glance/glance-scrubber.conf
chown root:glacne /etc/glance/glance-swift-store.conf</td></tr>
</table>

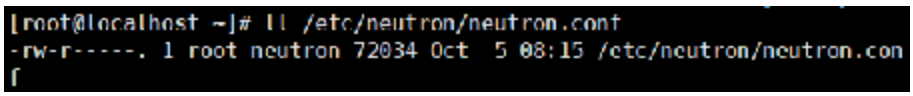
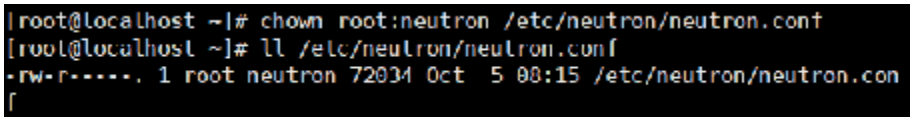
	# chown root:glacne /etc/glance/policy.json # chown root:glacne /etc/glance/schema-image.json # chown root:glacne /etc/glance/schema.json ex) # chown root:glance /etc/glance/glance-api.conf 
비고	

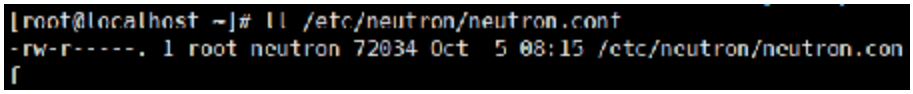
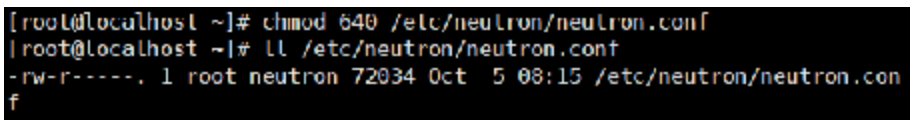
<table>
<tr><td>진단항목</td><td colspan="2">OT-10. 이미지 스토리지 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일의 접근권한은 엄격하게 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">이미지 스토리지 설정 파일의 퍼미션이 640 또는 그보다 엄격한 경우</td></tr>
<tr><td>취약</td><td colspan="3">이미지 스토리지 설정 파일의 퍼미션이 최소 640으로 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 이미지 스토리지 설정파일의 퍼미션이 640이하로 되어있는지 확인
ll /etc/glance/glance-api-paste.ini
ll /etc/glance/glance-api.conf
ll /etc/glance/glance-cache.conf
ll /etc/glance/glance-manage.conf
ll /etc/glance/glance-registry-paste.ini
ll /etc/glance/glance-registry.conf
ll /etc/glance/glance-scrubber.conf
ll /etc/glance/glance-swift-store.conf
ll /etc/glance/policy.json
ll /etc/glance/schema-image.json
ll /etc/glance/schema.json
ex)
ll /etc/glance/glance-api.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 이미지 스토리지 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/glance/glance-api-paste.ini
chmod 640 /etc/glance/glance-api.conf
chmod 640 /etc/glance/glance-cache.conf
chmod 640 /etc/glance/glance-manage.conf
chmod 640 /etc/glance/glance-registry-paste.ini
chmod 640 /etc/glance/glance-registry.conf
chmod 640 /etc/glance/glance-scrubber.conf
chmod 640 /etc/glance/glance-swift-store.conf</td></tr>
</table>

	# chmod 640 /etc/glance/policy.json # chmod 640 /etc/glance/schema-image.json # chmod 640 /etc/glance/schema.json ex) # chmod 640 /etc/glance/glance-api.conf [root@localhost ~]# chmod 640 /etc/glance/glance-api.conf [root@localhost ~]# ll /etc/glance/glance-api.conf -rw-r-----. 1 root glance 160579 Oct 5 00:59 /etc/glance/glance-api.conf
비고	

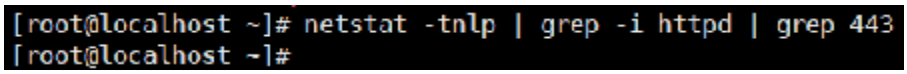
<table>
<tr><td>진단항목</td><td colspan="2">OT-11. 공유파일 시스템 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자 및 소유그룹은 root/manila로 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">공유파일 시스템 설정 파일의 소유자 및 소유그룹이 root/manila로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">공유파일 시스템 설정 파일의 소유자 및 소유그룹이 root/manila로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 공유파일 시스템 설정파일의 소유자 소유그룹이 root/manila로 출력되는지 확인
ll /etc/manila/manila.conf
ll /etc/manila/api-paste.ini
ll /etc/manila/policy.json
ll /etc/manila/rootwrap.conf
ex)
ll /etc/manila/manila.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 공유파일 시스템 설정파일의 소유자 소유그룹을 root/manila로 변경
chown root:manila /etc/manila/manila.conf
chown root:manila /etc/manila/api-paste.ini
chown root:manila /etc/manila/policy.json
chown root:manila /etc/manila/rootwrap.conf
ex)
chown root:manila /etc/manila/manila.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

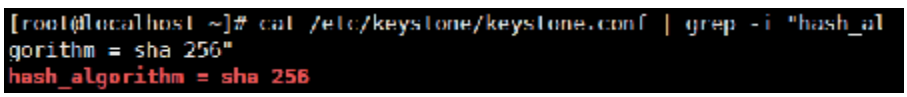
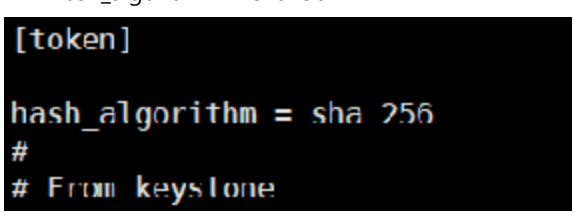
<table>
<tr><td>진단항목</td><td colspan="2">OT-12. 공유파일 시스템 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 접근권한을 엄격하게 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">공유파일 시스템 설정 파일의 퍼미션이 640 또는 그보다 엄격한 경우</td></tr>
<tr><td>취약</td><td colspan="3">공유파일 시스템 설정 파일의 640으로 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 공유파일 시스템 설정파일의 퍼미션이 640이하로 되어있는지 확인
ll /etc/manila/manila.conf
ll /etc/manila/api-paste.ini
ll /etc/manila/policy.json
ll /etc/manila/rootwrap.conf
ex)
ll /etc/manila/manila.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 공유파일 시스템 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/manila/manila.conf
chmod 640 /etc/manila/api-paste.ini
chmod 640 /etc/manila/policy.json
chmod 640 /etc/manila/rootwrap.conf
ex)
chmod 640 /etc/manila/manila.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-13. 네트워킹 서비스 설정파일 소유권 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들의 소유자/소유그룹은 root/neutron으로 설정하고 엄격한 접근권한을 설정하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">네트워킹 서비스 설정 파일의 소유자 및 소유그룹이 root/neutron으로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">네트워킹 서비스 설정 파일의 소유자 및 소유그룹이 root/neutron으로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 네트워킹 서비스 설정파일의 소유자/소유그룹이 root/neutron로 출력되는지 확인
ll /etc/neutron/neutron.conf
ll /etc/neutron/api-paste.ini
ll /etc/neutron/policy.json
ll /etc/neutron/rootwrap.conf
ex)
ll /etc/neutron/neutron.conf
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 네트워킹 서비스 설정파일의 소유자/소유그룹을 root/neutron로 변경
chown root:neutron /etc/neutron/neutron.conf
chown root:neutron /etc/neutron/api-paste.ini
chown root:neutron /etc/neutron/policy.json
chown root:neutron /etc/neutron/rootwrap.conf
ex)
chown root:neutron /etc/neutron/neutron.conf
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

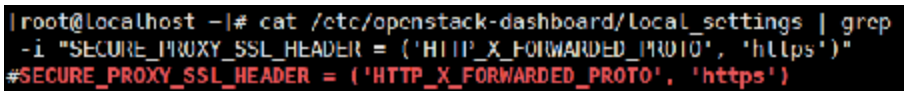
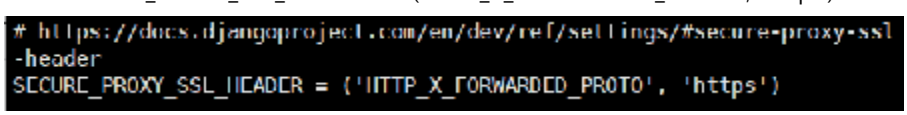
<table>
<tr><td>진단항목</td><td colspan="2">OT-14. 네트워킹 서비스 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일들에는 구성 요소의 원활한 기능을 수행하는데 필요한 중요한 매개변수와 정보가 들어있다. 권한이 없는 사용자가 의도적으로 또는 실수로 매개변수나 파일 자체를 수정하거나 삭제하면 심각한 가용성 문제로 인해 다른 사용자에게 서비스가 거부 될 수 있다. 따라서 중요한 설정 파일들에 엄격한 접근권한을 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">네트워킹 서비스 설정 파일의 퍼미션이 또는 그보다 엄격한 경우</td></tr>
<tr><td>취약</td><td colspan="3">네트워킹 서비스 설정 파일의 퍼미션이 640 최소 640으로 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 네트워킹 서비스 설정파일의 퍼미션이 640 이하로 되어있는지 확인
ll /etc/neutron/neutron.conf
ll /etc/neutron/api-paste.ini
ll /etc/neutron/policy.json
ll /etc/neutron/rootwrap.conf
ex)
ll /etc/neutron/neutron.conf
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 네트워킹 서비스 설정파일의 퍼미션을 640으로 설정
chmod 640 /etc/neutron/neutron.conf
chmod 640 /etc/neutron/api-paste.ini
chmod 640 /etc/neutron/policy.json
chmod 640 /etc/neutron/rootwrap.conf
ex)
chmod 640 /etc/neutron/neutron.conf
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

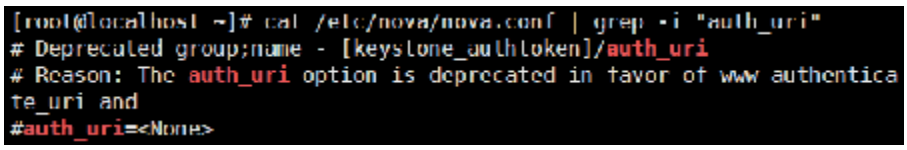
나. 암호화

<table>
<tr><td>진단항목</td><td colspan="2">OT-15. Identity TLS 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 통신에는 민감한 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보에 접근하기 위해 채널을 도청하려고 시도할 수 있다. 따라서 모든 구성요소는 HTTPS와 같은 보안 통신 프로토콜을 사용하여 통신해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">HTTP서버에 TLS가 활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">HTTP서버에 TLS가 활성화되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ TLS 서비스 포트가 오픈되어 있는지 확인
netstat –tnlp | grep –i httpd | grep 443
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ TLS 서비스 활성화
SSL 설정을 활성화한 뒤, TLS 프로토콜을 활성화</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

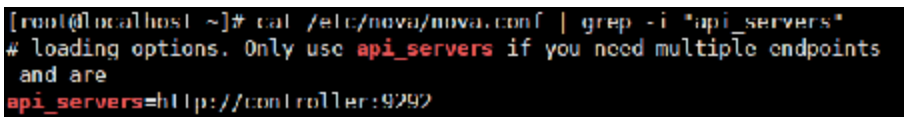
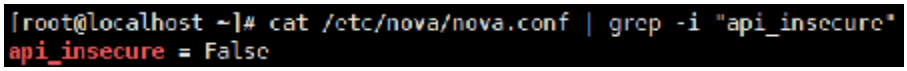
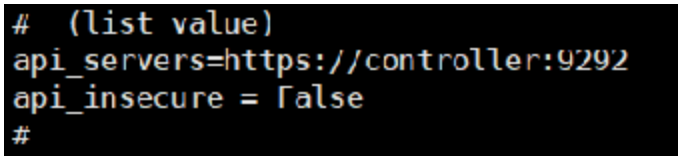
<table>
<tr><td>진단항목</td><td colspan="2">OT-16. PKI토큰의 강력한 해시 알고리즘 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">MD5는 취약하고 가치가 떨어지는 해시 알고리즘으로 무차별 대입 공격으로 크랙될 수 있다. 아이덴티티 토큰은 민감하므로 비인가 노출 및 접근을 방지하기 위해 강력한 해시 알고리즘으로 보호해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 [token] 섹션의 hash_algorithm 매개변수가 SHA256으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 [token] 섹션의 hash_algorithm 매개변수가 SHA256 보다 약한 알고리즘으로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/keystone/keystone.conf 파일에서 hash_algorithm 설정 값 확인
cat /etc/keystone/keystone.conf | grep –i “hash_algorithm = sha256”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ /etc/keystone/keystone.conf 파일에서 hash_algorithm 값을 sha256으로 설정
vi /etc/keystone/keystone.conf
[token]
...
hash_algorithm = sha256
 

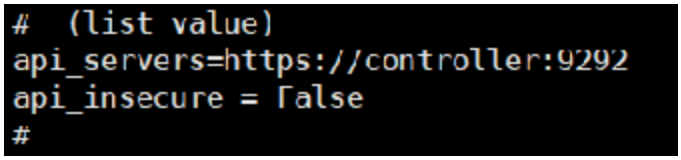
※ [default]로는 hash_algorithm = md5로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

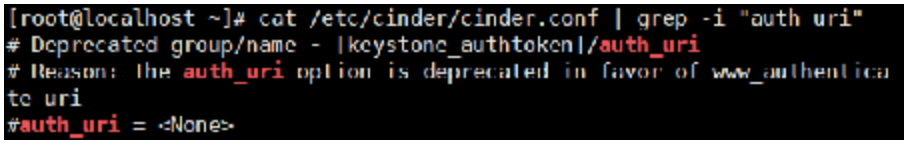
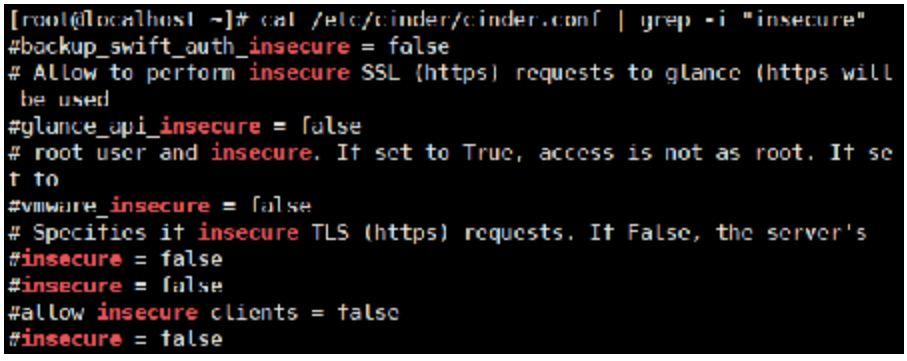
<table>
<tr><td>진단항목</td><td colspan="2">OT-17. Dashboard의 SECURE_PROXY_SSL_HEADER 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 대시보드가 프록시 뒤에 위치하고 프록시가 들어오는 모든 요청에 대해 X-Forwarded-Proto 헤더를 제거하거나 X-Forwarded-Proto를 설정하고 대시보드에 보내지만 HTTPS를 이용하는 경우에는 SECURE_PROXY_SSL_HEADER를 설정하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 매개변수가 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 매개변수가 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정되어 있지 않거나 주석처리 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 설정값 확인
cat /etc/openstack-dashboard/local_settings | grep -i "SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')"
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SECURE_PROXY_SSL_HEADER 값을 ('HTTP_X_FORWARDED_PROTO', 'https')로 설정
vi /etc/openstack-dashboard/local_settings.py
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')
또는
vi /etc/openstack-dashboard/local_settings
SECURE_PROXY_SSL_HEADER = ('HTTP_X_FORWARDED_PROTO', 'https')
 
※ [default]로는 SECURE_PROXY_SSL_HEADER = <none>으로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-18. Compute 인증을 위한 보안프로토콜 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하고, insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하지 않고, insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인
cat /etc/nova/nova.conf | grep –i “auth_uri”
 
■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인
cat /etc/nova/nova.conf | grep –i “insecure”
  </td></tr>
<tr><td>조치
방법</td><td colspan="4">■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정
vi /etc/nova/nova.conf
[keystone_authtoken]</td></tr>
</table>

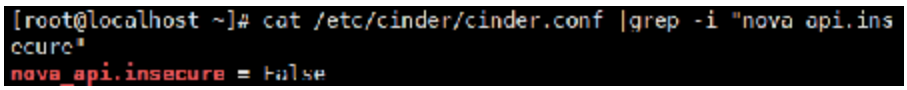
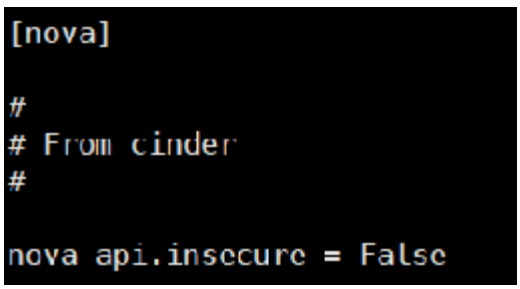
	... auth_uri = https://x.x.x.x [주소] [keystone_authtoken] auth uri = https://controller:5000 ■ /etc/nova/nova.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 false 로 설정 # vi /etc/nova/nova.conf [keystone_authtoken] ... insecure = false # Verify HTTPS connections. (boolean value) insecure=false ※ [default]로는 auth_uri = None으로 되어있음
비고	

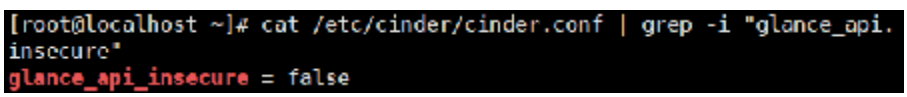
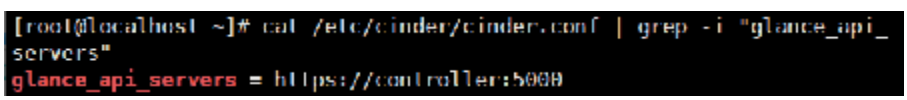
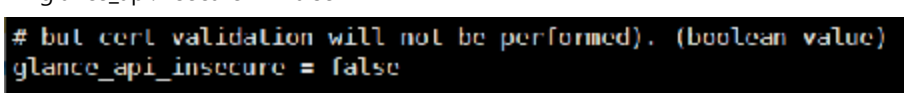
<table>
<tr><td>진단항목</td><td colspan="2">OT-19. Nova와 Glance의 안전한 통신</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 매개변수가 https://로 시작하고, api_insecure 매개변수가 False로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 매개변수가 https://로 시작하지 않고, api_insecure 매개변수가 True로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 설정값 확인
cat /etc/nova/nova.conf | grep –i “api_servers”
 
▪ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 설정값 확인
cat /etc/nova/nova.conf | grep –i “api_insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_servers 값을 https://로 시작하도록 설정
vi /etc/nova/nova.conf
[glance]
…
api_servers = https://x.x.x.x
 
▪ /etc/nova/nova.conf 파일에서 [glance] 섹션의 api_insecure 값을 false로 설정
vi /etc/nova/nova.conf
[glance]
…
api_insecure = False</td></tr>
</table>

	 ※ [default]로는 api_servers = None, api_insecure = False로 되어있음
비고	

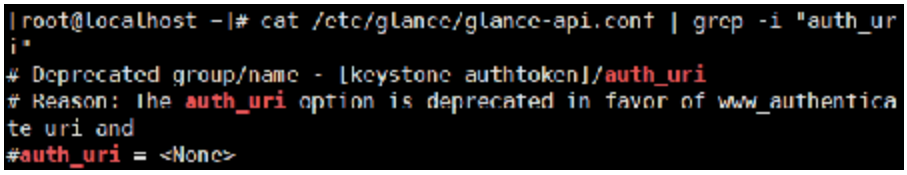
<table>
<tr><td>진단항목</td><td colspan="2">OT-20. 블록 스토리지 서비스 인증을 위한 TLS 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하고, insecure 매개변수가 False로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 시작하지 않고, insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “auth_uri”
 
▪ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 시작하도록 설정
vi /etc/cinder/cinder.conf
[keystone_authtoken]</td></tr>
</table>

	... auth_uri = https://x.x.x.x [keystone_authtoken] auth_uri = https://controller:5000 ▪ /etc/cinder/cinder.conf파일에서 [keystone_authtoken] 섹션의 insecure 값을 false로 설정 # vi /etc/cinder/cinder.conf [keystone_authtoken] ... insecure = false # Verify HTTPS connections. (boolean value) insecure = false ※ [default]로는 auth_uri = None으로 되어있음
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-21. cinder와 nova의 TLS 통신</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 매개변수가 False로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 매개변수가 True로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “nova_api.insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nova_api.insecure 설정값을 False로 설정
vi /etc/cinder/cinder.conf
nova_api.insecure = False
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-22. cinder와 glance의 TLS 통신</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 매개변수가 False로 되어있고, glance_api.servers 매개변수가 https://로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 매개변수가 True로 되어있고, glance_api.servers 매개변수가 https://로 되어있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “glance_api.insecure”
 
▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 설정값 확인
cat /etc/cinder/cinder.conf | grep –i “glance_api_servers”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api.insecure 값을 False로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]
glance_api.insecure = False
 
▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 glance_api_servers 값을 https://로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]
glance_api_servers = https://x.x.x.x</td></tr>
</table>

	# http. (list value) glance_api_servers = https://controller:5000
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-23. 이미지 스토리지 서비스 인증을 위한 TLS 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있고, /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 매개변수가 False로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있지 않고, /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 매개변수가 True로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정값 확인
cat /etc/glance/glance-api.conf | grep –i “auth_uri”
 
■ /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정값 확인
cat /etc/glance/glance-registry.conf | grep –i “insecure”</td></tr>
</table>

```
[root@localhost ~]# cat /etc/glance/glance-api.conf | grep -i "insecur
e"
# This option is ignored if the ``registry_client_insecure`` option
#     * registry_client_insecure
# registry's equivalent of specifying --insecure on the command line
#registry_client_insecure = false
# ``cinder_api_insecure`` must be set to ``True`` to enable the verifi
cation.
#     * cinder_api_insecure
# Allow to perform insecure SSL requests to cinder.
#cinder_api_insecure = false
# this option is set, the ``https_insecure`` option will be ignored an
d
#     * https_insecure
#https_insecure = True
#swift_store_auth_insecure = false
#     * swift_store_auth_insecure
# Deprecated group/name - [glance_store]/vmware_api_insecure
#vmware_insecure = false
# If this option is set, the "vmware_insecure" option will be ignored
#     * vmware_insecure
#insecure = false
#allow_insecure_clients = false
```

조치방법

- /etc/glance/glance-api.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정

  # vi /etc/glance/glance-api.conf

  [keystone_authtoken]

  auth_uri = https://x.x.x.x

```
# will be removed in the S  release.
auth_uri = https://controller:5000
```

- /etc/glance/glance-registry.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 False로 설정

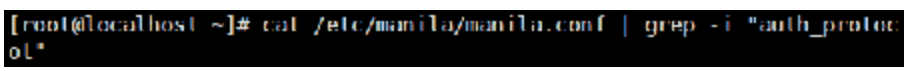
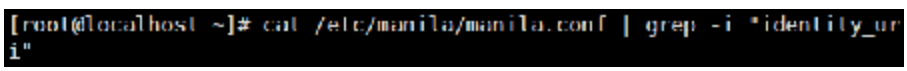
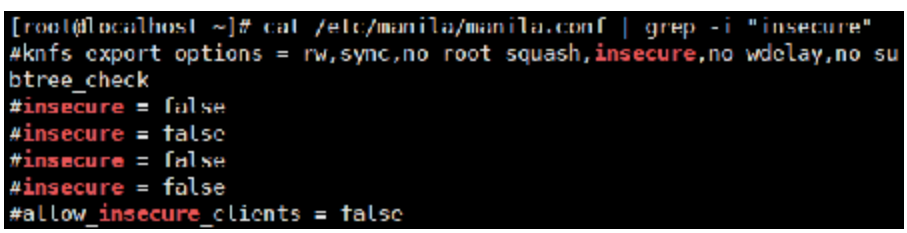
  # vi /etc/glance/glance-registry.conf

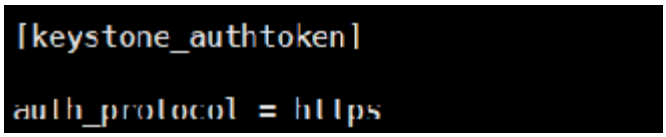
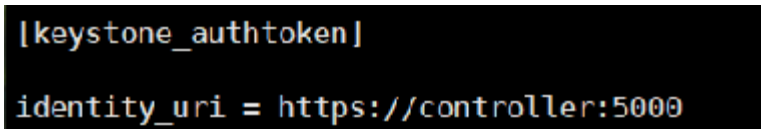
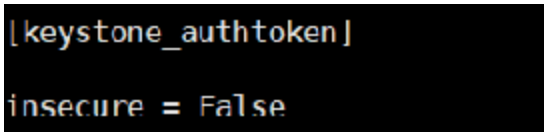
  [keystone_authtoken]

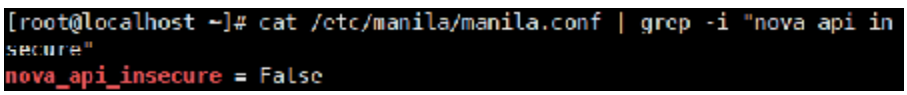
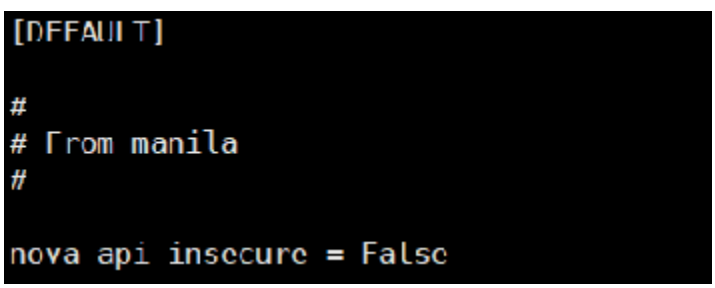
  insecure = False

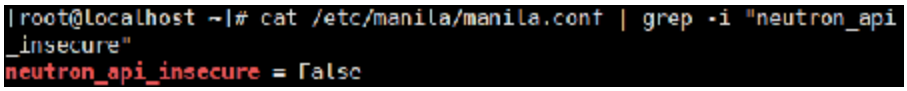
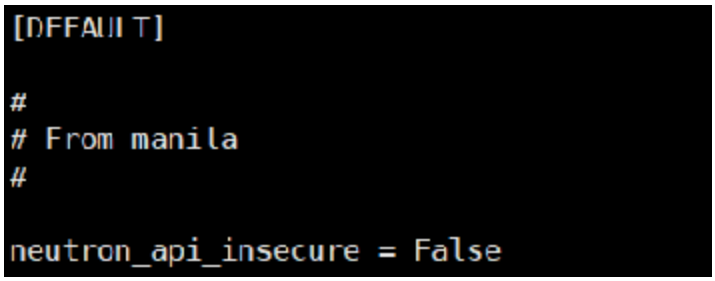
```
# Verify HTTPS connections. (boolean value)
insecure = false
```

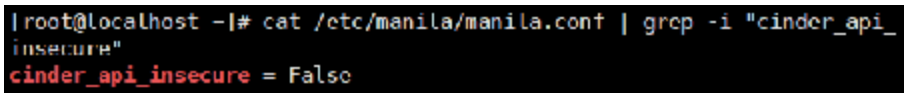
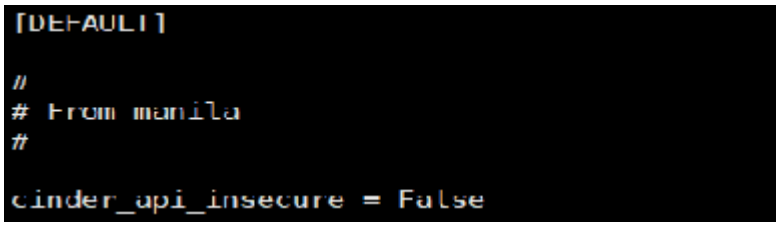
비고

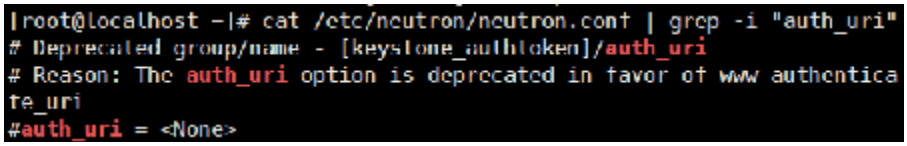
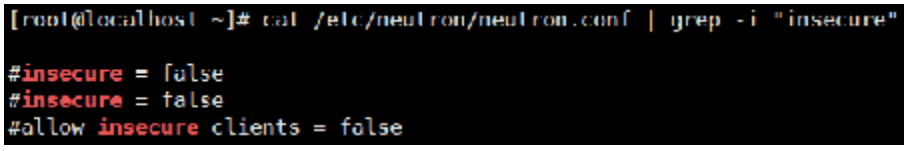
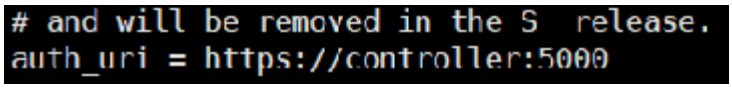
<table>
<tr><td>진단항목</td><td colspan="2">OT-24. 공유 파일 시스템 인증을 위한 TLS 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">1. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 매개변수가 https로 되어 있는 경우
2. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 매개변수가 https://로 되어 있고, insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">1. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 매개변수가 https로 되어 있지 않은 경우
2. /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 매개변수가 https://로 되어 있지 않고, insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 설정값 확인
cat /etc/manila/manila.conf | grep –i “auth_protocol”
 
또는
/etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 설정 값 확인
cat /etc/manila/manila.conf | grep –i “identity_uri”
 
■ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정값 확인
cat /etc/manila/manila.conf | grep –i “insecure”
  </td></tr>
</table>

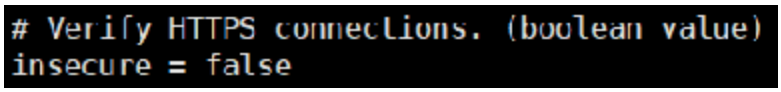
조치방법	▪ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 auth_protocol 값을 https로 설정 # vi /etc/manila/manila.conf [keystone_authtoken] ... auth_protocol = https  또는 /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 identity_uri 값을 https://로 설정 # vi /etc/manila/manila.conf [keystone_authtoken] ... identity_uri = https://x.x.x.x  ▪ /etc/manila/manila.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을 False로 설정 # vi /etc/manila/manila.conf [keystone_authtoken] ... insecure = False 
비고	

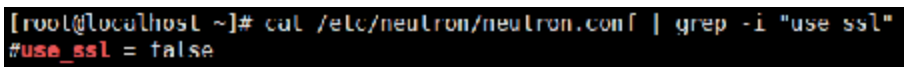
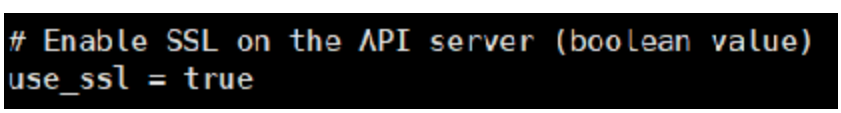
<table>
<tr><td>진단항목</td><td colspan="2">OT-25. TLS를 이용한 공유 파일 시스템과 Compute 통신</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 설정값 확인
cat /etc/manila/manila.conf | grep –i “nova_api_insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 nova_api_insecure 값을 False로 설정
vi /etc/manila/manila.conf
[DEFAULT]
...
nova_api_insecure = False
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-26. TLS를 이용한 공유 파일 시스템과 네트워킹연결</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 설정 값 확인
cat /etc/manila/manila.conf | grep –i “neutron_api_insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 neutron_api_insecure 값을 False로 설정
vi /etc/manila/manila.conf
[DEFAULT]
...
neutron_api_insecure = False
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

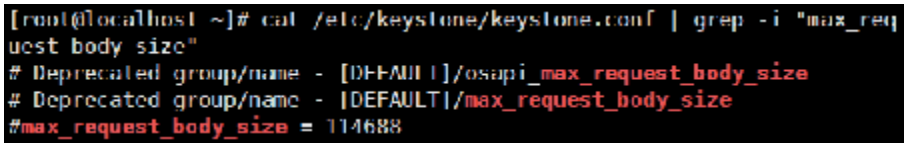
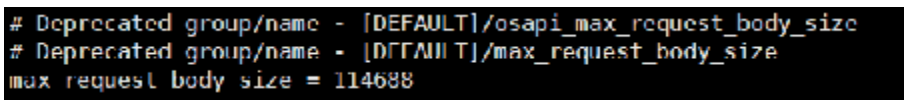
<table>
<tr><td>진단항목</td><td colspan="2">OT-27. TLS를 이용한 공유 파일 시스템과 블록 스토리지 서비스와의 연결</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 설정값 확인
cat /etc/manila/manila.conf | grep –i “cinder_api_insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 cinder_api_insecure 값을 False로 설정
vi /etc/manila/manila.conf
[DEFAULT]
…
cinder_api_insecure = False
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

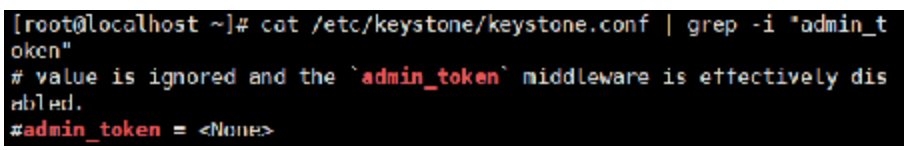
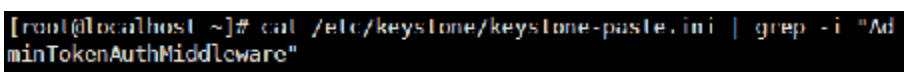
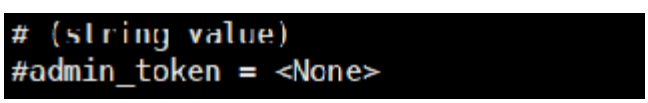
<table>
<tr><td>진단항목</td><td colspan="2">OT-28. 네트워킹 서비스의 인증을 위한 안전한 프로토콜 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있고, insecure 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 매개변수가 https://로 되어 있지 않고, insecure 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 설정 값 확인
cat /etc/neutron/neutron.conf | grep –i “auth_uri”
 
▪ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 insecure 설정 값 확인
cat /etc/neutron/neutron.conf | grep –i “insecure”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 auth_uri 값을 https://로 설정
vi /etc/neutron/neutron.conf
[keystone_authtoken]
...
auth_uri = https://x.x.x.x
 
▪ /etc/neutron/neutron.conf 파일에서 [keystone_authtoken] 섹션의 insecure 값을</td></tr>
</table>

	False로 설정 # vi /etc/neutron/neutron.conf [keystone_authtoken] ... insecure = False 
비고	

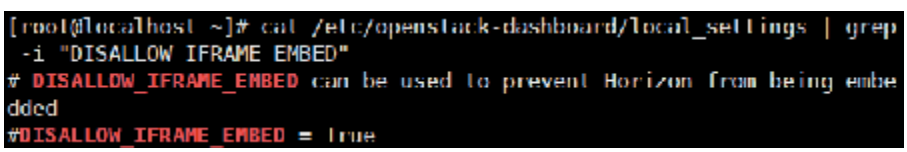
<table>
<tr><td>진단항목</td><td colspan="2">OT-29. Neutron API 서버의 TLS 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택 구성요소는 다양한 프로토콜을 사용하여 서로 통신하며 이러한 통신에는 민감하거나 기밀데이터가 포함되어 있을 수 있다. 공격자는 중요한 정보를 얻기 위해 채널을 도청하려고 시도할 수 있다. 모든 구성요소는 보안 통신 프로토콜을 사용하여 통신하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 설정값 확인
cat /etc/neutron/neutron.conf | grep –i “use_ssl“
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/neutron/neutron.conf 파일에서 [DEFAULT] 섹션의 use_ssl 값을 True로 설정
vi /etc/neutron/neutron.conf
[DEFAULT]
...
use_ssl = True
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 보안 설정

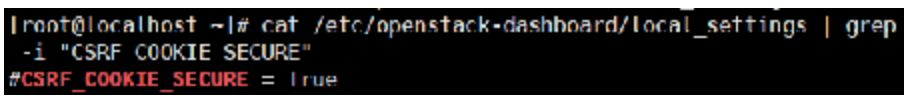
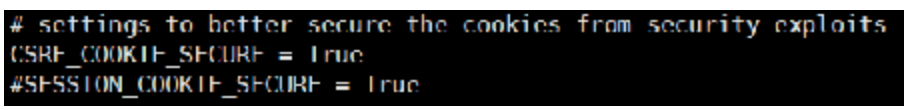
<table>
<tr><td>진단항목</td><td colspan="2">OT-30. Identity 서비스 max_request_body_size 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">max_request_body_size 매개변수는 요청당 최대 본문 크기를 바이트 단위로 정의한다. 최대 크기가 정의되지 않은 경우 공격자는 대량의 대용량 요청을 생성하여 서비스를 중단시키고 결국 DoS(서비스거부) 공격을 유발할 수 있다. 최댓값을 지정하면 악의적인 대용량 요청이 차단되어 구성요소의 지속적인 가용성을 보장할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 max_request_body_size가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/keystone/keystone.conf 파일에서 max_request_body_size 설정값 확인
cat /etc/keystone/keystone.conf | grep –i “max_request_body_size”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/keystone/keystone.conf 파일에서 max_request_body_size 값을 114688 또는 환경에 맞는 적절한 값으로 설정
vi /etc/keystone/keystone.conf
max_request_body_size = 114688
 
※ [default]로는 max_request_body_size = 114688로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

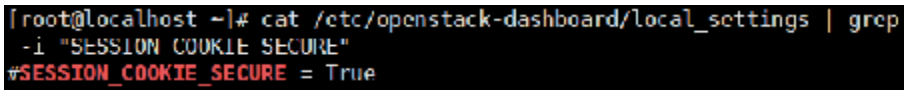
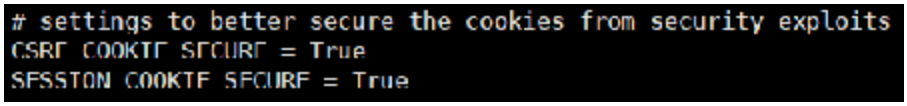
<table>
<tr><td>진단항목</td><td colspan="2">OT-31. admin 토큰 비활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자 토큰은 일반적으로 ID를 부트스트랩하는데 사용된다. 이 토큰은 클라우드 관리자 권한을 얻는데 사용할 수 있는 가장 유용한 아이덴티티 자산이다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 이 비활성화 되어 있고, /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware가 제거되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 이 활성화 되어 있고, /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware가 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 활성화 여부 확인
cat /etc/keystone/keystone.conf | grep –i “admin_token”
 
▪ /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware 존재 여부 확인
cat /etc/keystone/keystone-paste.ini | grep –i “AdminTokenAuthMiddleware”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/keystone/keystone.conf 파일에서 [DEFAULT] 섹션의 admin_token 비활성화
vi /etc/keystone/keystone.conf
[DEFAULT]
admin_token = 7e3a823....
 
▪ /etc/keystone/keystone-paste.ini 파일에서 [filter:admin_token_auth] 섹션의 AdminTokenAuthMiddleware 비활성화
vi /etc/keystone/keystone-paste.ini
[filter:admin_token_auth]
paste.filter_factory = keystone.middleware:AdminTokenAuthMiddleware.factory.</td></tr>
</table>

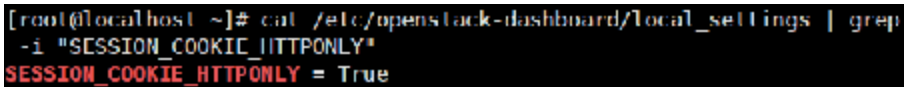
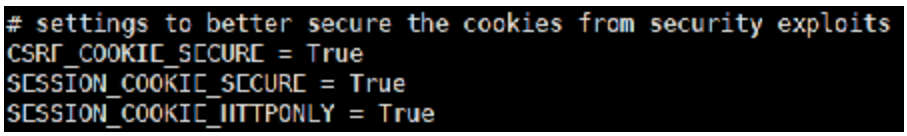
	[filter:admin_token_auth] # paste.filter_factory = keystone.middleware:AdminTokenAuthMiddleware.factory. ※ [default]로는 admin_token = ADMIN으로 되어있음
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-32. Dashboard의 DISALLOW_IFRAME_EMBED 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">DISALLOW_IFRAME_EMBED는 오픈스택 대시보드가 iframe 내에 포함되지 않도록 예방하는데 사용할 수 있다. 기존 브라우저는 여전히 XFS (Cross-Frame Scripting) 취약점에 취약하므로 이 옵션을 사용하면 배포 시 iframe을 사용하지 않는 경우 보안을 강화할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i “DISALLOW_IFRAME_EMBED”
또는
cat /etc/openstack-dashboard/local_settings | grep –i “DISALLOW_IFRAME_EMBED”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISALLOW_IFRAME_EMBED 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
DISALLOW_IFRAME_EMBED = True
또는
vi /etc/openstack-dashboard/local_settings
DISALLOW_IFRAME_EMBED = True
 

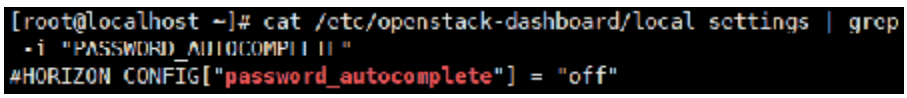
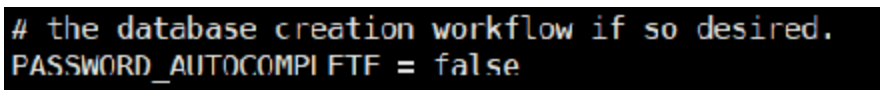
※ [default]로는 DISALLOW_IFRAME_EMBED = True로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

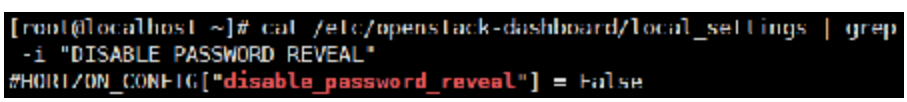
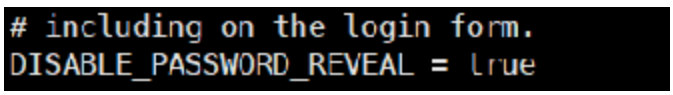
<table>
<tr><td>진단항목</td><td colspan="2">OT-33. Dashboard의 CSRF_COOKIE_SECURE 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">CSRF(사이트간 요청 변조)는 사용자가 현재 인증된 웹 응용프로그램에서 권한이 없는 명령을 실행하도록 하는 공격이다. CSRF 공격이 성공하면 사용자 데이터 및 운영을 손상시킬 수 있다. 사용자에게 관리자 권한이 있으면 전체 웹 응용프로그램이 손상될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i “CSRF_COOKIE_SECURE”
또는
cat /etc/openstack-dashboard/local_settings | grep –i “CSRF_COOKIE_SECURE”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 CSRF_COOKIE_SECURE 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
CSRF_COOKIE_SECURE = True
또는
vi /etc/openstack-dashboard/local_settings
CSRF_COOKIE_SECURE = True
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-34. Dashboard의 SESSION_COOKIE_SECURE 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">"SECURE" 쿠키 속성은 웹 브라우저가 암호화된 HTTPS(SSL / TLS) 연결을 통해서만 쿠키를 보내도록 한다. 이 세션 보호 메커니즘은 MitM (Main-in-the-Middle) 공격을 통한 세션 ID의 공개를 막기 위해 반드시 필요하다. 침입자는 단순히 웹 브라우저 트래픽에서 세션 ID를 캡쳐할 수 없다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i "SESSION_COOKIE_SECURE"
또는
cat /etc/openstack-dashboard/local_settings | grep –i "SESSION_COOKIE_SECURE"
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_SECURE 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
SESSION_COOKIE_SECURE = True
또는
vi /etc/openstack-dashboard/local_settings
SESSION_COOKIE_SECURE = True
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

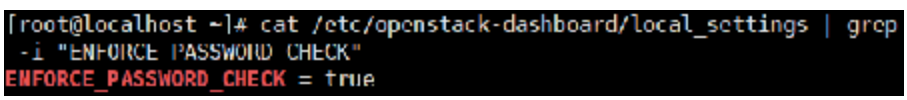
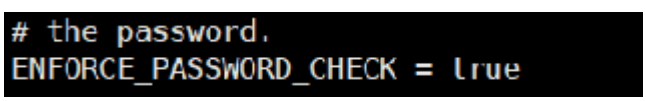
<table>
<tr><td>진단항목</td><td colspan="2">OT-35. Dashboard의 SESSION_COOKIE_HTTPONLY 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">"HTTPONLY" 쿠키 속성은 웹 브라우저가 스크립트(예 : JavaScript 또는 VBscript)가 DOM document.cookie 객체를 통해 쿠키에 액세스하는 것을 허용하지 않도록 한다. 이 세션 ID 보호는 XSS공격을 통한 세션 ID 도용을 방지하기 위해 필수적이다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i "SESSION_COOKIE_HTTPONLY"
또는
cat /etc/openstack-dashboard/local_settings | grep –i "SESSION_COOKIE_HTTPONLY"
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 SESSION_COOKIE_HTTPONLY 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
SESSION_COOKIE_HTTPONLY = True
또는
vi /etc/openstack-dashboard/local_settings
SESSION_COOKIE_HTTPONLY = True
 

※ [default]로는 SESSION_COOKIE_HTTPONLY = True로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

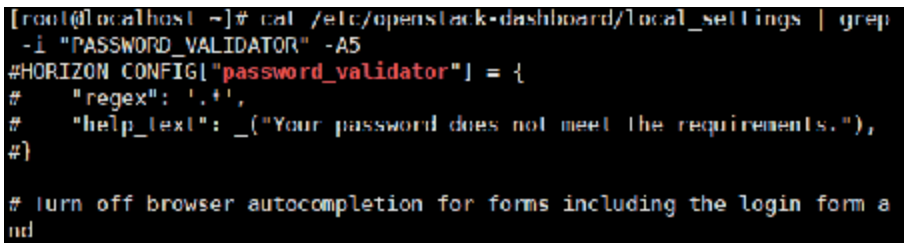
<table>
<tr><td>진단항목</td><td colspan="2">OT-36. Dashboard의 PASSWORD_AUTOCOMPLET 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">응용 프로그램이 사용자에게 편의를 제공하기 위해 사용하는 공통 기능은 암호를 클라이언트 컴퓨터의 브라우저에 로컬로 캐시하고 모든 후속 요청에서 암호를 미리 입력하는 것이다. 이러한 기능은 일반적인 사용자에게 매우 친숙한 것으로 인식될 수 있지만 동시에 클라이언트 시스템에서 동일한 계정을 이용하는 사용자가 계정에 쉽게 접근할 수 있어 계정이 손상될 수 있는 취약점을 유발할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_AUTOCOMPLETE 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_AUTOCOMPLETE 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_AUTOCOMPLETE 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i “PASSWORD_AUTOCOMPLETE”
또는
cat /etc/openstack-dashboard/local_settings | grep –i “PASSWORD_AUTOCOMPLETE”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_AUTOCOMPLETE 값을 False로 설정
vi /etc/openstack-dashboard/local_settings.py
PASSWORD_AUTOCOMPLETE = false
또는
vi /etc/openstack-dashboard/local_settings
PASSWORD_AUTOCOMPLETE = false
 
※ [default]로는 PASSWORD_AUTOCOMPLETE = off로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

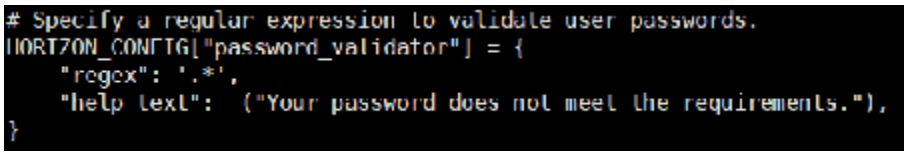
<table>
<tr><td>진단항목</td><td colspan="2">OT-37. Dashboard의 DISABLE_PASSWORD_REVEAL 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">클라이언트 시스템에서 동일한 계정을 이용하는 사용자가 계정에 쉽게 접근할 수 있어 계정이 손상될 수 있는 취약점을 유발할 수 있으므로 패스워드 필드를 노출하지 않아야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i “DISABLE_PASSWORD_REVEAL”
또는
cat /etc/openstack-dashboard/local_settings | grep –i “DISABLE_PASSWORD_REVEAL”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 DISABLE_PASSWORD_REVEAL 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
DISABLE_PASSWORD_REVEAL = true
또는
vi /etc/openstack-dashboard/local_settings
DISABLE_PASSWORD_REVEAL = true
 

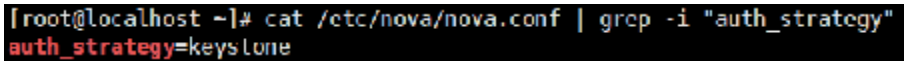
※ [default]로는 DISABLE_PASSWORD_REVEAL = false로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-38. Dashboard의 ENFORCE_PASSWORD_CHECK 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">ENFORCE_PASSWORD_CHECK를 True로 설정하면 실제로 암호를 변경하려는 관리자로 로그인했는지 검증하기 위해 패스워드 변경 폼에 'Admin Password' 필드가 화면에 표시된다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 매개변수가 True로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 매개변수가 False로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 설정 값 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i "ENFORCE_PASSWORD_CHECK"
또는
cat /etc/openstack-dashboard/local_settings | grep –i "ENFORCE_PASSWORD_CHECK"
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 ENFORCE_PASSWORD_CHECK 값을 True로 설정
vi /etc/openstack-dashboard/local_settings.py
ENFORCE_PASSWORD_CHECK = true
또는
vi /etc/openstack-dashboard/local_settings
ENFORCE_PASSWORD_CHECK = true
 

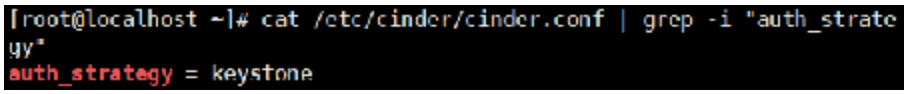
※ [default]로는 ENFORCE_PASSWORD_CHECK = false로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-39. Dashboard의 PASSWORD_VALIDATOR 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">사용자 패스워드 복잡성을 검증하기 위해 정규 표현식을 허용해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR 설정 확인
cat /etc/openstack-dashboard/local_settings.py | grep –i “PASSWORD_VALIDATOR” -A5
또는
cat /etc/openstack-dashboard/local_settings | grep –i “PASSWORD_VALIDATOR” -A5
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/openstack-dashboard/local_settings.py 또는 /etc/openstack-dashboard/local_settings 파일에서 PASSWORD_VALIDATOR 설정
vi /etc/openstack-dashboard/local_settings.py
HORIZON_CONFIG[“password_validator“] = {
“regex”: ‘.*’,
“help_text”: _(“Your password does not meet the requirements.”),
또는
vi /etc/openstack-dashboard/local_settings
HORIZON_CONFIG[“password_validator“] = {
“regex”: ‘.*’,
“help_text”: _(“Your password does not meet the requirements.”),</td></tr>
</table>

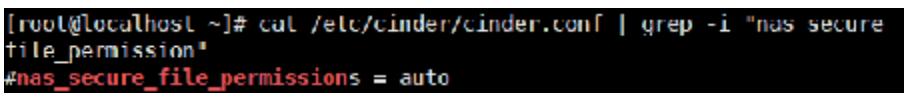
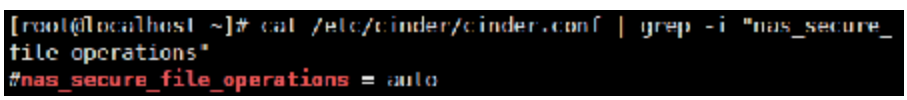
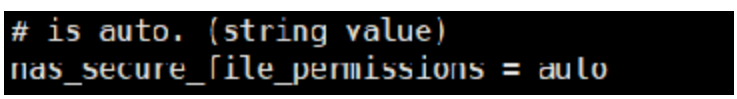
	 ※ [default]로는 password_validator = {'regex': '.*', 'help_text': _("Password is not accepted")}로 되어있음
비고	

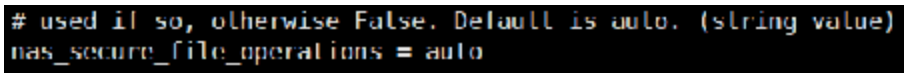
<table>
<tr><td>진단항목</td><td colspan="2">OT-40. Compute의 인증을 위한 keystone 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택은 noauth, keystone와 같은 다양한 인증 전략을 지원한다. noauth 전략을 사용하면 사용자는 인증없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth 또는 noauth2로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인
cat /etc/nova/nova.conf | grep –i “auth_strategy”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/nova/nova.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정
vi /etc/nova/nova.conf
[DEFAULT]
auth_strategy = keystone

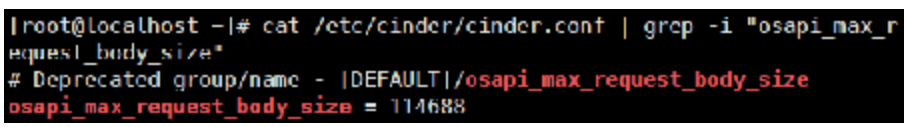
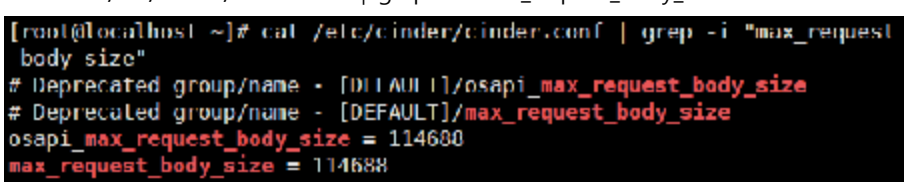
※ [default]로는 auth_strategy = keystone으로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

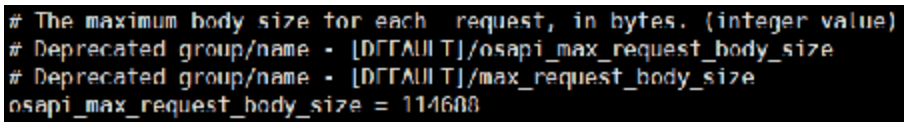
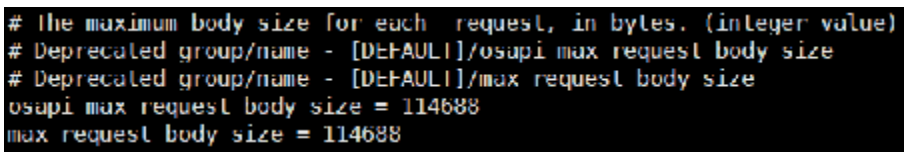
<table>
<tr><td>진단항목</td><td colspan="2">OT-41. 블록 스토리지 서비스의 인증을 위한 keystone 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택은 noauth, keystone와 같은 다양한 인증 전략을 지원한다. noauth 전략을 사용하면 사용자는 인증 없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “auth_strategy”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 값을 keystone으로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]
auth_strategy = keystone

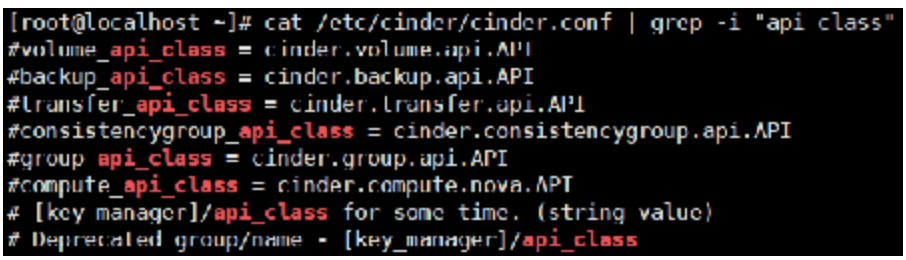
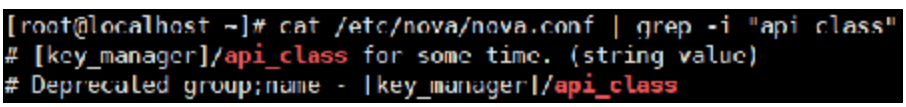
※ [default]로는 auth_strategy = noauth으로 되어있음</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

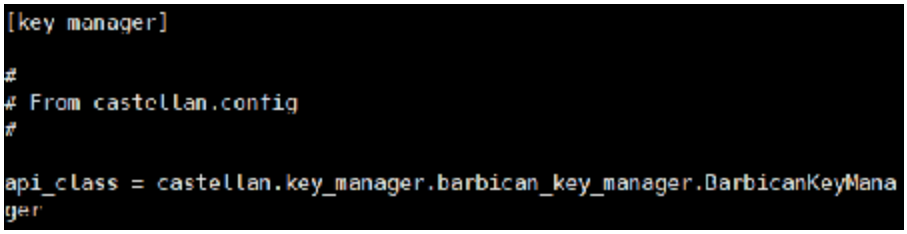
<table>
<tr><td>진단항목</td><td colspan="2">OT-42. 안전한 환경에서의 NAS 운영</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Cinder는 기존 블록 저장소 드라이버와 다르게 작동하는 NFS 드라이버를 지원한다. NFS 드라이버는 실제로 인스턴스가 블록 수준에서 저장 장치에 액세스하는 것을 허용하지 않는다. 대신 NFS 공유에 파일이 만들어지고 블록 장치를 에뮬레이트하는 인스턴스에 매핑된다. Cinder는 Cinder 볼륨이 생성될 때 파일 사용 권한을 제어하여 이러한 파일에 대한 보안 구성을 지원한다. 또한 Cinder 설정은 파일 작업이 루트 사용자로 실행되는지 또는 현재 오픈스택 프로세스 사용자로 실행되는지 여부를 제어할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 매개변수가 auto로 되어 있고, nas_secure_file_operations 매개변수가 auto로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 매개변수가 false로 되어 있고, nas_secure_file_operations 매개변수가 false로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “nas_secure_file_permission”
 
■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_operations 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “nas_secure_file_operations”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_permission 값을 auto로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]
nas_secure_file_permission = auto
 
■ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 nas_secure_file_operations 값을 auto로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]</td></tr>
</table>

	nas_secure_file_operations = auto  ※ [default]로는 nas_secure_file_operations = auto로 되어있음
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-43. 블록 스토리지 서비스에서 요청 본문 최대 크기 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">요청당 최대 본문 크기가 정의되지 않은 경우 공격자는 큰 사이즈의 임의 OSAPI 요청을 작성하여 서비스가 중단되는 Dos(Denial of Service) 공격이 발생할 수 있다. 최대값을 지정하면 악의적인 대량 요청이 차단되어 서비스의 지속적인 가용성을 보장할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본값(114688) 또는 적절한 값으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있지 않거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본값(114688) 또는 적절한 값으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “osapi_max_request_body_size”
 
▪ /etc/cinder/cinder.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “max_request_body_size”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 값을 114866 또는 환경에 맞는 적절한 값으로 설정
vi /etc/cinder/cinder.conf
[DEFAULT]
...
osapi_max_request_body_size = 114688</td></tr>
</table>

	 ■ /etc/cinder/cinder.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 값을 114866 또는 환경에 맞는 적절한 값으로 설정 # vi /etc/cinder/cinder.conf [oslo_middleware] ... max_request_body_size = 114688  ※ [default]로는 osapi_max_request_body_size = 114688, max_request_body_size = 114688 으로 되어있음
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-44. 블록 스토리지 볼륨 암호화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">암호화되지 않은 볼륨 데이터는 공격자가 여러 VM에 대한 데이터를 읽을 수 있으며 특히 볼륨 호스팅 플랫폼이 공격자에게 주요대상이 될 위험이 존재한다. 또한 물리적 저장 매체를 다른 컴퓨터에서 도난당하거나 재설치하거나 액세스할 수 있다. 볼륨 데이터를 암호화하면 이러한 위험이 완화되고 볼륨 호스팅 플랫폼에 심층적인 방어가 가능하다. 블록저장소(cinder)는 볼륨 데이터를 디스크에 쓰기 전에 암호화할 수 있으며 볼륨 암호화 기능을 사용하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">1. /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있는 경우
2. /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">1. /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있지 않은 경우
2. /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 매개변수가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정 값 확인
cat /etc/cinder/cinder.conf | grep –i “api_class”
 
▪ /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정 값 확인
cat /etc/nova/nova.conf | grep –i “api_class”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/cinder/cinder.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정
vi /etc/cinder/cinder.conf
[KEY_MANAGER]
…
api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyManager</td></tr>
</table>



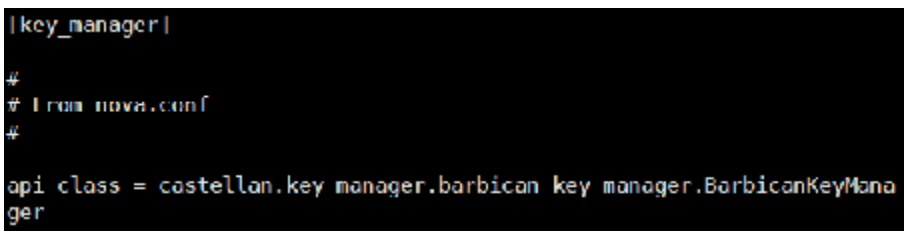
- /etc/nova/nova.conf 파일에서 [KEY_MANAGER] 섹션의 api_class 설정

  # vi /etc/nova/nova.conf

  [KEY_MANAGER]

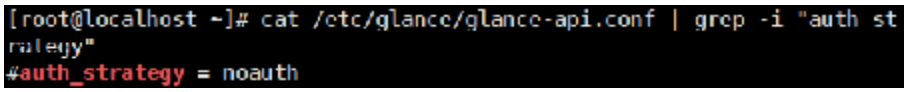
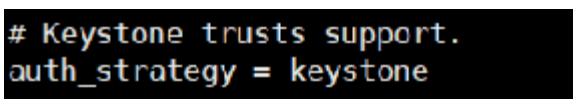
  ...

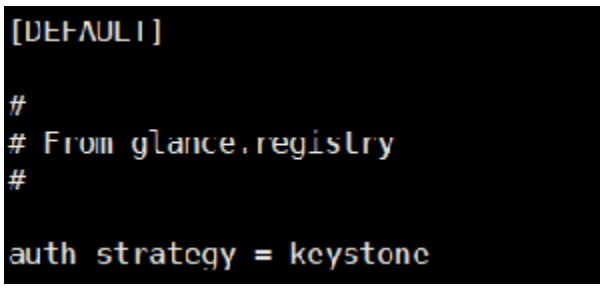
  api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyManager

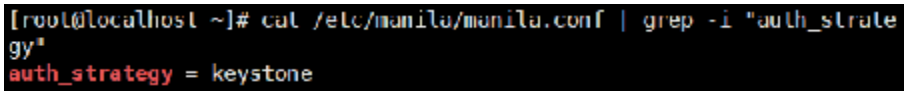
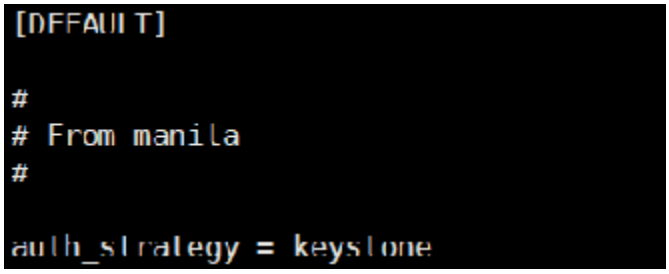


※ [default]로는 api_class = cinder.keymgr.conf_key_mgr.ConfKeyManager로 되어있음

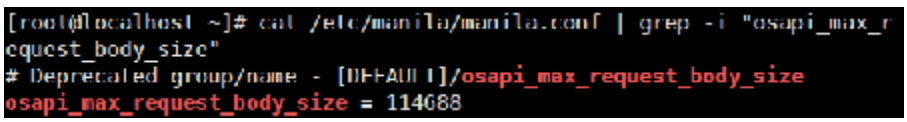
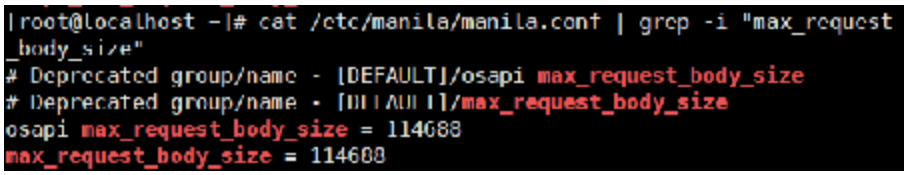
비고	

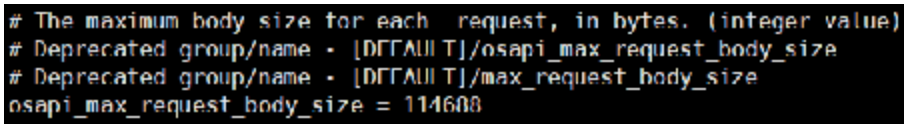
<table>
<tr><td>진단항목</td><td colspan="2">OT-45. 이미지 스토리지 서비스 인증을 위한 keystone 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택은 noauth, keystone과 같은 다양한 인증 전략을 지원한다. noauth 전략을 사용하면 사용자는 인증없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어 있고, /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어 있거나, /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인
cat /etc/glance/glance-api.conf | grep –i “auth_strategy”
 
▪ /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인
cat /etc/glance/glance-registry.conf | grep –i “auth_strategy”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/glance/glance-api.conf 파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정
vi /etc/glance/glance-api.conf
[DEFAULT]
auth_strategy = keystone
 
▪ /etc/glance/glance-registry.conf 파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정
vi /etc/glance/glance-registry.conf</td></tr>
</table>

	[DEFAULT] auth_strategy = keystone  ※ [default]로는 auth_strategy = keystone
비고	

<table>
<tr><td>진단항목</td><td colspan="2">OT-46. 공유파일 시스템 인증을 위한 오픈스택 Identity 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">오픈스택은 noauth, keystone과 같은 다양한 인증 전략을 지원한다. noauth 전략을 사용하면 사용자는 인증 없이 OpenStack 서비스와 상호 작용할 수 있다. 이것은 공격자가 오픈스택 구성요소에 비인가 접근을 할 수 있기 때문에 잠재적인 위험이 될 수 있다. 모든 서비스는 서비스 계정을 사용하여 keystone으로 인증해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 keystone으로 되어있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 매개변수가 noauth로 되어있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 auth_strategy 설정 값 확인
cat /etc/manila/manila.conf | grep –i “auth_strategy”
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/manila/manila.conf파일에서 [DEFAULT] 섹션의 auth_strategy를 keystone으로 설정
vi /etc/manila/manila.conf
[DEFAULT]
auth_strategy = keystone
 

※ [default]로는 auth_strategy = keystone</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">OT-47. 공유파일 시스템에서 요청 본문 최대 사이즈 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">요청 당 최대 본문 크기가 정의되지 않은 경우 공격자는 큰 사이즈의 임의 OSAPI요청을 작성하여 서비스가 중단되는 DoS(Denial of Service) 공격이 발생할 수 있다. 최댓값을 지정하면 악의적인 대량 요청이 차단되어 서비스의 지속적인 가용성을 보장할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본값(114688) 또는 적절한 값으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">/etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size가 기본값(114688) 또는 적절한 값으로 설정되어 있지 않거나, [oslo_middleware] 섹션의 max_request_body_size 매개변수가 기본값(114688) 또는 적절한 값으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 설정 값 확인
cat /etc/manila/manila.conf | grep –i “osapi_max_request_body_size”
 
▪ /etc/manila/manila.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 설정 값 확인
cat /etc/manila/manila.conf | grep –i “max_request_body_size”
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ /etc/manila/manila.conf 파일에서 [DEFAULT] 섹션의 osapi_max_request_body_size 값을 114866 또는 환경에 맞는 적절한 값으로 설정
vi /etc/manila/manila.conf
[DEFAULT]
...
osapi_max_request_body_size = 114688</td></tr>
</table>



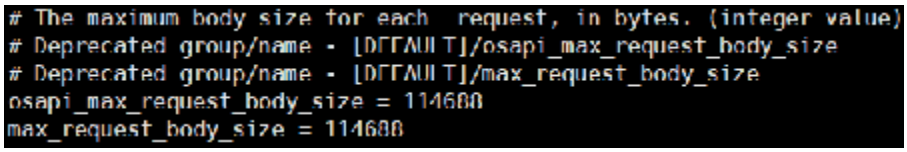
- /etc/manila/manila.conf 파일에서 [oslo_middleware] 섹션의 max_request_body_size 값을 114688 또는 환경에 맞는 적절한 값으로 설정

  # vi /etc/manila/manila.conf

  [oslo_middleware]

  ...

  max_request_body_size = 114688



※ [default]로는 osapi_max_request_body_size = 114688, max_request_body_size = 114688 으로 되어있음

비고	

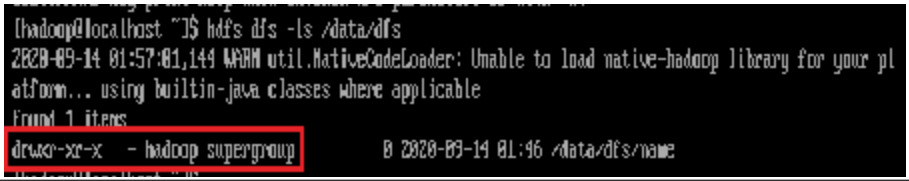
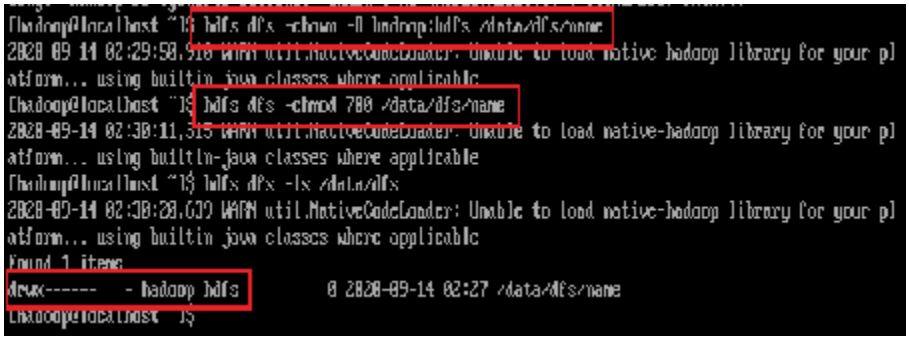
2.18. Hadoop

파일 및 디렉토리 권한(1개 항목), 파일 및 서비스 관리(1개 항목), 보안 설정(5개 항목), 패치 및 로그 관리(2개 항목) 총 4개 영역에서 9개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 파일 및 디렉토리 권한	HA-01	로컬 파일 시스템/HDFS 디렉토리 소유자 및 권한 설정	상
나. 파일 및 서비스 관리	HA-02	커버로스 인증 시 클러스터의 모든 시스템에서 YARN User 키 테이블/맵리듀스 User 키테이블 파일 권한 설정	중
다. 보안 설정	HA-03	Hadoop Security 활성화	상
	HA-04	WebHDFS 비활성화	중
	HA-05	Hadoop ACL 설정	상
	HA-06	RPC 암호화	상
	HA-07	데이터 전송 암호화	상
라. 패치 및 로그 관리	HA-08	최신 패치 및 버전 관리	상
	HA-09	감사로그 설정	상

[표 18] Hadoop 진단 체크리스트

가. 파일 및 디렉토리 권한

<table>
<tr><td>진단항목</td><td colspan="2">HA-01. 로컬 파일 시스템/HDFS 디렉토리 소유자 및 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">파일에 과도한 사용자 권한이 존재할 경우, 비인가 된 사용자가 해당 파일에 접근하여 HDFS 등 하둡 관련 정보를 수집하여 2차적인 공격에 사용될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로컬 파일 시스템/HDFS 소유자와 권한이 조치방법과 같이 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로컬 파일 시스템/HDFS 소유자가 권한이 조치방법보다 과도하게 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 로컬 파일 시스템/HDFS 디렉토리 권한 확인
1) hdfs dfs –ls [PATH]
또는
2) # ./bin/haddop fs –ls [파일명]
  </td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 로컬 파일 시스템(example)
// dfs.namenode.name.dir = hdfs:hadoop (700)
chown –R hdfs:hadoop /home/hadoop/data/dfs/name
chmod 700 /home/hadoop/data/dfs/name
 
// dfs.namenode.data.dir = hdfs:hadoop (700)
chown –R hdfs:hadoop /home/hadoop/data/dfs/data
chmod 700 /home/hadoop/data/dfs/data

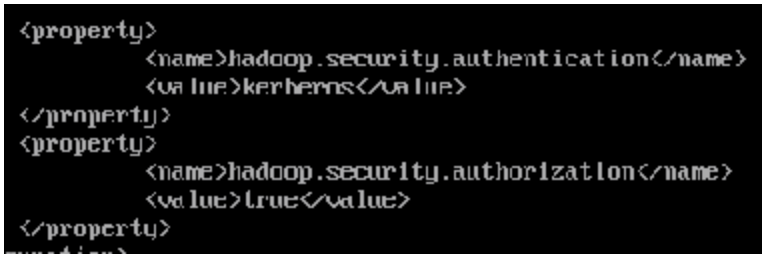
// dfs.journalnode.edits.dir = hdfs:hadoop (700)
chown –R hdfs:hadoop /home/hadoop/data/dfs/journalnode</td></tr>
</table>

	# chmod 700 /home/hadoop/data/dfs/journalnode // $HADOOP_LOG_DIR = hdfs:hadoop (775) # chown –R hdfs:hadoop /home/hadoop/logs # chmod 775 /home/hadoop/logs // yarn.nodemanager.local-dirs = yarn:hadoop (755) # chown -R yarn:hadoop /home/hadoop/data/yarn/nm-local-dir # chmod 755 /home/hadoop/data/yarn/nm-local-dir ▪ HDFS 디렉토리 / = hdfs:hadoop (775) /home/hadoop/bin/hdfs dfs –chown hdfs:hadoop / /home/hadoop/bin/hdfs dfs –chmod 755 / /user = hdfs:hadoop (755) /home/hadoop/bin/hdfs dfs –chown hdfs:hadoop /user /home/hadoop/bin/hdfs dfs –chmod 755 /user
비고	

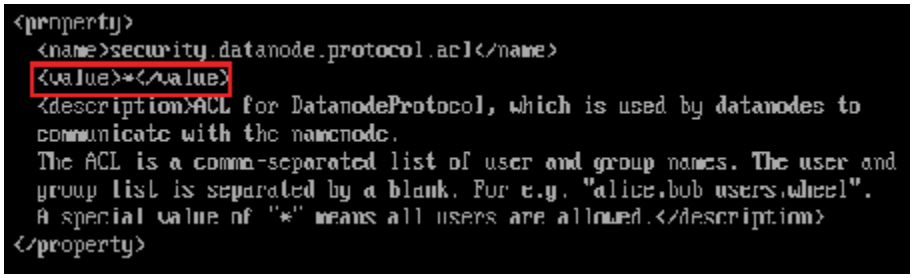
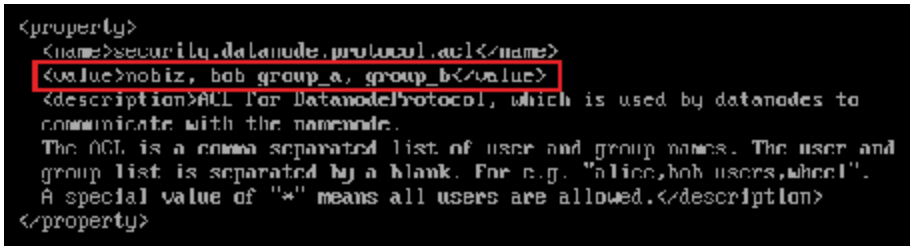
나. 권한 관리

<table>
<tr><td>진단항목</td><td colspan="2">HA-02. 커버로스 인증 시 클러스터의 모든 시스템에서 YARN User 키 테이블/맵리듀스 User 키테이블 파일 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">하둡 서비스는 티켓을 얻기 위해 암호화된 로그인 사용이 불가능하다. 그러므로 사용자의 인증 자격 증명을 위하여 각 서비스 및 하위 서비스에 Kerberos와 관련 있는 사용자 키테이블 파일을 통해 인증된 사용자만 접근이 가능하도록 설정하여야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">클러스터의 모든 시스템에 YARN User 키 테이블/맵리듀스 유저 키테이블의 권한이 400이하이고 소유자가 해당 keytab의 소유자일 경우</td></tr>
<tr><td>취약</td><td colspan="3">클러스터의 모든 시스템에 YARN User 키 테이블/맵리듀스 유저 키테이블의 권한이 400초과이고 소유자가 root일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 수동점검을 통해 직접 hadoop 안에 커버로스 관련 키 테이블이 존재하는지 확인
ls –al [hadoop config 디렉토리] | grep *.keytab</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ root 외의 소유자로 지정, 권한은 400이하로 설정
ex)
chown hdfs:hadoop hdfs.keytab
chmod 400 hdfs.keytab
chown yarn:hadoop yarn.keytab
chmod 400 yarn.keytab
chown mapred:hadoop mapred.keytab
chmod 400 mapred.keytab</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

다. 보안 설정

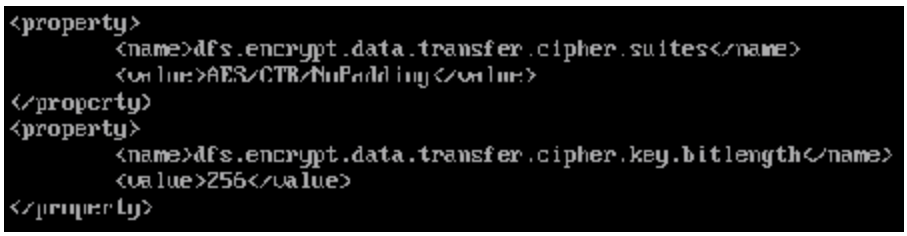
<table>
<tr><td>진단항목</td><td colspan="2">HA-03. Hadoop Security 활성화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">하둡은 보안을 강화하기 위해 커버로스 프로토콜을 사용할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">커버로스가 enable(true) 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">커버로스가 disable(false) 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ core-site.xml에 kerberos 설정 확인
cat core-site.xml</td></tr>
<tr><td>조치방법</td><td colspan="4">■ core-site.xml에 kerberos 설정
vi core-site.xml
- 아래와 같은 설정 사항 추가
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">HA-04. WebHDFS 비활성화</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">불필요한 서비스가 구동중일 경우 해당 포트가 활성화되어 공격루트로 이용될 위험이 존재한다,</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">불필요한 WebHDFS가 구동 중이지 않을 경우</td></tr>
<tr><td>취약</td><td colspan="3">불필요한 WebHDFS가 구동 중일 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ hdfs-site.xml에서 확인
cat hdfs-site.xml</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ WebHDFS를 사용하지 않는 경우 hdfs-site.xml에서 설정
vi hdfs-site.xml
  </td></tr>
<tr><td>비고</td><td colspan="4">▪ hdfs-site.xml에 설정이 존재하지 않을 경우
- default = true
- default port = 50070(namenode), 50075(datanode)</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">HA-05. 하둡 ACL 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인가되지 않은 사용자가 접근 가능하도록 설정하였을 경우 침해사고가 일어날 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인가된 계정 및 그룹만 접근 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">모두 접근이 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ hadoop-policy.xml에서 확인 가능(아래와 같이 *로 설정되어 있는 경우, 모두 접근이 가능하므로 취약함)
cat hadoop-policy.xml
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ hadoop-policy.xml에서 설정
vi hadoop-policy.xml
<value> 인가된 계정 및 그룹명 </value> 으로 수정
예시
 

※ 아무런 설정이 존재하지 않는 경우, default로 모두 접근 가능</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">HA-06. RPC 암호화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">하둡 클라이언트는 하둡 네임노드와 통신하기 위해 하둡 RPC를 이용한다. 하둡 RPC 메커니즘은 SASL 보안을 지원한다. SASL 암호화는 하둡 클라이언트와 네임노드 간의 통신을 보호하고 암호화한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">rpc 암호화 설정을 적용한 경우</td></tr>
<tr><td>취약</td><td colspan="3">rpc 암호화 설정을 적용하지 않은 경우</td></tr>
<tr><td>점검방법</td><td colspan="4">■ core-site.xml 파일에서 rpc 암호화 설정 적용 여부 확인
cat core-site.xml
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">■ core-site.xml 파일에서 rpc 암호화 설정
- 아래와 같은 설정 사항 추가
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">HA-07. 데이터 전송 암호화</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">네임노드는 클라이언트에게 첫 블록을 읽고 쓰기 위한 데이터노드의 주소를 알려준다. 이 때 실제 데이터의 전송에 이용되는 프로토콜이 DTP이다. 이 값이 네임노드와 모든 데이터노드에 설정되어 있으면 데이터가 암호화되어서 전송되며, 암호화 알고리즘도 설정할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">데이터 전송 암호화 설정이 적용되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">데이터 전송 암호화 설정이 적용되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ hdfs-site.xml 파일에서 데이터 전송 암호화 활성화 확인
▪ hdfs-site.xml 파일에서 암호화 알고리즘 확인
cat hdfs-site.xml</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ hdfs-site.xml 파일에서 암호화 설정 활성화
- 아래와 같은 설정 사항 추가
 
▪ hdfs-site.xml 파일에서 암호화 알고리즘 설정
- 아래와 같은 설정 사항 추가
 
※ 하둡 2.6 이전
<property>
<name>dfs.encrypt.data.transfer.algorithm</name>
<value>3des</value>
</property></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

라. 패치 및 백업 관리

<table>
<tr><td>진단항목</td><td colspan="2">HA-08. 최신 패치 및 버전 관리</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 패치 및 보안 업데이트를 실시하지 않을 경우, 버전에 따른 잘 알려진 취약점이 존재하며, 해당 취약점을 통해 시스템이 장악될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 패치 및 보안 업데이트를 적용한 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 패치 및 보안 업데이트를 적용하지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Hadoop 버전 확인
hadoop version
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 수동조치
최신 패치 및 보안 업데이트가 발표되었을 경우, 회의 및 테스트 베드를 통한 충분한 테스트 후 적용</td></tr>
<tr><td>비고</td><td colspan="4">시스템 업데이트는 영향도 산정을 한 이후에 진행되어야 함</td></tr>
</table>

진단항목	HA-09. 감사로그 설정		취약도	상
항목설명	지속적으로 User활동 및 서비스 활동 감사를 실시하여 보안사고가 발생할 경우 책임 추적 및 원인 분석을 빠르고 효과적으로 수행할 수 있도록 하여야 한다.			
진단기준	양호	운영되고 있는 하둡의 구성요소들에 대한 감사가 설정되어 로그를 기록하고 있는 경우		
	취약	운영되고 있는 하둡의 구성요소들에 대한 감사가 설정이 일부만 되어 있거나 되어있지 않은 경우		
진단방법	■ 인터뷰를 통해 해당 구성요소들의 감사로그 설정 확인(log4j.properties 파일 확인) # cat log4j.properties			
조치방법	■ 해당 구성요소들의 감사로그 방법에 따라 감사 로그 설정 1) HDFS 감사 로그 • user 활동을 위한 hdfs-audit.log와 서비스활동을 위한 SecurityAuth-hdfs.audit, 2가지 로그가 존재 • log4j 설정에서 아래와 같은 설정 확인 log4j.logger.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit log4j.category.SecurityLogger 2) MapReduce 감사로그 • user 활동을 위한 mapred-audit,log와 서비스활동을 위한 SecurityAuth-mapred.audit, 2가지 로그가 존재 • log4j 설정에서 아래와 같은 설정 확인 log4j.logger.org.apache.hadoop.mapred.AuditLogger log4j.category.SecurityLogger 3) YARN 감사로그 • 사용자 감사 로그 이벤트는 별도의 파일에 있지 않고 데몬 로그 파일과 혼합되어 있음 • log4j 설정에서 아래와 같은 설정 확인 log4j.category.SecurityLogger 4) Hive 감사 로그 • 서비스 로깅을 위해 Hive Metastore 사용 • 그 외에 다른 감사를 통해 Hive를 감사하려면 다른감사 설정 확인 org.apache.hadoop.hive.metastore.HiveMetaStore.audit 5) HBase 감사 로그 • 감사 이벤트가 HBase node로 확산될 수 있어 감사설정에 문제가 발생할 가능성이 있음			

	• log4j 설정에서 아래와 같은 설정 확인 log4j.category.SecurityLogger 6) KDC 감사로깅 • kdc.conf 파일 [logging] kdc = FILE:/var/log/kdc-audit.log admin_server = FILE:/var/log/kadmin.log
비고	

2.19. Elasticsearch

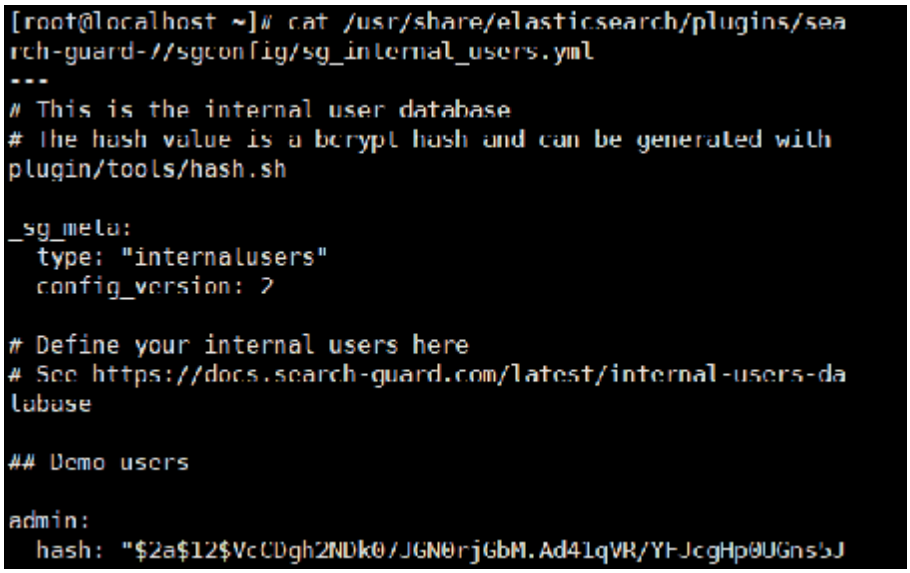
보안 설정(4개 항목), 디렉터리 및 파일권한 관리(4개 항목), 패치 및 로그 관리(2개 항목) 총 3개 영역에서 10개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 보안 설정	EL-01	Elasticsearch 인증 설정	중
	EL-02	디폴트 계정 및 패스워드 변경	상
	EL-03	불필요한 계정 제거	상
	EL-04	IP 접근 제한 설정	상
나. 디렉터리 및 파일권한 관리	EL-05	설치 디렉터리 접근 권한 설정	중
	EL-06	플러그인 디렉터리 접근 권한 설정	중
	EL-07	설정파일 접근권한 설정	상
	EL-08	Search-Guard 스크립트 접근권한 설정	상
다. 패치 및 로그 관리	EL-09	로그 활성화	하
	EL-10	최신 패치 적용	상

[표 19] Elasticsearch 진단 체크리스트

가. 보안 설정

<table>
<tr><td>진단항목</td><td colspan="2">EL-01. Elasticsearch 인증 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Elasticsearch 아이디 및 패스워드 설정이 되어 있지 않은 경우, 서버에 접근하는 사용자 모두 Elasticsearch에 접근이 가능하게 되어, Elasticsearch 장악 및 정보 유출의 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인증 아이디 및 패스워드가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">인증 아이디 및 패스워드가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
■ 설정 파일을 통해 확인
- Elasticsearch5.0 이상 X-Pack 플러그인
cat [Elasticsearch 설정 디렉터리]/x-pack/users


- Elasticsearch5.0 이상 Search-Guard 플러그인
cat [Elasticsearch 설치 디렉터리]/search-guard-버전/sgconfig/sg_internal_users.yml


■ CURL 명령어를 통해 확인
- Elasticsearch 5.0 이상
curl localhost:9200
</td></tr>
</table>

<table>
<tr><td></td><td>

```
[root@localhost ~]# curl localhost:9200
{
  "name" : "localhost.localdomain",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "wchWDXrNRyGfeiMwmqq-wA",
  "version" : {
    "number" : "7.9.1",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "083627f112ba94dffc1232e8b42b73492789ef91
",
    "build_date" : "2020-09-01T21:22:21.964974Z",
    "build_snapshot" : false,
    "lucene_version" : "8.6.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

</td></tr>
<tr><td>조치방법</td><td>

- Elasticsearch5.0 이상

[Elasticsearch 설치 디렉터리]/bin/x-pack/users useradd '계정명' -r '계정권한'

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users useradd es_admin -r superuser
Enter new password:
Retype new password:
```

■ Search-Guard 플러그인을 통해 설정

- Elasticsearch5.0 이상

1) # cd [Elasticsearch 설치 디렉터리]/bin/search-guard-*/tools를 통해 디렉터리 이동

```
[root@localhost ~]# cd /usr/share/elasticsearch/plugins/sear
ch-guard-//tools/
```

2) # ./hash.sh 명령어를 통해 패스워드 해시값 생성

```
[root@localhost tools]# sh ./hash.sh
WARNING: JAVA_HOME not set, will use /usr/bin/java
[Password:]
$2y$12$Jq2KVRYpTTaTlujl.1rQeeS0UTU7n67g5e/i13ul7D9xWfg1kuQv0
```

3) 출력된 해시 값과 계정 명을 [Elasticsearch 설치 디렉터리]/plugin/search-guard-*/sgconfig/sg_internal_users.yml 설정파일에 기입

```
test:
  hash: "$2y$12$Jq2KVRYpTTaTlujl.1rQeeS0UTU7n67g5e/i13ul7D9x
Wfg1kuQv0"
```

4) [Elasticsearch 설치 디렉터리]/bin/search-guard-*/sgconfig/sg_roles_mapping.yml 설정파일에서 role과 계정 매핑

</td></tr>
</table>

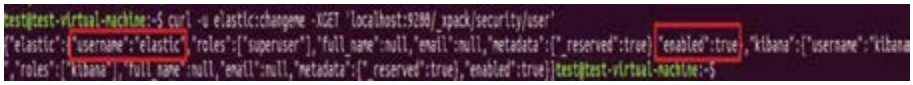
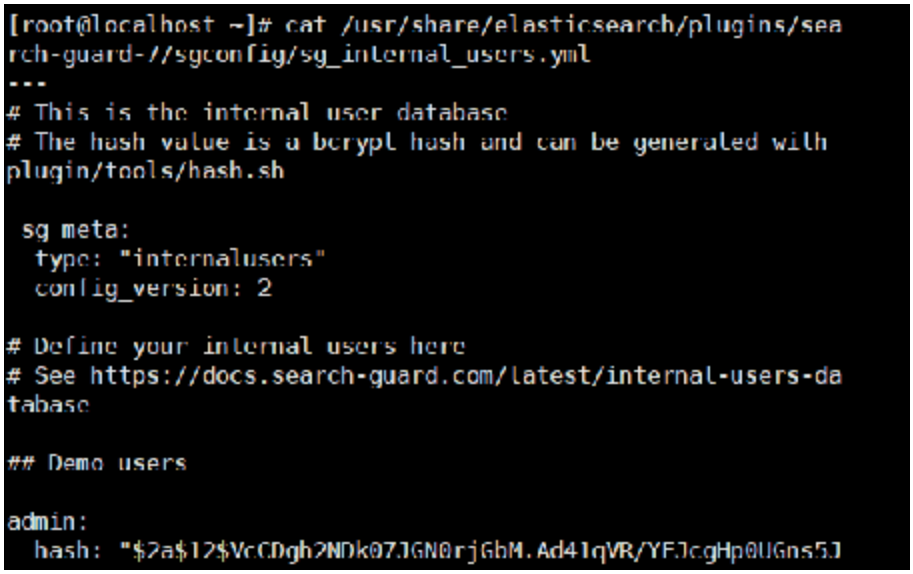
<table>
<tr><td></td><td>

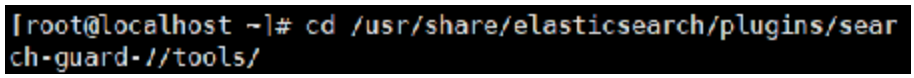
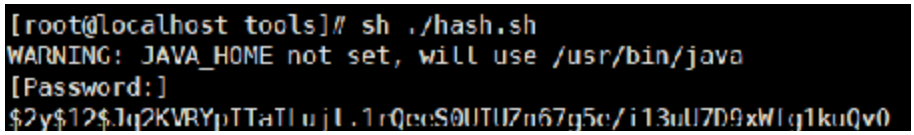
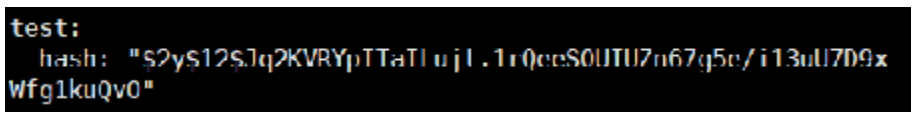
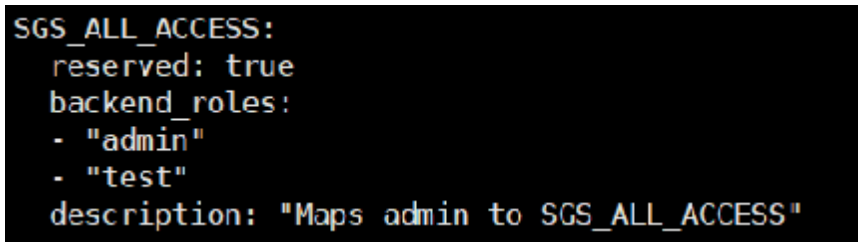
```
SGS_ALL_ACCESS:
  reserved: true
  backend roles:
  - "admin"
  - "test"
  description: "Maps admin to SGS ALL ACCESS"
```

5) [Elasticsearch 설치 디렉터리]/bin/search-guard-*/tools/sgadmin_demo.sh 스크립트를 실행하여 설정 적용

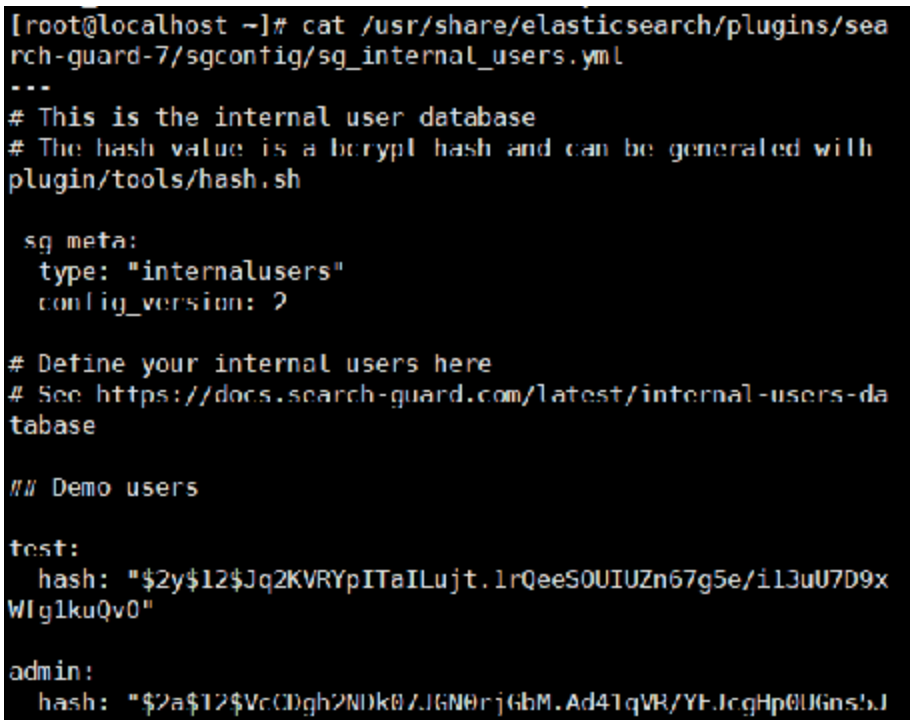
```
[root@ELK-TEST /]# /usr/share/elasticsearch/plugins/search-guard-5/tools/sgadmin_demo.sh
WARNING: JAVA_HOME not set, will use /bin/java
Search Guard Admin v5
Will connect to localhost:9300 ... done

### LICENSE NOTICE Search Guard ###

If you use one or more of the following features in production
make sure you have a valid Search Guard license
(See https://floragunn.com/searchguard-validate-license)
```

</td></tr>
<tr><td>비고</td><td>※ 1. Elasticsearch X-Pack(Shield)버전 별 관리자 권한 이름
- Elasticsearch2.4 이하
admin - 관리자 권한
- Elasticsearch5.0 이상
superuser - 관리자 권한
2. Elasticsearch SearchGuard 관리자 권한 이름
admin - 관리자 권한</td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">EL-02. 디폴트 계정 및 패스워드 변경</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Elasticsearch는 인증을 위해 플러그인 설치 시 디폴트 계정 및 패스워드가 존재하며, 각 정보는 인터넷 등을 통해 쉽게 구할 수 있다. 이를 통해 악의적인 사용자가 디폴트 계정, 패스워드를 이용하여 Elasticsearch에 접근이 가능하게 되어 데이터 변조, 정보 유출 등의 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">디폴트 계정 및 패스워드가 변경 되어 있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">디폴트 계정 및 패스워드가 변경 되어 있지 않았을 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ X-Pack 사용 시
1) CURL 명령어를 통해 확인
curl -u elastic:changeme –XGET 'localhost:9200/_xpack/security/user'
 
■ SearchGuard 사용 시
1) 설정파일을 통해 확인
cat [elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_internal_users.yml
 
※ Elasticsearch 버전 2.4 이하 일 경우 디폴트 계정 존재하지 않음</td></tr>
<tr><td>조치방법</td><td colspan="4">■ X-Pack 사용 시
1) 디폴트계정을 비활성화하기 전 새로운 관리자 권한의 계정생성 필요
 
2) CURL를 통해 기존 관리자 계정 비활성화</td></tr>
</table>

	# curl -u es_admin:root00 -XPUT 'localhost:9200/_xpack/security/user/elastic/_disable'  ■ SearchGuard 사용 시 1) # cd [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/tools를 통해 디렉터리 이동  2) # ./hash.sh 명령어를 통해 패스워드 해시값 생성  3) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_internal_users.yml 파일을 수정하여 기존 관리자 계정 영역 삭제 및 신규 계정 및 패스워드 적용  4) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_roles_mapping.yml 파일을 수정하여 기존 관리자 계정 삭제 및 신규 계정 적용  5) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/tools/sgadmin_demo.sh을 실행하여 설정 적용 
비고	※ Elasticsearch Shield 플러그인의 경우 디폴트 계정이 존재하지 않음 ※ Elasticsearch X-Pack 플러그인의 경우 디폴트 계정은 elastic, 패스워드는 changeme로 설정되어 있음 ※ Elasticsearch Search-Guard 플러그인의 경우 디폴트 계정은 admin, 패스워드는 admin으로 설정되어 있음

<table>
<tr><td>진단항목</td><td colspan="2">EL-03. 불필요한 계정 제거</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Elasticsearch의 계정 중 인가되지 않은 계정, 퇴직자 계정, 테스트 계정 등 실질적으로 업무에 사용하지 않은 불필요한 계정들이 있는 경우 비인가자가 쉽게 데이터베이스에 접속하여 데이터를 열람, 삭제, 수정 등을 할 위험이 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">테스트 계정, 의심스러운 계정, 불필요한 계정이 존재하지 않는 경우</td></tr>
<tr><td>취약</td><td colspan="3">테스트 계정, 의심스러운 계정, 불필요한 계정이 존재하는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
■ 설정 파일을 통해 확인
- Elasticsearch5.0 이상 X-Pack 플러그인 사용 시
cat [Elasticsearch 설정 디렉터리]/x-pack/users_roles


- Elasticsearch5.0 이상 Search-Guard 플러그인 사용 시
cat [Elasticsearch 설정 디렉터리]/sgconfig/sg_internal_users.yml


■ 명령어를 통해 확인
- Elasticsearch5.0 이상 X-Pack 플러그인 사용 시
[Elasticsearch 설치 디렉터리]/bin/x-pack/users list
</td></tr>
</table>

<table>
<tr><td></td><td>

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users list
test              : ingest_admin
es_admin          : superuser
```

</td></tr>
<tr><td>조치방법</td><td>

■ 명령어를 통해 변경

- Elasticsearch5.0 이상 X-Pack 플러그인 사용 시

[Elasricsearch 설치 디렉터리]/bin/x-pack/users userdel '계정명'

```
test@test-virtual-machine:~/elasticsearch-5.0.2/bin/x-pack$ ./users userdel test
```

■ 설정 파일 및 명령어를 통해 변경

- Elasticsearch5.0 이상 SearchGuard 플러그인 사용 시

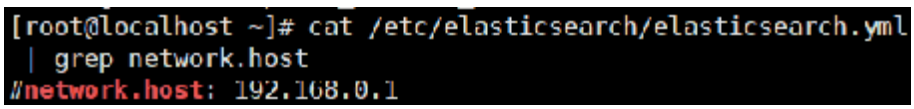
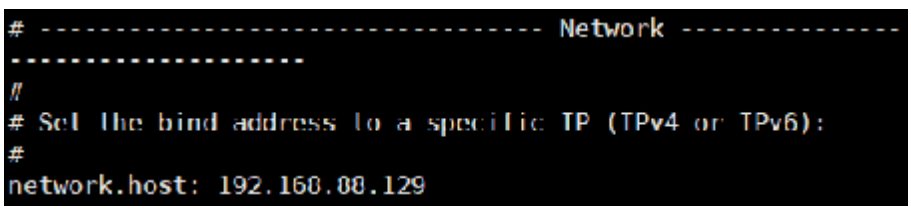
1) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig/sg_roles_mapping.yml 파일을 수정하여 불필요한 계정 제거

```
[root@localhost ~]# vi /usr/share/elasticsearch/plugins/sear
ch-guard-7/sgconfig/sg_internal_users.yml
[root@localhost ~]# cat /usr/share/elasticsearch/plugins/sea
rch-guard-7/sgconfig/sg_internal_users.yml
---
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with
plugin/tools/hash.sh

_sg_meta:
  type: "internalusers"
  config_version: 2

# Define your internal users here
# See https://docs.search-guard.com/latest/internal-users-da
tabase

## Demo users

admin:
  hash: "$2a$12$VcCDgh2NDk07JGN0rjGbM.Ad41qVR/YFJcgHp0UGns5J
```

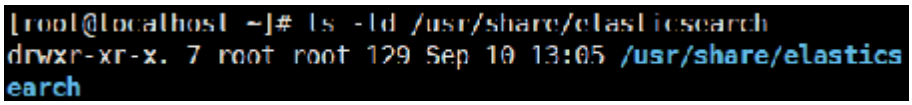
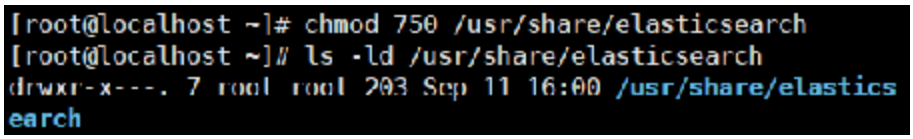
2) # [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/tools/sgadmin_demo.sh 을 실행하여 설정 적용

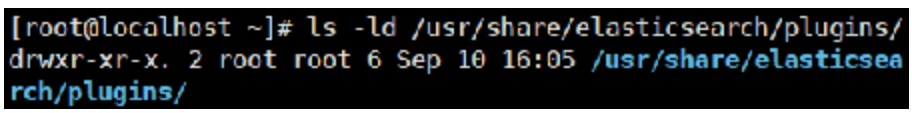
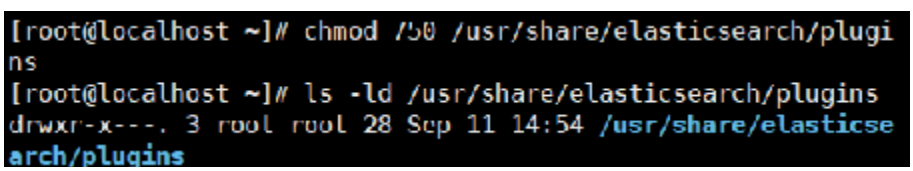
```
[root@ELK-TEST /]# /usr/share/elasticsearch/plugins/search-guard-5/tools/sgadmin_demo.sh
WARNING: JAVA_HOME not set, will use /bin/java
Search Guard Admin v5
Will connect to localhost:9300 ... done

### LICENSE NOTICE Search Guard ###

If you use one or more of the following features in production
make sure you have a valid Search Guard license
(See https://floragunn.com/searchguard-validate-license)
```

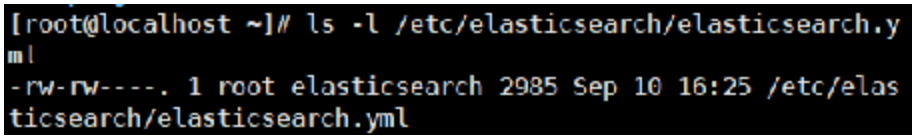
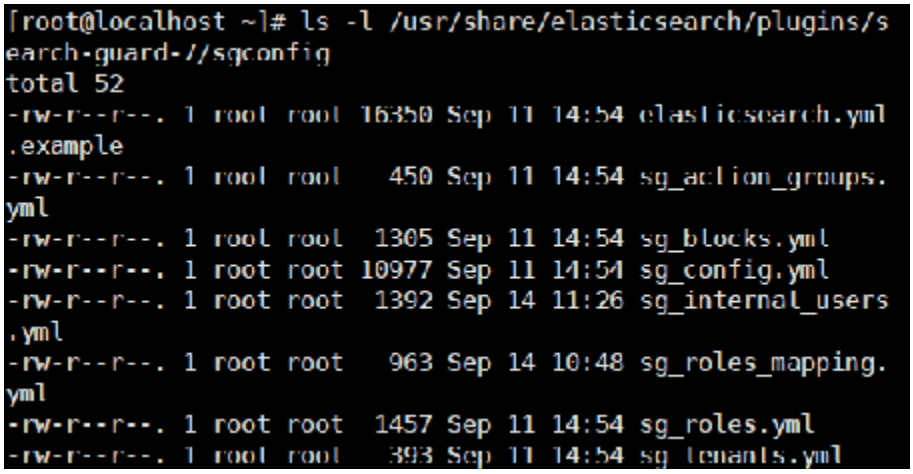
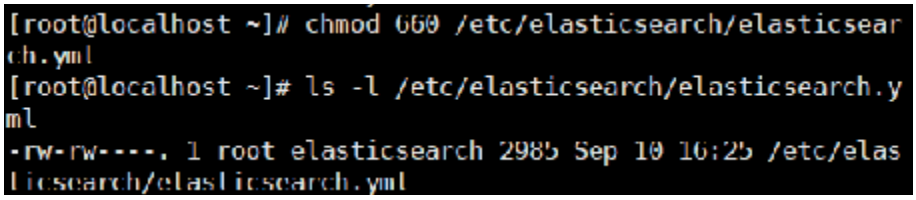
</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

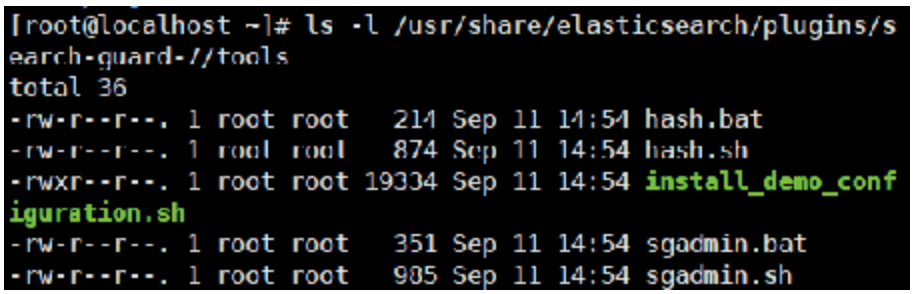
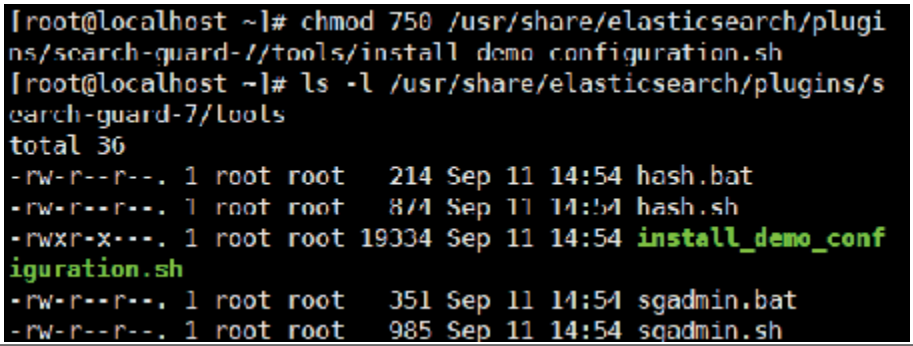
<table>
<tr><td>진단항목</td><td colspan="2">EL-04. IP 접근 제한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인가된 IP만 접근 가능하도록 설정되어 있지 않은 경우, 비 인가된 사용자가 해당 데이터베이스에 접근할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">인가된 IP만 접근 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">비 인가된 IP의 접근이 가능하도록 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Elasticsearch.yml 설정파일에서 network.host에 인가된 IP만 적용되어 있는지 확인
[Elasticsearch 설정 디렉터리]/cat elasticsearch.yml | grep network.host
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Elasticsearch 디렉터리> elasticsearch.yml 파일 안의 network.host 설정 변경
vi elasticsearch.yml 실행 후 network.host 설정을 인가된 IP로 변경
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

나. 디렉터리 및 파일권한 관리

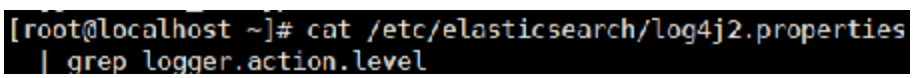
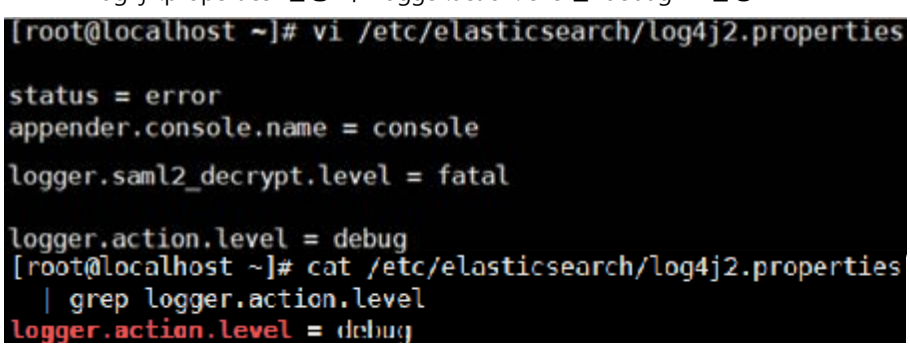
<table>
<tr><td>진단 항목</td><td colspan="2">EL-05. 설치 디렉터리 접근 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목 설명</td><td colspan="4">일반 사용자가 Elasticsearch 설치 디렉토리에 임의의 파일을 생성, 삭제 및 변경할 수 있으면, 중요파일 삭제, 백도어 삽입 등의 피해가 발생 할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">설치 디렉터리의 권한이 750 이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">설치 디렉터리의 권한이 750 이하로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Elasticsearch 설치 디렉터리 권한 확인
ls -ld [Elasticsearch 설치 디렉터리]
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Elasticsearch 설치 디렉터리 권한을 750으로 변경
chmod 750 [Elasticsearch 설치 디렉터리]
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

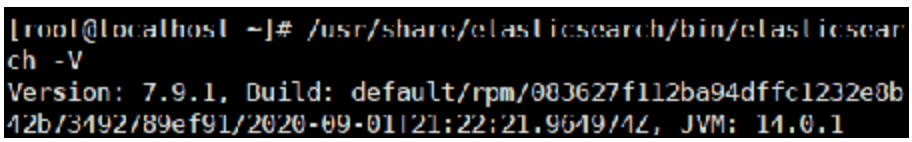
<table>
<tr><td>진단항목</td><td colspan="2">EL-06. 플러그인 디렉터리 접근 권한 설정</td><td>취약도</td><td>중</td></tr>
<tr><td>항목설명</td><td colspan="4">Elasticsearch 플러그인을 설치하게 되면 플러그인 디렉터리가 생성되고 그 안에서 설치한 플러그인을 관리하게 된다. 만약 일반 사용자가 해당 디렉터리에 접근 가능할 경우 임의의 파일을 생성, 삭제 및 변경 할 수 있으며 플러그인 파일 삭제, 백도어 삽입 등의 피해가 발생할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">플러그인 디렉터리 권한이 750 이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">플러그인 디렉터리 권한이 750 이하로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Elasticsearch 플러그인 디렉터리 권한 확인
ls -ld [Elasticsearch 설치 디렉터리]/plugins
 
</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Elasticsearch 플러그인 디렉터리 권한을 750으로 변경
chmod 750 [Elasticsearch 플러그인 디렉터리]
 
</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">EL-07. 설정파일 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">설정 파일에 others 권한이 존재할 경우, 비 인가된 사용자가 설정파일에 접근하여 설정 변경을 통해 서비스 장애를 일으킬 위험이 존재하며 또한 설정 파일을 통해 정보를 획득하여 2차 공격의 정보로 사용할 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">설정 파일 권한이 660 이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">설정 파일 권한이 660 이하로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Elasticsearch.yml 파일 권한 확인
ls -l [Elasticsearch 설정 디렉터리]/elasticsearch.yml
 
▪ SearchGuard 이용 시 설정 파일의 권한 확인
ls -l [Elasticsearch 설치 디렉터리]/plugins/search-guard-*/sgconfig 실행
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 설정 파일의 권한을 660 이하로 변경
chmod 660 [Elasticsearch 설정 파일]
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">EL-08. Search-Guard 스크립트 접근권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Search-guard를 통해 인증을 적용할 때 설정파일에 적용 후 Search-guard에서 제공하는 스크립트를 실행해야 인증 설정이 적용된다. 스크립트 파일 권한에 other 권한이 있을 경우 스크립트 내용이 노출되거나 스크립트가 실행되어 악의적인 영향을 끼칠 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Search-guard 스크립트 파일 권한이 750 이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Search-guard 스크립트 파일 권한이 750 이하로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ Elasticsearch 설정 파일의 권한 확인
ls –l [Elasticsearch 설정 디렉터리]/plugins/search-guard-*/tools
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ Search-guard 스크립트 파일 권한을 750 이하로 변경
chmod 750 [Elasticsearch 설정 디렉터리]/plugins/search-guard-*/tools/[Search-Guard 스크립트 파일]
ex)
chmod 750 /usr/share/elasticsearch/plugins/search-guard-7/tools/install_demo_configuration.sh
  </td></tr>
<tr><td>비고</td><td colspan="4">▪ Search-guard 플러그인이 설치되어 있지 않은 경우 해당 사항 없음</td></tr>
</table>

다. 패치 및 로그 관리

<table>
<tr><td>진단항목</td><td colspan="2">EL-09. 로그 활성화</td><td>취약도</td><td>하</td></tr>
<tr><td>항목설명</td><td colspan="4">로그를 정기적으로 분석하여 침입 유무를 파악하고, 침입 시도 의심 사례를 분석하여 사전에 해당 장비에 대한 접근을 차단하는 등 체계적인 로그 관리 작업이 이루어져야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">로그가 활성화되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">로그가 비 활성화되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 로그 레벨 설정 확인
- Elasticsearch5.0 이상
cat log4j2.properties | grep logger.action.level
  </td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 로그 레벨 설정 변경
- Elasticsearch5.0 이상
vi log4j2.properties 실행 후 logger.action.level를 debug로 설정
  </td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">EL-10. 최신 패치 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 패치가 적용되어 있지 않을 경우, 잘 알려진 취약점에 데이터베이스가 노출될 위험이 존재한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">잘 알려진 취약점이 존재하지 않는 버전을 사용 중인 경우</td></tr>
<tr><td>취약</td><td colspan="3">잘 알려진 취약점이 존재하는 버전을 사용 중인 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
■ CLI를 통해 확인
[Elasticsearch 설치 디렉터리]/bin/elasticsearch -V


■ CURL를 통해 확인
curl localhost:9200


</td></tr>
<tr><td>조치방법</td><td colspan="4">
■ 수동 조치
1) 잘 알려진 취약점이 없는 버전으로 업그레이드 하여야 함
</td></tr>
</table>

<table>
<tr><td>비고</td><td>※ Elasticsearch End of Life 정보
<table>
<tr><th>버전 정보</th><th>제공 종료 날짜</th><th>제품 유지 기한</th></tr>
<tr><td>6.7.x</td><td>2020-09-25</td><td>6.8.0</td></tr>
<tr><td>6.8.x</td><td>2020-11-20</td><td>8.0.0</td></tr>
<tr><td>7.0.x</td><td>2020-10-10</td><td>7.1.0</td></tr>
<tr><td>7.1.x</td><td>2020-11-20</td><td>7.2.0</td></tr>
<tr><td>7.2.x</td><td>2020-12-25</td><td>7.3.0</td></tr>
<tr><td>7.3.x</td><td>2021-01-31</td><td>7.4.0</td></tr>
<tr><td>7.4.x</td><td>2021-04-01</td><td>7.5.0</td></tr>
<tr><td>7.5.x</td><td>2021-06-02</td><td>7.6.0</td></tr>
<tr><td>7.6.x</td><td>2021-08-11</td><td>7.7.0</td></tr>
<tr><td>7.7.x</td><td>2021-11-13</td><td>7.8.0</td></tr>
<tr><td>7.8.x</td><td>2021-12-18</td><td>7.9.0</td></tr>
<tr><td>7.9.x</td><td>2022-02-18</td><td>7.10.0</td></tr>
</table></td></tr>
</table>

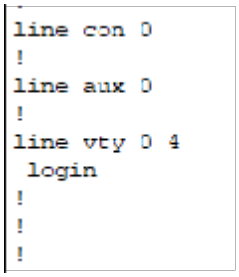
2.20. 네트워크장비

계정 관리(3개 항목), 접근 관리(2개 항목), 패치 관리(1개 항목), 기능 관리(6개 항목) 총 4개 영역에서 12개 항목으로 구성된다.

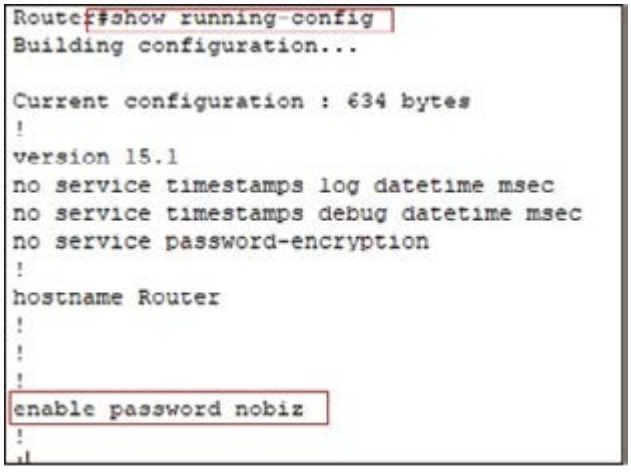
구분	진단코드	진단 항목	취약도
가. 계정 관리	NW-01	패스워드 설정	상
	NW-02	패스워드 복잡성 설정	상
	NW-03	암호화된 패스워드 사용	상
나. 접근 관리	NW-04	VTY접근(ACL) 설정	상
	NW-05	Session Timeout 설정	상
다. 패치 관리	NW-06	최신 보안 패치 및 벤더 권고사항 적용	상
라. 기능 관리	NW-07	SNMP 서비스 확인	상
	NW-08	SNMP community string 복잡성 설정	상
	NW-09	SNMP ACL 설정	상
	NW-10	SNMP 커뮤니티 권한 설정	상
	NW-11	TFTP 서비스 차단	상
	NW-12	사용하지 않는 인터페이스의 shutdown 설정	상

[표 20] 네트워크장비 진단 체크리스트

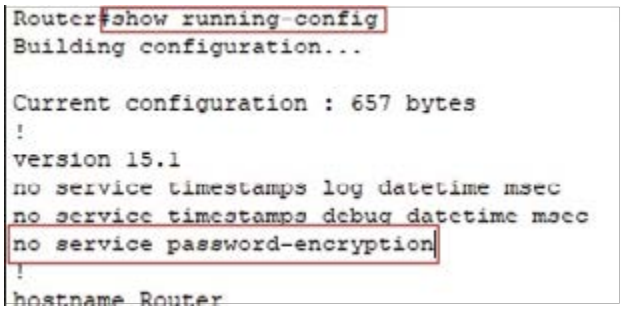
가. 계정 관리

<table>
<tr><td>진단항목</td><td colspan="2">NW-01. 패스워드 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">원격에서 라우터를 관리할 때 사용하는 패스워드를 장비의 초기 설정 그대로 사용할 경우, 누구라도 라우터에 접근할 수 있다. 이러한 기본 패스워드는 인터넷상에서 검색을 통해 쉽게 접할 수 있으므로, 패스워드는 반드시 설정 또는 변경한 후에 사용해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">장비의 패스워드가 초기 패스워드가 아닌 별도의 패스워드로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">장비의 패스워드가 초기 설정 그대로 설정되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
■ 패스워드 설정 정보 확인
(config)# show running-config
line con 0
password <password>
login
line vty 0 4
password <password>
login
 
<Juniper>
■ 패스워드 설정 정보 확인
R1> show configuration
system {
root-authentication {
encrypted-password "password";
SECRET-DATA
}
login {
user mims {
full-name mims;
uid 2000;</td></tr>
</table>

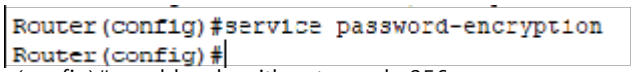
	class super-user; authentication { **encrypted-password** "password"; ## SECRET-DATA }
조치방법	<CISCO> ■ Privileged mode 암호 설정 (config)# enable secret <패스워드> `Router(config)# enable secret nobiz` `Router(config)#` ■ vty 패스워드 설정 (config)# line vty 0 4 (config-line)# login (config-line)# password <패스워드> `Router(config)#line vty 0 4` `Router(config-line)#login` `% Login disabled on line 388, until 'password' is set` `% Login disabled on line 389, until 'password' is set` `% Login disabled on line 390, until 'password' is set` `% Login disabled on line 391, until 'password' is set` `% Login disabled on line 392, until 'password' is set` `Router(config-line)#password nobiz` ■ Console 패스워드 설정 (config)# line console 0 (config-line)# login (config-line)# password <패스워드> `Router(config)#line console 0` `Router(config-line)#login` `% Login disabled on line 0, until 'password' is set` `Router(config-line)#password nobiz` <Juniper> ■ root 패스워드 설정 R1# set system root-authentication plain-text-password New Password : Retype new password: ■ User 계정 패스워드 설정 R1# edit system login R1# edit user 계정명 R1# set authentication plain-text-password New Password : Retype new password:
비고	■ default 설정은 패스워드가 설정되어 있지 않음

<table>
<tr><td>진단항목</td><td colspan="2">NW-02. 패스워드 복잡성 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">Console, VTY, AUX로 접속하여 enable 모드 접속 시 추측하기 쉬운 패스워드를 사용할 경우, 비인가자가 패스워드 추측을 통해 장비에 접속할 수 있다. 또한 장비의 설정은 읽기만 하는 권한과 설정을 변경할 수 있는 권한으로 구분되는데, 접속 패스워드와 enable password가 같을 경우 하나의 패스워드 추측만으로 장비의 설정을 변경할 수 있으므로 접속 패스워드, enable password, enable secret를 다르게 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드가 대·소문자, 숫자, 특수문자가 포함된 8자리 이상으로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드가 대·소문자, 숫자, 특수문자가 포함된 8자리 이상으로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
■ 패스워드 설정 정보 확인
(config)# show running-config
enable password <패스워드>
line con 0
password <패스워드>
 
...
 
<Juniper>
■ 패스워드 설정 정보 확인
R1> show configuration
system {
root-authentication {</td></tr>
</table>

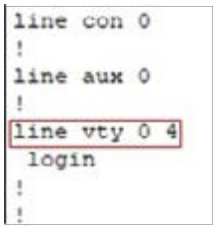
	encrypted-password "<**password**>"; ## SECRET-DATA } login { class super-user-local { idle-timeout 1; permissions all; } user ksel { full-name monitor; uid 110; class super-user-local; authentication { encrypted-password "<**password**>"; ## SECRET-DATA
조치방법	■ 패스워드 설정을 참고하여 패스워드 설정 시 아래와 같은 규칙을 적용하여 변경 1) 암호는 적어도 8자 이상이어야 함 2) 사용자 계정 이름이나 표시 이름의 문자를 3개 이상 연속하여 포함하지 않아야 함 3) 암호에는 다음 네 가지 중 세 가지 범주의 문자가 포함되어야 함 ① 대문자(A, B, C, ...) ② 소문자(a, b, c, ...) ③ 숫자(0, 1, 2, 3, 4, 5, 6, 7, 8, 9) ④ 영숫자 이외의 문자와 유니코드 문자
비고	

<table>
<tr><td>진단항목</td><td colspan="2">NW-03. 암호화된 패스워드 사용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">패스워드를 암호화하지 않을 경우, Username password, Authentication key password, Privileged command password, Console access password, VTY access password와 BGP neighbor password 등의 패스워드들이 평문으로 저장된다. Config(설정 값) 유출 시 장비 접근에 대한 패스워드 노출의 위험성이 있으므로 패스워드 생성시 암호화하여 저장해야 한다. 구조가 단순한 Vigenere 알고리즘이 사용되므로 enable 패스워드의 경우 Secret 패스워드를 별도로 지정하는 것이 보다 안전하다. 사용자 계정 권한 및 패스워드 관리 미흡으로 인한 불법적인 공격 또는 기밀정보가 유출될 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">패스워드 암호화 설정이 되어 있을 경우</td></tr>
<tr><td>취약</td><td colspan="3">패스워드 암호화 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
■ 패스워드 설정 정보 확인
(config)# show running-config
no service password-encryption
 
<Juniper>
■ 패스워드 설정 정보 확인
R1> show configuration
password {
format sha1;
}

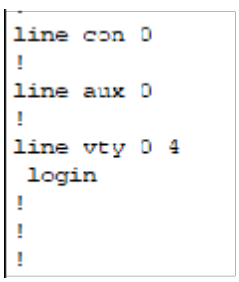
※ 해당 OS 버전에서 지원이 가능한 경우, SHA-256 이상 적용 필요
- Cisco IOS15.3(3)M부터 지원(Type8)
- SHA-256 적용 가능한 Juniper 버전 리스트 아래 페이지 참조
https://apps.juniper.net/feature-explorer/feature-info.html?fKey=287&fn=Hash%20Algorithms%20SHA-2%20(SHA-256)</td></tr>
</table>

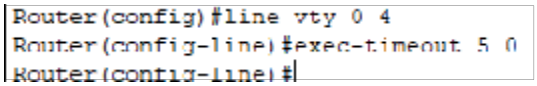
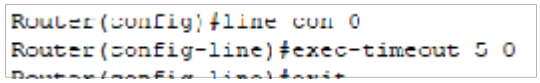
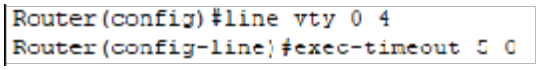
조치방법	<CISCO> ▪ 명령어를 통해 패스워드 암호화 설정 (config)# service password-encryption  (config)# enable algorithm-type sha256 (config)# secret cisco ※ 단순 암호화 설정할 경우 취약한 알고리즘이 적용되므로 별도의 SHA2 이상 암호화 적용이 필요함 <Juniper> ▪ 명령어를 통해 plain-text-password 설정 시 암호를 sha2로 암호화한다. R# set system login password format sha2
비고	

나. 접근 관리

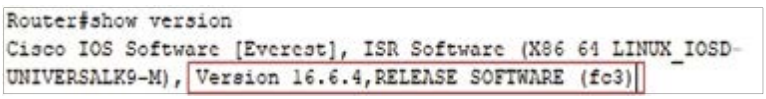
<table>
<tr><td>진단항목</td><td colspan="2">NW-04. VTY접근(ACL) 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">인터넷으로부터 VTY 접근을 차단하지 않았을 경우 VTY 장치를 통해서 네트워크 접속을 시도할 수 있으며, 원격 접속 패스워드 추측공격 및 sniffer 공격을 통해 장비에 접근할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">VTY 접근이 차단되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">VTY 접근이 차단되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
▪ 설정 정보 확인
(config)# show running-config
 
<Juniper>
▪ 설정 정보 확인
R2>Show configuration
firewall {
family inet {
filter local-access-control {
term terminal-access {
from {
address {
192.168.xxx.xxx/24;
}
protocol tcp;
port [ssh telnet];
}
then accept;
}
term terminal-access-denied {
from {
protocol tcp;
port [ssh telnet];
}</td></tr>
</table>

	then { log; reject; } } term default-term { then accept; } } } }
조치방법	<CISCO> ▪ 다음 명령어를 통해 VTY 접근 설정 (config)# access-list [1-99] {permit|deny} [Source Network] [WildcardMask] (config)# access-list [1-99] {deny|permit} any (config)# line vty 0 4 (config-line)# access-class [1-99] in ex) Router(config)#access-list 1 deny 150.100.7.128 0.0.0.31 Router(config)#access-list 1 permit any Router(config)#line vty 0 4 Router(config-line)#access-class 1 in Router(config-line)# <Juniper> ▪ 다음 명령어를 통해 VTY 접근 설정 R# edit firewall family inet filter **filter-name** R# set term **rule-name1** from address IP/32 허용 지정 R# set term **rule-name1** from protocol tcp R# set term **rule-name1** from port ssh R# set term **rule-name1** from port telnet R# set term **rule-name1** then accept R# set term **rule-name2** from protocol tcp R# set term **rule-name2** from port ssh R# set term **rule-name2** from port telnet R# set term **rule-name2** then log R# set term **rule-name2** then reject R# set term default-term then accept R# exit R# set interfaces lo0 unit 0 family inet filter input **filter-name** R# set interfaces lo0 unit 0 family inet address 127.0.0.1/32
비고	

<table>
<tr><td>진단항목</td><td colspan="2">NW-05. Session Timeout 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">관리자가 장비에 접속하고 무의식적으로 장시간 접속 터미널을 떠났을 때 자동으로 접속을 종료하거나 로그아웃이 되도록 설정하는 것이 좋다. 이는 실수로 로그아웃을 하지 않고 자리를 뜨는 경우에 존재하는 위험에 대비할 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">Session Timeout이 600초 이하로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">Session Timeout이 600초 이하로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
▪ 설정 정보 확인
(config)# show running-config
line con 0
exec-timeout <minute> <second>
line vty 0 4
exec-timeout <minute> 
(config-line)# exec-timeout 0 0 // Telnet에 대한 timeout이 발생하지 않도록 하는 설정이므로 이를 확인한다.
<Juniper>
▪ 일반적인 방법으로 확인
R> show configuration
system {
root-authentication {
...
}
login {
class super-user-local {
idle-timeout 1;
permissions all;
}
user ksel {
full-name monitor;
uid 110;</td></tr>
</table>

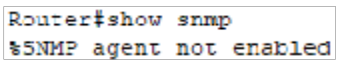
<table>
<tr><td></td><td>class super-user-local;
■ 개별 세션들에 대한 방법 확인
R> show cli
CLI complete-on-space set to on
CLI idle-timeout set to 5minutes</td></tr>
<tr><td>조치방법</td><td><CISCO>
■ 다음 명령어를 통해 Session Timeout 설정
(config)# line vty 0 4
(config-line)# exec-timeout 5 0 → 접속 후 5분 동안 어떠한 입력이 없는 경우
 
■ 자동 종료 설정
(config)# line con 0
(config-line)# exec-timeout <minute> <second>
→ idle timeout 시간을 분, 초로 설정
ex)
 
(config)# line vty 0 4
(config-line)# exec-timeout <minute> <second>
→ idle timeout 시간을 분, 초로 설정
ex)
 
<Juniper>
■ Session Timeout 설정
R# set system login class class-name idle-timeout 1
R# set system login class class-name permissions all
R# set system login user 계정명 class class-name</td></tr>
<tr><td>비고</td><td></td></tr>
</table>

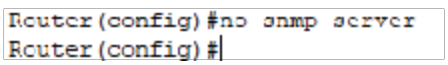
다. 패치 관리

<table>
<tr><td>진단항목</td><td colspan="2">NW-06. 최신 보안 패치 및 벤더 권고사항 적용</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">최신 취약점에 대한 패치 및 업데이트를 점검한다. 네트워크 장비의 보안수준을 제고하고 성능 및 기능 향상을 위해서는 지속적인 Version upgrade 및 보안 patch 작업을 수행하여 최신 취약점을 보완하는 작업이 필요하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">최신 보안 패치 및 업데이트가 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">최신 보안 패치 및 업데이트가 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
▪ 다음 명령어를 통해 버전 정보를 확인
(config)# show version
버전정보 확인
 
<Juniper>
▪ 다음 명령어를 통해 버전 정보를 확인
R> show version
Model: olive
JUNOS Base OS boot [12.1R1.9]
JUNOS Base OS Software Suite [12.1R1.9]
JUNOS Kernel Software Suite [12.1R1.9]
JUNOS Crypto Software Suite [12.1R1.9]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.1R1.9]
JUNOS Packet Forwarding Engine Support (M20/M40) [12.1R1.9]
JUNOS Online Documentation [12.1R1.9]
JUNOS Voice Services Container package [12.1R1.9]
JUNOS Border Gateway Function package [12.1R1.9]
JUNOS Services AACL Container package [12.1R1.9]
JUNOS Services LL-PDF Container package [12.1R1.9]
JUNOS Services PTSP Container package [12.1R1.9]
JUNOS Services Stateful Firewall [12.1R1.9]
JUNOS Services NAT [12.1R1.9]
JUNOS Services Application Level Gateways [12.1R1.9]
JUNOS Services Captive Portal and Content Delivery Container package [12.1R1.9]
JUNOS Services RPM [12.1R1.9]
JUNOS Services HTTP Content Management package [12.1R1.9]</td></tr>
</table>

	JUNOS AppId Services [12.1R1.9] JUNOS IDP Services [12.1R1.9] JUNOS Services Crypto [12.1R1.9] JUNOS Services SSL [12.1R1.9] JUNOS Services IPSec [12.1R1.9] JUNOS Runtime Software Suite [12.1R1.9] JUNOS Routing Software Suite [12.1R1.9]
조치방법	■ 벤더 사의 권장 버전을 적용 1) 보안의 관점에서 본다면 오랜 기간의 테스트와 수정을 통하여 검증받은 GD 단계의 IOS를 사용하여야 하며, 다른 버전은 꼭 필요한 기능이 있는 경우만 사용해야 함. IOS의 버전 체계 및 버전별 정보는 아래 사이트를 통하여 얻을 수 있음 CISCO : http://www.cisco.com/web/about/security/intelligence/ios-ref.html JUNIPER : https://kb.juniper.net/InfoCenter/index?page=content&id=KB21476&actp=search 2) 위의 IOS 버전 체계와 더불어 IOS 버전 이름이 붙여지는 방법 또한 IOS 적용을 위하여 꼭 알고 있어야 할 사항임. "Version 12.2(2)T4"에서 12.2는 Major Release의 버그 수정은 8주를 주기로 이루어지며 Major Release 번호 옆의 괄호의 번호가 버그 수정이 몇 번째 이루어졌는가를 나타냄
비고	

라. 기능 관리

<table>
<tr><td>진단항목</td><td colspan="2">NW-07. SNMP 서비스 확인</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP는 UDP를 이용하기 때문에 공격 주소를 속여 DOS 공격을 할 수 있다. 라우터의 성능저하, 크래쉬, 리로드 등의 장애가 초래하게 되어 불필요할 경우는 비활성화 시키는 것이 좋다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP 서비스가 비활성화 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SNMP 서비스가 활성화 되어 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
<CISCO>
■ SNMP 설정 현황 확인
(config)# show snmp
 

<Juniper>
■ SNMP 설정 현황 확인
R# show configuration
snmp {
...
}</td></tr>
<tr><td>조치방법</td><td colspan="4">
<CISCO>
■ SNMP 서비스를 사용하지 않을 경우 다음 명령어를 통해 비활성화
(config)# no snmp-server
 

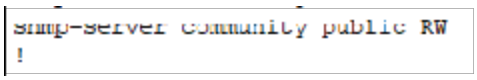
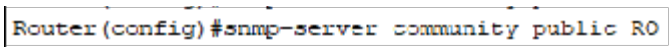
<Juniper>
■ SNMP 서비스를 사용하지 않을 경우 다음 명령어를 통해 비활성화
R# delete snmp</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

<table>
<tr><td>진단항목</td><td colspan="2">NW-08. SNMP community string 복잡성 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP에서 community string은 SNMP(데몬)와 클라이언트가 데이터를 교환하기 전에 인증하는 일종의 패스워드로서 초기값으로 설정되어 있는 Public, Private과 같은 SNMP default community string을 이용할 시에 해당 장비의 routing table, MAC address 등의 중요한 정보를 외부로 노출시킬 가능성이나 네트워크 장비 설정 등을 변경(RW)시킬 수 있는 위험성이 많다. 이를 그대로 사용하는 것은 패스워드를 사용하지 않는 계정을 사용하는 것 이상 위험함에도 불구하고 대부분의 시스템, 네트워크 관리자들이 기본적인 문자열인 public을 그대로 사용하거나 다른 문자열로 변경을 해도 상호나 monitor, router, mrtg 등 사회 공학적으로 추측할 수 있는 문자열을 사용하고 있어 문제가 되고 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP Community String을 디폴트가 아닌 특정 문자열을 사용하고 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SNMP Community String을 디폴트 문자열로 사용하고 있는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
▪ SNMP Community String 확인
(config)# show running-config
SNMP 설정 확인
<pre>!
snmp-server community public RW
!</pre><Juniper>
▪ SNMP Community String 확인
R> show configuration
community name {
authorization read-only;</td></tr>
<tr><td>조치방법</td><td colspan="4"><CISCO>
▪ SNMP Community String 변경
(config)# config terminal
(config)# snmp-server Community <커뮤니티 명>
ex)
<pre>Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#snmp server Community nobiz123</pre>※ snmp-server community command는 IOS 10.0 버전부터 기능 제공
<Juniper></td></tr>
</table>

	■ SNMP Community String 변경 R# edit snmp R# rename community 기존-community-string to community 새로운-community-string
비고	

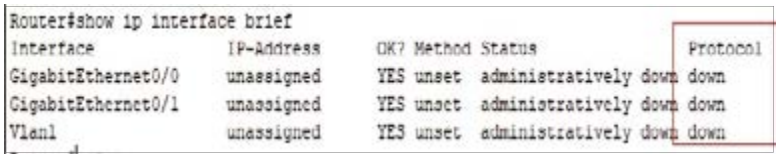
<table>
<tr><td>진단항목</td><td colspan="2">NW-09. SNMP ACL 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP 정보를 액세스 할 수 있는 인가된 호스트를 제한함으로써 불법적인 액세스에 대해 원천적인 차단이 가능하며, SNMP Community String을 이용한 인증 이외에 접근제어가 설정됨으로써 SNMP의 보안성이 한층 더 강화될 수 있다. IP access-list를 활용하여 특정 호스트 혹은 네트워크만이 SNMP 정보를 액세스 할 수 있도록 설정해야 한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">IP access-list가 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">IP access-list가 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">
<CISCO>
■ SNMP ACL 확인
(config)#show running-config
access-list 1 permit xxx.xxx.xxx.xxx
snmp-server community Community_string RO
<pre>
!
access-list 70 deny 13.13.10.0.0.0.0.255
access-list 70 permit any
!
!
!
!
!
snmp server community public RW
!
</pre>
<Juniper>
■ SNMP ACL 확인
snmp {
...
client-list list0 {
192.168.100.123/32;
}
community snmp-syp {
protect: authorization read-only;
protect: client-list-name list0;
or clients {
192.168.40.128/32;
}
or
community "community-ed-10$" {
client-list-name prefixlist;
}
</td></tr>
</table>

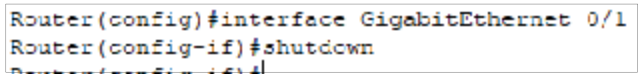
	} **policy-options {** **prefix-list prefixlist{** 192.168.100.32/32; 192.168.100.40/32; 192.168.100.80/32;
조치방법	<CISCO> ▪ SNMP ACL 적용 (config)# snmp-server community Community_string [ro | rw] (config)# access-list [number] permit xxx.xxx.xxx.xxx ex) Router(config)#snmp-server community public RO Router(config)#access list 1 permit 192.138.15.4 ※ snmp-server community command는 IOS 10.0 버전부터 기능 제공 <Juniper> ▪ SNMP ACL 적용 R# set snmp client-list clinet-number 192.168.0.0/24 R# set snmp community 기존-community-string client-list-name clinet-number R# set snmp community 기존-community-string clients 192.170.0.0/24 restrict 또는 R# edit policy-options R# set prefix-list prefix-list-name 허용IP/32 R# exit R# edit snmp R# community 기존-community-string client-list-name prefix-list-name
비고	

<table>
<tr><td>진단항목</td><td colspan="2">NW-10. SNMP 커뮤니티 권한 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP에서는 RO(Read Only)와 RW(Read/Write) 모드를 제공하는데, 대부분 RO모드를 사용하지만 일부 관리자들은 SNMP를 이용한 쉬운 관리를 위해 RW(Read/Write) community 문자열을 사용하는 경우도 있다. 이러한 경우 보안 설정을 확실하게 하지 않을 경우 SNMP를 이용하여 설정을 수정할 수 있는 등 심각한 보안문제를 유발할 수 있으며, SNMP를 이용하면 전체 네트워크의 구성, MAC 주소, IP 주소, SW 정보, HW 정보 등을 알 수 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP community String 권한이 RO로 설정되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">SNMP community String 권한이 RO로 설정되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
▪ SNMP Community 권한 확인
(config)#show running-config
snmp-server community community_string RO
 
<Juniper>
▪ SNMP Community 권한 확인
R> show configuration
community name {
authorization read-only;</td></tr>
<tr><td>조치방법</td><td colspan="4"><CISCO>
▪ SNMP Community String 권한을 Read Only로 설정
(config)# snmp-server community <스트링명> RO (읽기권한)
 
※ snmp-server community command는 IOS 10.0 버전부터 기능 제공

<Juniper>
▪ SNMP Community String 권한을 Read Only로 설정
R# edit snmp
R# set community -community-string authorization read-only</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	NW-11. TFTP 서비스 차단		취약도	상
항목설명	TFTP 서비스는 특정 호스트가 아닌 일반적으로 어느 호스트에게 접근할 수 있게 되며, 특히 서버에 수행되는 데몬 프로세서가 자신의 파일 시스템에 대한 접근을 두지 않는 경우에는 읽기 가능한 어느 파일도 외부에 있는 시스템에서 침입 정보를 빼내어 갈 가능성이 있다. TFTP는 인증 과정을 거치지도 않고 누구든지 파일을 읽거나 쓸 수 있도록 허용하기 때문에 가급적이면 차단시키는 것이 좋다.			
진단기준	양호	TFTP 서비스가 비활성화 되어 있는 경우		
	취약	TFTP 서비스가 활성화 되어 있는 경우		
진단방법	<CISCO> ■ TFTP 설정 현황 확인 (config)#show run tftp-server <Juniper> ■ TFTP 설정 현황 확인 R# show system services { tftp-server; }			
조치방법	<CISCO> ■ TFTP 서비스 비활성화 (config)# no tftp-server <Juniper> ■ TFTP 서비스 비활성화 R# delete system services tftp-server			
비고	■ default disabled			

<table>
<tr><td>진단항목</td><td colspan="2">NW-12. 사용하지 않는 인터페이스의 shutdown 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">라우터와 스위치에는 많은 포트가 있는데 사용하지 않은 포트에 연결시킨 인터페이스 상태가 Up이 되어 있다면 다른 외부 침입자에 의해 라우터의 정보와 내부 네트워크 망에 손실을 입힐 수가 있다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">사용하지 않은 인터페이스의 Shutdown 설정이 되어 있는 경우</td></tr>
<tr><td>취약</td><td colspan="3">사용하지 않은 인터페이스의 Shutdown 설정이 되어 있지 않은 경우</td></tr>
<tr><td>진단방법</td><td colspan="4"><CISCO>
■ 해당 인터페이스 Shutdown 확인
(config)# show ip interface brief
(우측부분에 해당포트가 down/up 이 되어 있는지 확인 할 수 있다.)
 

<Juniper>
■ 해당 인터페이스 Shutdown 확인
user@juniper>show configure</td></tr>
<tr><td>조치방법</td><td colspan="4"><CISCO>
■ 사용하지 않은 인터페이스 차단
(config)# interface GigabitEthernet 0/1
(config-if)# shutdown
 

<Juniper>
■ 사용하지 않은 인터페이스 차단
[edit interface interface-name] ← 해당 인터페이스 이름 삽입
set disable;</td></tr>
<tr><td>비고</td><td colspan="4">■ 아래 페이지를 참조
http://www.cisco.com/en/US/products/ps6017/products_command_reference_chapter09186a0080882d91.html</td></tr>
</table>

2.21. 정보보호시스템

계정 관리(4개 항목), 접근 관리(3개 항목), 패치 관리(1개 항목), 기능 관리(6개 항목), 총 4개 영역에서 14개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. 계정 관리	NF-01	정보보호시스템 Default 계정 변경	상
	NF-02	정보보호시스템 Default 패스워드 변경	상
	NF-03	정보보호시스템 계정별 권한 설정	상
	NF-04	정보보호시스템 계정 관리	상
나. 접근 관리	NF-05	정보보호시스템 원격 관리 접근 통제	상
	NF-06	정보보호시스템 보안 접속	상
	NF-07	Session timeout 설정	상
다. 패치 관리	NF-08	벤더에서 제공하는 최신 업데이트 적용	상
라. 기능 관리	NF-09	정책 관리	상
	NF-10	최소한의 서비스만 제공	상
	NF-11	이상 징후 탐지 경고 기능 설정	상
	NF-12	장비 사용량 검토	상
	NF-13	SNMP 서비스 확인	상
	NF-14	SNMP Community string 복잡성 설정	상

[표 21] 정보보호시스템 진단 체크리스트

가. 계정 관리

진단항목	NF-01. 정보보호시스템 Default 계정 변경		취약도	상
항목설명	디폴트 로그인 계정은 장비 제조업체에서 출고 시 설정되어 나오는 기본 계정정보를 의미한다. 각 제조사의 장비별 디폴트 계정 리스트는 인터넷 등을 통해 쉽게 구할 수 있으며 악의적인 사용자가 이러한 디폴트 계정을 이용하여 불법적으로 방화벽 장비에 접근할 수 있고 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있다.			
진단기준	양호	장비에서 제공하고 있는 디폴트 계정 명을 변경하여 사용하는 경우 (ID 변경이 불가능 할 경우 패스워드로 보완 필요)		
	취약	장비에서 제공하고 있는 디폴트 계정 명을 변경하지 않고 사용하는 경우		
진단방법	■ Default 계정 확인 1) Web을 통한 접속 2) 디폴트 계정, 비밀번호 입력 3) 접속확인			
조치방법	■ Default 계정 변경 1) 보안장비에서 제공하고 있는 계정 메뉴에서 ID 변경 2) ID 변경이 불가능할 경우 패스워드로 보완 필요			
비고				

진단항목	NF-02. 정보보호시스템 Default 패스워드 변경		취약도	상
항목설명	디폴트 로그인 패스워드는 장비 제조업체에서 출고 시 설정되어 나오는 기본 로그인 패스워드 정보를 의미한다. 각 제조사의 장비별 디폴트 로그인 패스워드 리스트는 인터넷 등을 통해 쉽게 구할 수 있으므로 악의적인 사용자가 이러한 디폴트 로그인 패스워드를 이용하여 불법적으로 방화벽 장비에 접근할 수 있고 시스템 침입 경로를 제공하는 등 일반적인 정보시스템 침해사고보다 심각한 피해를 초래할 수 있다.			
진단기준	양호	장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하지 않은 경우 (특수문자, 숫자, 영문 대소문자 포함 8자리 이상)		
	취약	장비 디폴트 패스워드 또는 유추 가능한 패스워드를 사용하는 경우		
진단방법	■ Default 패스워드 확인 1) Web을 통한 접속 2) 디폴트 계정, 비밀번호 입력 3) 접속확인			
조치방법	■ Default 패스워드 변경 1) 패스워드 메뉴에서 패스워드 변경 2) 보안장비가 제공하는 범위에서 패스워드 설정 (특수문자, 숫자, 영문 대소문자 포함 8자리이상)			
비고				

진단항목	NF-03. 정보보호시스템 계정별 권한 설정	취약도	상
항목설명	여러 사용자가 접속하여 사용하는 경우, 계정의 부적절한 권한 설정으로 인해 시스템의 침입 경로가 유출 될 수 있다. 예를 들어 보안정책과 관련 없는 사용자에게 보안정책을 수정할 수 있는 권한이 부여된다면, 의도하지 않게 보안정책이 수정될 수 있으므로, 계정별 권한의 타당성을 확인해야 한다.		
진단기준	양호	사용자별 계정의 용도 파악 및 적절한 권한을 부여하는 경우	
	취약	사용자별 계정의 용도 파악 및 적절한 권한을 부여하지 않는 경우	
진단방법	▪ 보안장비에서 제공하고 있는 계정 메뉴에서 계정별 권한 확인		
조치방법	▪ 계정별 불필요한 권한 제거 변경 1) 보안장비에서 제공하고 있는 계정 메뉴에서 새로운 계정 생성 2) 새로운 계정 담당자에 대한 역할 확인 후 권한 부여		
비고			

진단항목	NF-04. 정보보호시스템 계정 관리	취약도	상
항목설명	계정 관리가 미흡한 경우 자신의 업무와 관련이 없는 애플리케이션 및 자원에 접속할 수 있기 때문에 보안사고의 위험이 증가한다. 공용계정 및 휴면계정이 존재하는 시스템은 침해사고 및 장애 발생 시 사후 추적이 어렵다. 공용 계정의 사용을 금지하고, 사용하지 않는 계정은 즉시 삭제하도록 계정 관리를 해야 한다.		
진단기준	양호	불필요한 공용계정 및 휴면계정을 제거하거나 관리하는 경우	
	취약	불필요한 공용계정 및 휴면계정을 제거하거나 관리하지 않는 경우	
진단방법	■ 보안장비에서 제공하고 있는 계정 메뉴에서 계정 및 담당자 확인		
조치방법	■ 공용계정 및 불필요한 계정 제거 1) 시스템에 대해 1인 1계정 사용을 원칙으로 하고 공용으로 사용하는 계정 사용 금지 2) 사용하지 않는 계정은 삭제하고 시스템 접근 이력을 관리하여 명시적인 계정 관리 설정 ※ 시스템이 아닌 사람을 중심으로 하는 통합된 계정관리가 중요함		
비고			

나. 접근 관리

진단항목	NF-05. 정보보호시스템 원격 관리 접근 통제		취약도	상
항목설명	대부분 보안 장비는 원격에서 관리하기 위한 관리자 접근방법을 제공하고 있어 이에 대한 통제가 필요하다. 일반적으로 IP 단위로 접근제한을 하여 보안 장비에 대한 관리자 접근을 통제한다. 보안 장비에서 제공하는 관리자 접근제한 기능을 통해 관리자 단말기 또는 콘솔 장비의 IP를 등록하고 접근을 제한할 수 있다.			
진단기준	양호	원격 관리 시 관리자 IP만 접근 가능하도록 설정한 경우		
	취약	원격 관리 시 관리자 IP만 접근 가능하도록 설정하지 않은 경우		
진단방법	▪ 보안장비에서 제공하고 있는 메뉴에서 접속 IP나 계정 제한 확인			
조치방법	▪ 특정 IP 및 계정에서만 접속할 수 있도록 설정			
비고				

진단항목	NF-06. 정보보호시스템 보안 접속	취약도	상
항목설명	암호화되지 않은 데이터 전송 시 *스니핑 등을 통한 정보유출 위험이 존재하므로 SSL 인증 등의 암호화 접속을 통해 장비에 접속하도록 설정해야 한다. * 스니핑(Sniffing): 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러다니는 트래픽을 엿듣는 도청장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말한다.		
진단기준	양호	보안장비 접속 시 암호화 통신을 하는 경우	
	취약	보안장비 접속 시 암호화 통신을 하지 않는 경우	
진단방법	▪ https 또는 ssh를 통한 접속 확인 1) https를 통한 접속 확인 2) ssh를 통한 접속 확인		
조치방법	▪ 보안장비 접속 시, 가능하다면 *SSL 등의 암호화 접속 활용(제품마다 상이하므로 벤더 사에 문의) ※ SSL(Secure Socket Layer): 인터넷상에서 정보를 암호화하여 송/수신하는 프로토콜. 현재 인터넷에서 널리 쓰이고 있는 WWW, FTP 등의 데이터를 암호화하여, 프라이버시에 관한 정보나 신용카드 번호, 기업 비밀 등을 안전하게 송/수신 할 수 있음		
비고			

진단항목	NF-07. Session timeout 설정		취약도	상
항목설명	외부에서의 서비스 사용자가 일정 시간 동안 통신이 없을 시 해당 세션을 종료시키는 것으로 각 TCP/UDP 등에 대하여 time out을 설정해야 한다. 이로 인해 불필요한 session을 정리하고 보안을 강화할 수 있다.			
진단기준	양호	Session Timeout 시간을 600초 이하로 설정한 경우		
	취약	Session Timeout 시간을 600초 이하로 설정하지 않은 경우		
진단방법	▪ 관리자의 부재 시 불법 사용자들의 접속을 차단하기 위해서 관리자의 logout을 하지 않고 자리를 비우는 실수에도 자동적으로 logout 사용여부를 확인			
조치방법	▪ 보안장비가 제공하는 Timeout 기능 활성화			
비고				

다. 패치 관리

진단항목	NF-08. 벤더에서 제공하는 최신 업데이트 적용	취약도	상
항목설명	보안장비는 지속적으로 취약점이 알려지고 있으며 이에 대한 패치도 지속해서 제공되고 있으므로 보안장비의 보안수준을 높이고 성능 및 기능 향상을 위해서는 버전 업그레이드 및 보안 패치 작업을 수행하여 최신 취약점을 보완하는 작업이 필요하다.		
진단기준	양호	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있을 경우	
	취약	패치 적용 정책을 수립하여 주기적으로 패치를 관리하고 있지 않을 경우	
진단방법	▪ 자동 업데이트 기능 설정이 활성화 되어 있는지 확인 ▪ 정기점검 수행 여부와 크리티컬 이슈 발생 시 즉각적으로 패치를 진행하는지 확인 필요함		
조치방법	▪ 벤더사에 문의하여 자동 업데이트 기능 설정		
비고			

라. 기능 관리

진단항목	NF-09. 정책 관리		취약도	상
항목설명	관리자마다 각기 다른 관리 방법을 적용한다면 보안 장비의 정책은 다양한 버전이 존재하게 되고 관리자가 퇴사하거나 팀을 옮기게 될 경우, 이는 보안 장비 정책 보안성에 심각한 문제를 발생할 수 있으므로 표준 절차와 지침이 필요하다. 관리자에 따라서 개별적인 정책 관리 방법이 존재하지 않도록 표준적인 정책 관리와 지침이 필요하다.			
진단기준	양호	정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거하는 경우		
	취약	정책에 대한 주기적인 검사로 미사용 및 중복된 정책을 확인하여 제거하지 않은 경우		
진단방법	▪ 정책에 대한 주기적인 검사로 미사용 & 중복된 정책을 확인			
조치방법	▪ 정책 적용 시 아래와 같이 적용 1) 침입차단 시스템의 정책 관리 시, 객체관리는 관리자의 편의로 발생할 수 있는 오류를 최소화하기 위하여 기존 IP 대신에 관리자가 인식하기 쉬운 "객체 명"을 사용함. "객체 명"을 이용해서 관리자가 숫자(IP ADDRESS)의 오타나 서버의 착각을 최대한 방지 할 수 있음. 2) 객체를 관리할 때 가장 중요한 것은 관리자가 직관적으로 인식할 수 있도록 명명하는 것이며, 다른 관리자들의 혼동을 최소화할 수 있는 "표준 명명 규약"이 있어야 함. 3) 객체 관리와 더불어 정책의 입력 시, 서로 연관성이 있는 서비스들은 비슷한 카테고리로 분류하여 정책 점검 시 검색이 쉬워야 하고 관리자마다 같은 정책 내의 세부 규칙을 여러 곳에 분산시키지 않도록 해야 함. 추가로 정책내의 세부 규칙에 대한 카테고리가 존재하는지, 그리고 관리자가 다르더라도 그 카테고리 내에서 정렬 규칙이 존재하는지 등에 대해서 "정책 명명 방식"의 차이가 최소화되도록 해야 함. 즉, 어떤 관리자가 정책을 변경하더라도 같은 방법으로 정책을 변경할 수 있는 정책 변경/관리 세부 지침이 존재해야 함. 4) 정책 입력 시, 정책이 침입차단시스템의 성능과의 관계를 고려하였는가에 대해서 점검해야 함. 일반적으로 가장 정책의 적용을 많이 받게 되는 공개 서비스군 카테고리가 정책의 최고 상단에 존재하고 그 다음으로 접근이 많은 서비스군 카테고리가 존재하는 것이 바람직함.			
비고				

진단항목	NF-10. 최소한의 서비스만 제공		취약도	상
항목설명	방화벽은 기본적으로 all deny 설정이다. 이와 더불어 허용할 포트와 IP만 추가함으로써, 관리 포인트도 적어지게 됨. 필요 없는 포트는 차단되어 침입자의 침입 가능성을 낮출 수 있다.			
진단기준	양호	all deny 설정을 하고, 방화벽에 최소 서비스만 허용할 경우		
	취약	all deny 설정이 되어 있지 않거나, 방화벽에 불필요한 서비스를 허용할 경우		
진단방법	▪ 방화벽에서 허용되지 않은 포트 접속 확인			
조치방법	▪ 아래의 보안설정방법에 따라 설정을 변경 방화벽 기본 정책인 all deny에 최소 서비스만 허용 확인 (허용된 IP와 서비스 포트만 오픈, IP 및 서비스 ANY 적용 금지)			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">NF-11. 이상 징후 탐지 경고 기능 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">유해 트래픽은 정상적인 네트워크 운용 및 서비스에 지장을 주는 악의적인 공격성 패킷과 바이러스 패킷으로, 망 운영에 치명적인 장애를 유발하며 동시 다발적인 급속한 확산이 특징이다. 유해 트래픽의 위험성은 지속적인 증가 추세이며 트래픽 관리는 망운용에 필수적인 요소로 부각되고 있다. 24시간 모니터링을 통한 감시가 여건상 어려울 경우 이메일이나 SMS를 통한 경고 기능 설정으로 대체한다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">이상 징후 탐지 시 관리자에게 이메일이나 SMS로 통보되는 경우</td></tr>
<tr><td>취약</td><td colspan="3">이상 징후 탐지 시 관리자에게 이메일이나 SMS로 통보되지 않는 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">▪ 정보보호시스템의 인터뷰 및 UI 설정을 통해 정보보호시스템 이상 시 알람 기능을 설정하고 있는지 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">▪ 24시간 모니터링을 통한 감시가 여건상 어려울 경우 이메일이나 SMS를 통한 경고 기능 설정으로 대체</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

진단항목	NF-12. 장비 사용량 검토		취약도	상
항목설명	장비 사용량에 대한 검토로 인해 네트워크 트래픽의 수준을 파악하게 되고, 그에 따른 가용성 향상을 고려해 볼 수 있다. 보안장비의 Web Dash Board를 모니터링 한다.			
진단기준	양호	장비 사용량을 정기적으로 모니터링 및 검토할 경우		
	취약	장비 사용량을 정기적으로 모니터링 및 검토하지 않을 경우		
진단방법	▪ 보안장비의 실시간 알람, 이메일, SMS 경고 기능 설정 확인			
조치방법	▪ 보안장비의 Web Dash Board 모니터링			
비고				

진단항목	NF-13. SNMP 서비스 확인		취약도	상
항목설명	SNMP는 UDP 프로토콜을 사용하기 때문에 SNMP 서비스를 활성화하면 각종 공격, 예를 들어 DOS 공격에 취약해질 뿐만 아니라 보안장비의 성능저하, 크래쉬, 리로드 등의 위험이 존재한다. 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 Community String을 유추가 불가능하게 설정한다.			
진단기준	양호	SNMP 서비스를 불필요하게 사용하지 않는 경우		
	취약	SNMP 서비스를 불필요하게 사용 할 경우		
진단방법	■ 보안장비의 SNMP 설정 메뉴에서 확인			
조치방법	■ 불필요하다면 SNMP 서비스를 중지하고, 관리를 위해 NMS 솔루션과의 연동이 필요하다면 SNMP 설정			
비고				

<table>
<tr><td>진단항목</td><td colspan="2">NF-14. SNMP Commuity String 복잡성 설정</td><td>취약도</td><td>상</td></tr>
<tr><td>항목설명</td><td colspan="4">SNMP의 Public Private와 같은 디폴트 Community String이 변경되지 않고 그대로 사용될 경우, 악의적인 사용자가 장비 설정을 쉽게 변경(RW)하여 중요 시스템 정보가 노출될 수 있는 위험이 존재한다. 그러므로 추측하기 어려운 Community String으로 변경하는 작업이 필요하다.</td></tr>
<tr><td rowspan="2">진단기준</td><td>양호</td><td colspan="3">SNMP 서비스를 사용하지 않거나, 유추하기 어려운 community string을 설정한 경우</td></tr>
<tr><td>취약</td><td colspan="3">디폴트 community string을 변경하지 않거나, 유추하기 쉬운 community string을 설정한 경우</td></tr>
<tr><td>진단방법</td><td colspan="4">■ 정보보호시스템의 보안장비의 SNMP 설정 메뉴에서 커뮤니티 스트링 확인한다. 어플라이언스 제품을 제외한 소프트웨어 방식의 시스템인 경우 자체 OS 취약점 점검이 이루어지고 있는지 확인</td></tr>
<tr><td>조치방법</td><td colspan="4">■ 아래와 같이 SNMP Community String 변경
1) 보안 장비는 SNMP로 취약성이 존재하므로 누구나 추측하기 어렵고 의미가 없는 문자열, 영문자 혼합으로 변경 권고
(SNMP 버전은 v1, v2, v3가 존재하는데 v1, v2는 암호화가 되어 있지 않고 텍스트 열로 전송되지만 v3는 암호화가 설정되어 있고 해쉬 값으로 전송)
2) 보안장비의 SNMP 설정에서 커뮤니티 이름 변경</td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

클라우드 취약점 점검 가이드