



안전한 데이터 보호를 위한

NAS 보안 가이드

2024. 2.



과학기술정보통신부



한국인터넷진흥원





유의사항

본 가이드는 NAS(Network Attached Storage) 장비의 보안수준 제고를 위해 발간된 보고서로 수록된 점검 방법은 일반적인 취약점 점검 수행 중 활용할 수 있는 참조의 대상일 뿐, 절대적이지 않습니다. 더욱이 점검 대상의 제조사, 세부 버전에 따라 진단 방법은 언제든지 변경될 수 있습니다. 따라서 본 가이드에 수록된 내용 이외에도 다양한 진단 방법을 사용하여 취약점 점검을 수행하시기 바랍니다.

본 가이드에 수록된 진단 결과에 대한 판단기준은 최종적으로 운전자 또는 담당자에 의해 결정되어야 하며, 예를 들어 본 가이드에 수록된 판단기준에 의하여 취약판단을 받게 되어도 그 위험을 부담할 수 있는 합당한 보안조치와 근거를 수반하고 있다면 양호로 판단할 수 있습니다.

본 가이드에 수록된 버전 및 조치 사례는 각 제조사의 특정 운영체제 및 소프트웨어를 활용하여 실증되었으며, 세부 정보는 제조사별 보안가이드 내 명시하였습니다. 본 가이드에 대한 개선의견은 항상 소중히 듣겠습니다.

CONTENTS

01

개요

08

1.1 배경 및 필요성	08
1.2 NAS 서버 개요	08
1.3 NAS 서버 주요 기능	10

02

NAS 서버 보안

12

2.1 NAS 서버 보안의 중요성	12
2.2 NAS 서버 보안 위협	12
2.3 NAS 서버 보안취약점	14
2.4 NAS 서버 대상 해킹 공격 현황	15
2.5 NAS 서버 대상 랜섬웨어 동향	17

03

NAS 보안수칙

20

3.1 암호화 사용	20
3.2 접근제어와 권한관리	20
3.3 네트워크 보안	20
3.4 펌웨어 및 소프트웨어 업데이트	20
3.5 백업 및 복원 전략	21
3.6 감사 로깅과 모니터링	21
3.7 업데이트된 안전한 앱 사용	21
3.8 랜섬웨어 방지	21

04

NAS 제조사별 보안 가이드

24

4.1 안내 사항	24
4.2 유의 사항	24
4.3 실증 장비	24



05

Synology NAS 보안가이드

26

5.1 진단 항목	26
5.2 계정 관리	28
5.3 접근 관리	40
5.4 패치 및 보안 관리	50
5.5 로그 및 백업 관리	64
5.6 서비스 관리	72

06

QNAP NAS 보안가이드

80

6.1 진단 항목	80
6.2 계정 관리	82
6.3 접근 관리	93
6.4 패치 및 보안 관리	104
6.5 로그 및 백업 관리	116
6.6 서비스 관리	121

07

ipTIME NAS 보안가이드

130

7.1 진단 항목	130
7.2 계정 관리	132
7.3 접근 관리	138
7.4 패치 및 보안 관리	143
7.5 로그 및 백업 관리	148
7.6 서비스 관리	154

08

맺음말

160



개요

1.1 배경 및 필요성	08
1.2 NAS 서버 개요	08
1.3 NAS 서버 주요 기능	10

01

01

개요



1.1 배경 및 필요성

한국인터넷진흥원에서는 정부의 랜섬웨어 대응 강화방안(관계부처 합동, 21.8)의 일환으로 중소기업의 정보시스템 보안수준 제고를 위해 2022년부터 기업에서 보유하고 있는 주요 서버에 대한 원격보안점검 서비스(이하 ‘내서버 돌보미 서비스’)를 제공하고 있다. 점검 결과 다수의 중소기업에서 랜섬웨어 공격 예방을 위한 데이터 백업 매체로 NAS 장비를 도입하여 운영하고 있음을 확인하였다.

NAS 서버의 주된 목적은 데이터 백업을 위한 스토리지 장치로 활용되고 있지만, 단순히 파일 서버 역할을 넘어 웹 호스팅, 웹 어플리케이션, 미디어 스트리밍, 가상화 및 컨테이너 관리도구 등 다양한 서비스와 설치형 패키지를 지원하고 있다. 이와 같은 이유로 기업뿐만 아니라 많은 사람들이 개인용 NAS를 구매하여 이용하고 있다. NAS 서버는 기업(또는 개인)의 중요 정보를 저장하고 공유하고 있기 때문에 해커들의 주요 공격 대상이 되고 있으며, NAS 서버를 대상으로 하는 특화된 랜섬웨어도 발견되고 있다.

따라서 NAS 서버는 기업(개인)의 주요 자산으로서 철저한 보안 관리가 필요하다. 이에 본 가이드에서는 NAS 서버에서 발생할 수 있는 주요 보안위협 및 보안수칙을 설명하고, 중소기업에서 많이 사용하고 있는 NAS 제품군에 대한 세부 보안점검 항목을 소개할 예정이다.

1.2 NAS 서버 개요

NAS (Network-Attached Storage) 장비는 네트워크에 연결되어 중앙 집중식으로 데이터를 저장하고 공유하는 데 사용되는 스토리지 장치이다. NAS 장비는 일반적으로 별도의 서버나 컴퓨터와는 다르게 전용 스토리지 장치로 사용되며 파일 서버 역할을 하며 데이터를 다양한 디바이스에서 액세스하도록 허용한다.

NAS 제조사(Synology, QNAP, Iptime, Western Digital 등)에서는 이용자 편의를 위해 NAS 전용 운영체제 및 관리 플랫폼을 개발하여 제공하고 있다. 관리 플랫폼은 이용자에게 친화적인 인터페이스를 제공하여 파일 관리, 백업 및 복원 관리, 앱 센터, 미디어 스트리밍, 원격 액세스, 보안 및 권한 관리 등 주요 서비스를 편리하게 이용 할 수 있도록 지원한다.

대표적인 NAS 장비 제조기업



1.3 NAS 서버 주요 기능

데이터 저장과 공유

NAS의 주요 목적 중 하나로 데이터를 안전하게 저장하고 필요한 사용자 또는 장치와 데이터를 공유하는데 사용된다. 또한 여러 사용자가 중요 문서, 사진, 비디오 및 기타 파일에 접근하고 공동 작업을 할 수 있다.

백업 및 복원

NAS는 중요한 데이터를 백업하고 장애 시 복원할 수 있는 중요한 백업 도구로 사용되며, 자동 백업 스케줄 설정을 통해 데이터 손실을 예방 할 수 있다.

미디어 스트리밍

NAS는 미디어 스트리밍 서버로 사용될 수 있다. 음악, 사진 및 비디오 파일을 NAS에 저장하고 다양한 장치에서 스트리밍할 수 있다. 이를 통해 다른 미디어 장치, 스마트 TV, 태블릿, 노트북 등 어디서든지 멀티미디어 콘텐츠를 공유하고 스트리밍할 수 있다.

원격 접근

NAS는 다양한 방식의 원격 액세스 기능을 제공하여 어디서나 데이터에 접근할 수 있다. 도메인을 통한 접근 방식 외에도 FTP, SSH, SMB, NFS, AFP 등 다양한 방식의 원격 서비스를 통해 외부 네트워크에서 NAS에 저장된 파일을 검색, 다운로드 및 업로드를 할 수 있다.

그 밖의 기능

일부 제조사의 NAS 서버에서는 다양한 추가 기능을 제공한다. 기본 제공 또는 추가 패키지를 통해 웹 서버, 데이터베이스, 스마트 홈 자동화, 보안 카메라 관리 등 사용자가 NAS 서버를 다목적으로 활용 할 수 있도록 지원한다.

예를 들어 WordPress, Joomla, Wiki과 같은 콘텐츠 관리 시스템(CMS)을 설치하여 웹사이트를 만들고 운영할 수 있으며, PHP, MySQL 등의 웹 개발 스택을 지원하여 사용자 지정 웹 애플리케이션을 구축할 수도 있다. 또한 이메일 서버 호스팅, VPN 서버 구축, 가상화 및 컨테이너 관리 등 엔터프라이즈 애플리케이션 운영을 통해 기업 프로세스를 자동화하고 데이터베이스를 유지 관리할 수 있다.

NAS 서버 보안

2.1 NAS 서버 보안의 중요성	12
2.2 NAS 서버 보안 위협	12
2.3 NAS 서버 보안취약점	14
2.4 NAS 서버 대상 해킹 공격 현황	15
2.5 NAS 서버 대상 랜섬웨어 동향	17

02

NAS 서버 보안



2.1 NAS 보안의 중요성

NAS 서버 보안은 중요한 데이터의 보호, 개인 정보 보호, 랜섬웨어 공격 방지, 규정 준수 및 비즈니스 연속성 유지를 위해 필수적이다. 먼저 NAS 시스템은 기업(또는 개인)의 중요 데이터를 저장하고 관리하는데 사용된다. 이 데이터에는 개인 정보, 회사 문서, 미디어 파일 및 중요한 업무 정보가 포함될 수 있다. 따라서 NAS 보안의 목적은 데이터 유출, 위변조 같은 데이터 손실 위험으로부터 보호하는 것이 핵심이다.

또한 NAS 보안 강화를 통해 저장된 데이터가 손상되거나 수정되지 않도록 보호하여야 한다. 만약 데이터의 무결성, 신뢰성이 깨진다면 기업의 비즈니스 연속성에도 큰 문제가 발생할 수 있다. 따라서 NAS 장비를 도입하여 운영 중이라면 중요한 자산으로 등록하여 관리하여야 한다. 보안 정책을 수립하고 주기적인 보안 업데이트 및 패치와 사용자 교육, 모니터링이 필요하다. 이를 통해 데이터를 안전하게 보호하고 잠재적인 보안 위험으로부터 위험을 최소화 하여야 한다.

2.2 NAS 서버 보안 위협

근래의 NAS 서버는 단순히 중요 데이터 저장, 백업 기능을 넘어 각 NAS 제조사에서 제공하는 다양한 서비스로 인해 외부에 공개되어 있는 경우가 많다. 따라서 다양한 요인에 의해 공격 대상이 될 수 있으며 보안 위협에 노출될 수 있다. 특히 NAS를 대상으로 하는 랜섬웨어가 등장하고 있으며, 각 제조사 소프트웨어 취약점이 공개되고 있다. 다음 제시되는 내용은 NAS 장비에서 발생할 수 있는 보안위협이다.

2.2.1 악성코드(랜섬웨어 등) 감염

랜섬웨어와 같은 악성 소프트웨어가 NAS에 설치되어 데이터를 손상시키거나 암호화할 수 있다. 특히 NAS 서버는 파일을 중앙에서 관리하므로 랜섬웨어 공격의 주요 대상이 될 수 있다. 랜섬웨어는 데이터를 암호화하고 금전을 요구하며, 데이터의 손실을 초래할 수 있다.

2.2.2 데이터 유출

랜섬웨어 공격 외에도 NAS에 저장된 데이터가 노출되거나 유출될 수 있다. 취약한 암호 사용, 업데이트 부재로 인한 취약점 악용 등 악의적인 사용자가 무단으로 접근하여 데이터를 탈취하는 위험이 있다. 이러한 데이터 유출은 민감한 정보의 노출을 초래하고 개인 정보 침해로 이어질 수 있다.

2.2.3 데이터 위변조

데이터 유출과 마찬가지로 이유로 악의적 사용자에게 의해 중요자료의 데이터 위변조로 인한 데이터 손실을 초래할 수 있다. 데이터 손실에 따른 데이터 신뢰성과 무결성이 무너질 수 있으며 이는 심각한 업무 중단을 초래 할 수 있다.

2.3 NAS 서버 보안 취약점

NAS 서버의 보안 위협을 발생시키는 여러 보안 취약점이 존재하며 이를 효과적으로 해결하지 못하면 중대한 문제가 발생할 수 있다. 암호 사용의 취약성, 데이터 암호화 부재, 미처리된 공개 포트, 그리고 사용자 실수로 인한 악성코드 감염 등 여러 측면에서 보안 취약점이 발견될 수 있으며 이러한 문제들은 심각한 보안 위협으로 이어질 수 있어 사용자 및 기업은 이에 대한 강력한 대응이 필요하다.

취약점	상세내용
 약한 인증 및 취약한 비밀번호 사용	사용자 및 관리자의 암호가 간단하거나 약하게 설정된 경우, 공격자가 더 쉽게 시스템에 접근할 수 있다.
 암호화 부재	데이터가 암호화되지 않는 경우, 물리적 또는 원격 공격자가 데이터를 읽을 수 있다.
 소프트웨어 취약점 및 부족한 보안 업데이트 관리	NAS 시스템의 운영 체제, 앱 및 소프트웨어에 취약점이 발견될 수 있으며, 악용될 가능성이 있다. 보안 패치와 업데이트를 적용하지 않으면 취약점이 그대로 남아있을 수 있다.
 접근 권한 및 파일 공유 설정 오류	접근 권한이 부적절하게 설정되거나 최소한으로 관리되지 않는 경우, 허가되지 않은 사용자가 데이터에 무단으로 접근할 수 있다. 파일 공유 설정이 부적절하게 구성되어 있는 경우, 중요한 데이터가 무단으로 공유될 수 있다.
 미처리된 공개 포트	미처리된 공개 포트에 의해 접근 제어가 부족하게 되어 공격자의 진입이 가능해질 수 있다.
 사용자 실수로 인한 악성코드 감염	사용자 부주의로 인해 악성 소프트웨어가 다운로드되거나 설치될 수 있으며, 데이터 손실 및 네트워크 감염의 위험을 초래할 수 있다. 특히 사용자를 속여 악성 링크를 클릭하게 만들거나 인증 정보를 빼내는 사회 공학 기술이 사용될 수 있다.

2.4 NAS 서버 대상 해킹 공격 현황

NAS 장비를 대상으로 한 해킹 공격의 가장 큰 목적은 NAS에 저장된 기업의 중요한 데이터를 탈취하거나 랜섬웨어를 감염시켜 금전을 요구하는 것이다. 이를 위해 공격자는 무차별 대입 공격 등 약한 강도의 암호를 크래킹하여 접근권한을 획득하거나, NAS 장비의 하드웨어 또는 소프트웨어의 취약점을 이용하여 악성코드를 주입하거나 권한을 획득할 수 있다. 이외에도 관리자를 대상으로 악성 첨부파일 또는 링크가 포함된 해킹 메일을 발송하여 인증 정보를 빼내는 등 사회 공학 기술이 사용될 수 있다.

※ NAS 서버 대상 해킹 공격 사례

전 세계 웨스턴 디지털 NAS 기기, 데이터 삭제 공격 받아...피해 속출(21.6.28)

전 세계 웨스턴 디지털 마이 북 라이브 NAS 기기 다수가 공장 초기화되면서 파일이 삭제되고 앱을 통해 로그인도 불가능해지는 대형 사고가 발생했다. 이번 사고를 통해 사용자 일부는 PhotoRec 파일 복구 툴을 사용해 일부 파일을 성공적으로 복구할 수 있었다고 전했지만, 다수의 많은 사용자들이 복구에 실패했다. 보안전문가들은 웨스턴 디지털 서버가 해킹을 당해 공격자가 연결된 모든 기기를 공장 초기화한 것이라며 패치되지 않은 취약점을 악용한 공격으로 추정하고 있다.

※ 출처 : 데일리시큐(<https://www.dailysecu.com>)

대학·기업 원격저장장치(NAS)도 해킹 피해..."연구·특허 자료 유출 우려" (21.12.7, YTN)

원격저장장치를 사용해 연구나 특허, 업무 자료를 공유하는 대학과 기업이 늘어나고 있다. 이렇게 민감한 내부 자료가 주로 담긴 NAS 장비가 최근 해커들의 공격 목표가 되었다. 국내 한 업체가 생산한 NAS 장비가 해외 기관 대상 해킹 공격에 동원됐다는 사실이 통보되었다. 해커들은 NAS 장비에 접속해 관리자 권한을 빼앗은 뒤 장비를 숙주 삼아 해외 기관 서버를 공격한 것으로 추정된다. 장비가 출고될 때 설정된 기본 아이디와 비밀번호를 그대로 사용하던 기기가 주요 목표가 되었으며, 해당 업체가 생산한 NAS 장비 3만여 대를 전수 조사한 결과 4천여 대 정도가 초기 설정 값을 바꾸지 않아 해킹 위험에 그대로 노출되어 있었다.

※ 출처 : YTN(<https://www.ytn.co.kr>)

큐냅과 시놀로지의 NAS 장비들에서 다수 취약점 발견돼(22.5.2)

NAS 장비 제조사인 큐냅(QNAP)과 시놀로지(Synology)가 다량의 취약점 정보를 공개했다. 자사 제품에 통합된 오픈소스 파일 서버에서 발견된 것들이다. 일부는 원격 코드 실행을 가능하게 하며, 따라서 위험하다. 문제의 오픈소스 파일 서버는 애플 파일 프로토콜(Apple File Protocol)의 오픈소스 버전인 네타토크(Netatalk)이다. 이번에 발견된 네타토크 취약점의 영향을 받는 건 시놀로지와 큐냅 외에 웨스턴디지털(Western Digital)이라는 업체도 있다

※ 출처 : 보안뉴스(<https://www.boannews.com>)

새로운 Deadbolt 랜섬웨어 공격에 사용되는 QNAP 패치 제로데이(22.9.5)

QNAP은 Photo Station의 제로데이 취약점을 악용한 지속적인 DeadBolt 랜섬웨어 공격에 대해 경고하였다. DeadBolt 랜섬웨어 집단은 인터넷에 노출된 NAS 장치의 제로데이 취약점을 이용하여 2022년 1월부터 NAS 장치를 표적으로 삼아 왔다. 대부분의 공격에서 DeadBolt는 작동하는 암호 해독기에 대한 대가로 영향을 받은 사용자에게 1000달러가 조금 넘는 금액을 요구하였다. QNAP에서는 NAS가 인터넷에 직접 연결되지 않도록 강력히 조치하고, 사용자는 QNAP에서 제공하는 myQNAPcloud Link 기능을 사용하거나 VPN 서비스를 활성화할 것을 권고하였다.



※ 출처 : 블리핑컴퓨터(<https://www.bleepingcomputer.com>)

시놀로지 NAS 노리는 무차별 공격 주의보(22.10.12)

시놀로지 NAS(네트워크 저장장치)를 대상으로 한 대규모 공격이 진행되고 있어 해당 제품 사용자들의 주의가 요구된다. 국내뿐만 아니라 일본이나 중국 등 다양한 접속 IP를 통해 시놀로지 NAS용 운영체제 'DSM'(디스크스테이션매니저) 침입 시도가 이어지고 있다. 공격자 그룹은 외부 접속을 위한 페이지에 접근한 다음 초기 설정 과정에서 관리자용 ID로 쓰이는 'admin' 계정에 비밀번호를 달리하며 접속을 시도하였다.

※ 출처 : 지디넷코리아(<https://zdnet.co.kr>)

2.5 NAS 서버 대상 랜섬웨어 동향

최근 몇 년 동안 랜섬웨어 공격이 기술적으로 진보하면서, NAS 장비를 향한 공격 또한 빈번하게 발생하고 있다. 특히, SynoLocker, QLocker, eCh0raix, 그리고 DeadBolt와 같은 랜섬웨어들은 대중적인 NAS 제조사들의 제품을 타겟으로 하고 있다. 이에 따라 사용자들은 보다 높은 수준의 보안 조치와 업데이트가 필요하다.

※ 랜섬웨어(Ransomware)는 악의적인 소프트웨어로, 컴퓨터 사용자의 파일을 암호화하거나 컴퓨터 자체를 잠금 상태로 만들어 사용자에게 금전을 요구하는 악성 프로그램으로 주로 금전적 이익을 목적으로 하는 사이버 범죄자들에 의해 수행되며, 흔히 악성 이메일, 피싱 공격, 혹은 웹사이트 방문을 통해 사용자의 시스템으로 침입한다.

SynoLocker 랜섬웨어

2014년 8월 발견된 Synology NAS를 대상으로 공격하는 랜섬웨어. 공격자는 Synology에서 이용자 편의를 위해 제공하는 웹 기반 운영체제인 Disk Station Manager(DSM)의 취약점을 이용하여 SynoLocker 랜섬웨어를 감염시켜 NAS에 저장된 파일을 암호화한다. 또한 Telnet 및 SSH 서비스를 비활성화시켜 시스템 접근을 불가능하게 한다. SynoLocker 랜섬웨어는 2013년 전세계 인터넷 사용자에게 막대한 영향을 끼친 CryptoLocker 랜섬웨어와 유사하게 제작되었으며, 감염 후 관리자 웹 페이지를 이용해 Tor 네트워크에 접근하여 비트코인(몸값을 요구한다.)

※ 패치된 버전, 감염 증상, 업데이트 방법

업데이트된 버전

- DSM 4.3-3827 이상
- DSM 4.2-3243 이상
- DSM 4.0-2259 이상
- ※ DSM 3.X 이전 버전 및 5.X 이상 버전은 영향 없음

QLocker 랜섬웨어

2021년 4월 발표된 랜섬웨어로 대만의 NAS 제조기업인 QNAP社의 제품을 공격 대상으로 한다. 공격자는 QNAP에서 제공 중인 소프트웨어 3종(멀티미디어 콘솔, 미디어 스트리밍 애드온, 하이브리드 백업 싱크 앱)의 취약점을 이용하였다. 최초 공격 후 QLocker 랜섬웨어에 감염된 장비에 저장되어 있는 파일을 7-zip(*.7z) 파일로 암호화하여 암호화 시킨다. 공격자는 복호화 키를 제공하는 댓가로 0.01비트코인(당시 약 500달러 상당)을 요구하였다. 당시 공격자에게 지불된 피해액은 알려진 규모만 35만불 이상이라고 밝혀졌다. 이후 2022년에는 QLocker2라는 이름으로 변종 랜섬웨어가 등장하기도 하였다.

※ 취약점 코드(CVE) : CVE-2020-2509, CVE-2020-36195, CVE-2021-28799

업데이트된 버전

- HBS 3 v16.0.0415 (QTS 4.5.2용) 이상
- HBS 3 v3.0.210412 (QTS 4.3.6용) 이상
- HBS 3 v3.0.210411(QTS 4.3.3 및 4.3.4용)
- HBS 3 v16.0.0419(QuTS hero h4.5.1 및 QuTScloud c4.5.1~c4.5.4용) 이상
- ※ HBS 2와 HBS 1.3 버전은 영향 없음

eCh0raix 변종 랜섬웨어

2021년 8월 Synology社와 QNAP社를 모두 겨냥하는 변종 랜섬웨어 eCh0raix가 발견되었다. eCh0raix 랜섬웨어는 2016년 최초 발견된 이후로 꾸준히 발전해왔다. 변종 eCh0raix 랜섬웨어는 앞서 언급된 CVE-2021-28799 취약점을 악용하였으며 비교적 간단한 코드로 Go 언어로 제작되었다. 감염 후에는 AES 암호화 알고리즘을 이용해 파일을 암호화하고 감염된 파일에는 .encrypt 확장자가 추가 된다. 또한 공격자는 감염된 NAS를 이용하여 시스템 공격에 이용할 악성 봇넷을 생성하기도 하였다. 당시 조사된 결과에 따르면 위험에 노출된 NAS 장비가 최소 25만대에 이른다고 밝혀졌다.

업데이트된 버전

- CVE-2021-28799 취약점이 패치된 펌웨어 및 소프트웨어 사용

DeadBolt 랜섬웨어

2022년 1월 발견된 랜섬웨어로 QNAP NAS를 공격 대상으로 한다. DeadBolt 랜섬웨어는 QNAP에서 사진 관리를 위해 제공하는 Photo Station 소프트웨어의 취약점을 악용하였으며, 랜섬웨어에 감염되면 저장된 데이터는 AES128 알고리즘으로 암호화하고 파일명에 .deadbolt 확장자가 추가된다. DeadBolt 랜섬웨어 공격이 최고조에 달했을 때 인터넷에 있는 13만대의 대상 장비중 4,988대의 장비가 감염되기도 하였다. DeadBolt 랜섬웨어는 이후에도 ASUSTOR社의 NAS장비를 공격 대상으로 피해를 끼치기도 하였다.

업데이트된 버전

- QTS 5.0.0.1891 빌드 20211221 이상
- QTS 4.5.4.1892 빌드 20211223 이상
- QuTS hero h5.0.0.1892 빌드 20211222 이상
- QuTScld c5.0.0.1919 빌드 20220119 이상

NAS 보안수칙

3.1 암호화 사용	20
3.2 접근제어와 권한관리	20
3.3 네트워크 보안	20
3.4 펌웨어 및 소프트웨어 업데이트	20
3.5 백업 및 복원 전략	21
3.6 감사 로깅과 모니터링	21
3.7 업데이트된 안전한 앱 사용	21
3.8 랜섬웨어 방지	21

03

NAS 보안수칙



3.1 암호화 사용

NAS 서버에 저장되는 데이터를 암호화해서 사용한다. 디스크 레벨 암호화 및 파일 레벨 암호화를 활용하여 데이터의 안전성을 보장할 수 있다. 또한 데이터 전송 중에도 SSL/TLS 암호화를 사용하여 데이터를 암호화하여야 한다. 데이터가 암호화 되지 않는 경우 물리적 또는 원격 공격자가 데이터를 쉽게 읽을 수 있다.

3.2 접근 제어와 권한 관리

사용자 및 그룹별로 적절한 접근 권한을 설정하여 사용하고, 사용자별 필요한 권한만 부여하는 최소 권한 원칙을 준수한다. 이를 통해 주요 데이터에 대한 접근을 엄격하게 제한하고, 강력한 암호정책을 적용하여 복잡한 비밀번호 사용을 강제하여야 한다.

3.3 네트워크 보안

NAS 장비를 네트워크에서 안전하게 보호하기 위해서 불필요한 서비스 포트를 차단하고, 방화벽을 설정하여 외부에서의 불필요한 접근을 제한해야 한다. 또한 VPN(Virtual Private Network)을 사용하여 안전한 원격 액세스를 활성화하고, 데이터 인증 및 암호화를 통해 보호하여야 한다. 필요시 가상 사설 네트워크(VPN)를 사용하여 내부 트래픽 분리를 구현할 수 있다.

3.4 펌웨어 및 소프트웨어 업데이트

NAS 서버의 펌웨어, 운영 체제 및 소프트웨어를 주기적으로 업데이트 하여 최신 버전을 유지해야 한다. 또한 각 제조사 및 소프트웨어 공급업체에서 제공하는 보안 패치를 즉각 적용하여 취약점을 악용한 해킹 공격을 예방하여야 한다.

3.5 백업 및 복원 전략

NAS에 저장된 데이터도 정기적으로 백업하여 데이터 손실을 방지하여야 한다. 백업은 외부 저장 장치 또는 클라우드에 저장할 수 있으며, 제조사별 제공하는 스냅샷 기능을 활용 할 수도 있다. 또한 복원 테스트를 주기적으로 수행하여 데이터를 신속하게 복구 할 수 있는지 확인하여야 한다.

3.6 감사 로깅과 모니터링

NAS 서버의 모든 활동(로그인 시도, 파일 액세스, 백업 작업 등)에 대한 감사 로그를 설정한다. 또한 시스템 상태 및 비정상 행위에 대한 실시간 경고 및 이벤트 알람을 설정하고, 정기적으로 로그 모니터링을 해서 신규 액세스 및 비정상 활동을 감지하고 대응할 수 있다.

3.7 업데이트된 안전한 앱 사용

NAS 장치에 설치된 어플리케이션 및 확장 프로그램은 제조사에서 제공하는 공식 패키지 센터에서 다운로드하고 설치한다. 이를 통해 무분별한 앱 설치를 방지하고 보안 검토를 거친 신뢰할 수 있는 앱을 보장받을 수 있다. 또한 주기적인 패치가 이루어지는 인기 있는 앱을 사용할 것을 권장하며 보안 업데이트를 주시하여 새로운 보안 취약점에 대비한다. 마지막으로 가능하다면 NAS 서버에서 앱에 부여되는 권한을 검토하여 최소 권한만 부여하고, 앱이 어떻게 동작하며 어떤 데이터에 접근하는지 이해하여 불필요한 접근 권한을 제한한다.

3.8 랜섬웨어 방지

NAS 서버의 데이터를 랜섬웨어 공격으로부터 안전하게 보호할 수 있어야 한다. 이를 위해 민감한 데이터에 읽기 전용 권한을 부여하면 랜섬웨어가 데이터를 수정하거나 삭제하는 것을 방지할 수 있다. 또한 제조사에서 제공하는 백신 솔루션을 활성화하여 사용하여 악성코드 및 활동을 식별하고 차단 할 수 있다. 마지막으로 NAS 서버를 사용하는 모든 사용자에게 의심되는 첨부파일 또는 링크를 클릭하지 않는 등 랜섬웨어에 대한 주기적인 교육을 실시한다. 랜섬웨어 예방 방법에 대한 지침을 제공하는 것도 좋다.

안전한 데이터 보호를 위한

NAS 보안수칙

01 암호화 사용

저장된 데이터를 디스크 및 파일 레벨에서 암호화하고, SSL/TLS 암호화를 통해 데이터 전송 중에도 보호합니다.



02 접근 제어와 권한 관리

사용자와 그룹별로 적절한 접근 권한을 설정하고, 최소한의 권한 원칙을 준수하여 데이터에 엄격한 접근을 제한합니다.



03 네트워크 보안

불필요한 서비스 포트 차단, 방화벽 설정 및 안전한 원격 액세스를 위해 VPN 사용 등으로 NAS 장비를 안전하게 보호합니다.



04 펌웨어 및 소프트웨어 업데이트

주기적인 펌웨어, 운영 체제, 소프트웨어 업데이트를 통해 최신 보안 패치를 유지하고 취약점을 예방합니다.



05 백업 및 복원 전략

주기적인 데이터 백업을 통해 데이터 손실을 방지하고, 복원 테스트를 수행하여 빠르게 데이터를 회복할 수 있는지 확인합니다.



06 감사 로깅과 모니터링

모든 활동에 대한 감사 로그를 설정하고, 비정상적인 활동을 감지하기 위해 실시간 모니터링과 이벤트 알람을 활용합니다.



07 업데이트된 및 안전한 앱 사용

공식 패키지 센터에서 신뢰할 수 있는 앱을 다운로드하고, 주기적인 패치 및 보안 업데이트를 수행하여 보안 취약점에 대비합니다.



08 랜섬웨어 방지

데이터에 읽기 전용 권한을 할당하여 랜섬웨어로부터 데이터를 보호하고, 랜섬웨어 안티 솔루션을 활성화하여 악성코드를 차단하며, 사용자에게 랜섬웨어에 대한 주기적인 교육을 제공합니다.



과학기술정보통신부



한국인터넷진흥원

NAS 제조사별 보안 가이드

4.1 안내 사항	24
4.2 유의 사항	24
4.3 실증 장비	24

04

NAS 제조사별
보안 가이드

4.1 안내 사항

본 보고서에 언급된 NAS 제품은 글로벌 시장현황 및 한국인터넷진흥원에서 운영 중인 내서버 돌보미 서비스의 이용 통계를 반영하여 선정하였습니다. 또한 가정 및 기업에서 모두 이용할 수 있는 제품군을 중심으로 선정되었으며 각 NAS 장비별 운영 체제 및 소프트웨어 버전에 따라 점검 및 조치 방법이 다를 수 있습니다.

그 결과 사용빈도가 상대적으로 높은 3개 제조사(Synology, QNAP, ipTIME)를 선정하여 세부 진단항목을 설계하였습니다. 진단 및 조치 방법은 각 제조사에 제공하는 관리 콘솔을 통해 수행이 가능합니다.

4.2 유의 사항

본 가이드는 각 진단항목에 대한 이해를 돕기 위해 진단항목 설명, 진단기준, 진단방법, 대응방안을 제시하고 있다. 다만 일반적인 권고사항이므로 운영환경과 시스템에 미치는 영향도를 검토하여 적용하여야 한다.

4.3 실증 장비

본 가이드 제작을 위해 사용된 제조사별 제품명 및 펌웨어 버전은 아래와 같으며, 제품 또는 펌웨어 버전에 따라 점검 및 조치 방법이 상이할 수 있으므로 본 가이드에 제시된 방법론을 기반으로 사용자 매뉴얼을 참고하여 진행하여 주시기 바랍니다.

제조사	제품명	펌웨어 버전
시놀로지(Synology)	D1821+	DSM 7.2.1
큐냅(QNAP)	TS-264	QTS 5.1.3
아이피타임(ipTIME)	NAS200	1.0.46

Synology NAS 보안가이드

5.1 진단 항목	26
5.2 계정 관리	28
5.3 접근 관리	40
5.4 패치 및 보안 관리	50
5.5 로그 및 백업 관리	64
5.6 서비스 관리	72

05

05

Synology NAS
보안 가이드

5.1 진단 항목

항목 분류	항목 코드	항목명
계정 관리	Synology-01	기본 관리자 계정(default) 사용금지
	Synology-02	계정별 권한 관리
	Synology-03	불필요한 공용계정 및 휴면계정 관리
	Synology-04	패스워드 만료 기간 설정
	Synology-05	패스워드 복잡도 설정
	Synology-06	로그인 실패 횟수 제한
접근 관리	Synology-07	암호화 통신 및 기본포트 변경
	Synology-08	Session Timeout 설정
	Synology-09	USB 장치 사용금지
	Synology-10	불필요한 공유폴더 미사용 및 암호화 활성화
	Synology-11	MFA(Multi-Factor Authentication) 인증 적용 여부
패치 및 보안관리	Synology-12	보안 어드바이저 예약검사 적용
	Synology-13	제조사에서 제공하는 최신 업데이트 적용
	Synology-14	백신 프로그램 설치
	Synology-15	백신 프로그램 최신 패턴 업데이트 및 예약검사 적용
	Synology-16	방화벽 기능 활성화
	Synology-17	DoS 보호 활성화
로그 및 백업 관리	Synology-18	로그 관리
	Synology-19	백업 관리
	Synology-20	NTP 서버 연동
서비스 관리	Synology-21	불필요한 서비스 사용 금지
	Synology-22	안전한 SNMP 서비스 사용
	Synology-23	안전한 FTP 서비스 사용

23개 항목



유의사항

본 가이드는 NAS 취약점 평가항목에 대한 이해를 돕기 위해 항목설명, 점검기준, 점검방법, 대응방안을 제시하며 취약점 조치에 활용할 수 있습니다. 다만 일반적인 권고사항이므로 운영환경과 시스템에 미치는 영향을 검토하여 적용하여야 합니다.

※ 본 가이드 작성 기준은 **Synology NAS 장비의 GUI 기반으로 작성**되었으며, 타제품 사용 시 각 항목에 해당하는 설정 탭의 모양, 설명, 현황 등이 제품에 따라 상이할 수 있으므로 **각 제조사의 사용자 매뉴얼을 참고**하여 본 가이드 안내에 따라 보안 설정할 것을 권고 드립니다.

5.2 계정 관리

Synology-01 기본 관리자계정(default) 사용금지

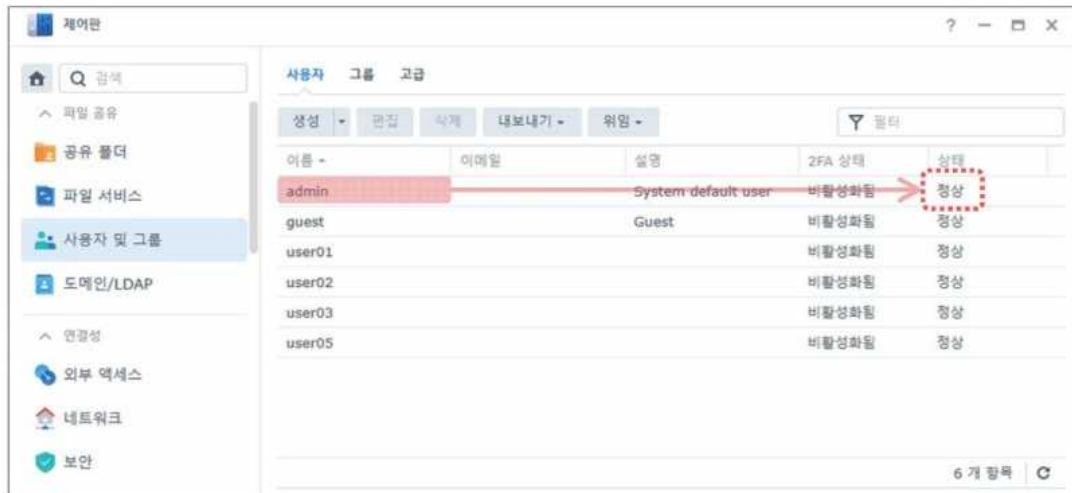
🛡️ 취약점 개요

점검 내용	제조사가 생성한 기본 관리자계정(default) 사용 여부 점검										
점검 목적	이미 알려진 default 계정을 이용한 계정 접속 시도 및 탈취를 예방하기 위해 기본 관리자 계정의 비활성화 여부 점검										
보안 위협	공격자가 알려진 Default 계정 정보를 이용하여 무차별 대입 공격(Brute Force Attack), 사전 공격(Dictionary attack), 혼합 공격(Hybrid Attack), 레인보우 테이블 공격(Rainbow Table Attack) 등 패스워드 크래킹 공격을 통해 계정이 도용될 수 있으며, 이를 통해 시스템 가용성 훼손, 자료 유출 등의 위험이 존재함										
점검 기준	<table> <tr> <td>양호</td><td>기본 관리자계정(admin)를 사용하지 않는 경우</td></tr> <tr> <td>취약</td><td>기본 관리자계정(admin)를 사용하는 경우</td></tr> </table>	양호	기본 관리자계정(admin)를 사용하지 않는 경우	취약	기본 관리자계정(admin)를 사용하는 경우						
양호	기본 관리자계정(admin)를 사용하지 않는 경우										
취약	기본 관리자계정(admin)를 사용하는 경우										
참고	※ Synology NAS의 기본계정(default) : admin, guest ※ 대표적인 패스워드 크래킹 공격 <table> <thead> <tr> <th>서비스명</th><th>점검 방법</th></tr> </thead> <tbody> <tr> <td>무차별 대입 공격 (Brute Force Attack)</td><td>모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격</td></tr> <tr> <td>사전 공격 (Dictionary attack)</td><td>자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격</td></tr> <tr> <td>혼합 공격 (Hybrid Attack)</td><td>사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격</td></tr> <tr> <td>레인보우 테이블 공격 (Rainbow Table Attack)</td><td>해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격</td></tr> </tbody> </table>	서비스명	점검 방법	무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격	사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격	혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격	레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격
서비스명	점검 방법										
무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격										
사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격										
혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격										
레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격										

점검 및 조치방법

○ 제조사에서 제공된 기본 관리자계정(admin) 활성화 여부 확인

▶ [제어판] > [사용자 및 그룹] > [사용자] 탭에서 admin 계정 상태 확인

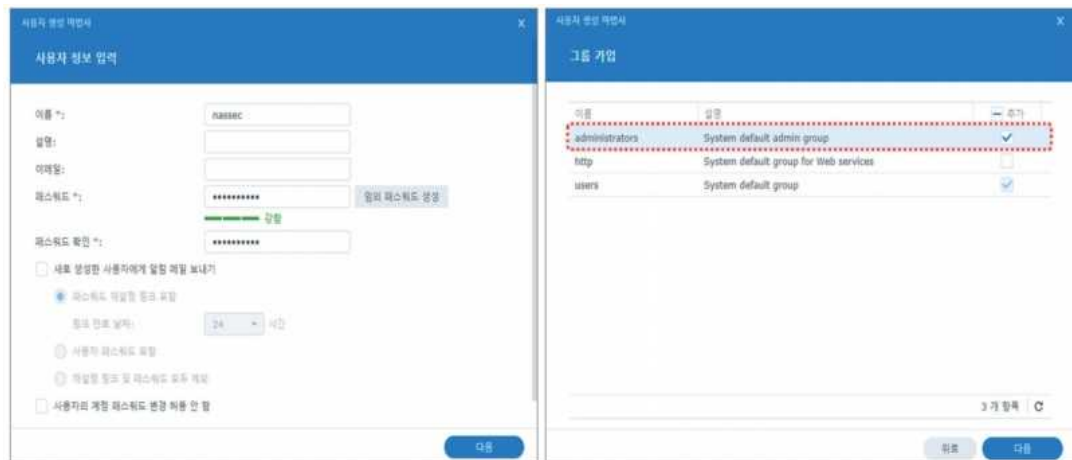


※ DSM 7.X 버전부터 초기 설정 후 admin 계정이 기본 비활성화 되어있음

○ 새 관리자 계정 생성

▶ admin 계정이 '정상'인 경우 비활성화를 위해 관리자 계정으로 사용할 신규 관리자 생성

▶ [제어판] > [사용자 및 그룹] > [사용자] > [생성] > [사용자 생성 마법사] 기능을 통해 신규 관리자 생성 및 '관리자 그룹' 권한 부여



○ 기본 관리자 계정 비활성화

- ▶ 신규 생성한 관리자 계정으로 로그인 후 기본 관리자계정(admin) 비활성화 진행
- ▶ [제어판] > [사용자 및 그룹] > [사용자] > admin 계정 선택 > [편집] 메뉴를 클릭하여 '이 계정 비활성화' 체크박스 선택 후 저장

admin

정보 사용자 그룹 권한 할당량 속도 제한

이름: admin

설명: System default user

이메일:

패스워드: 마지막으로 변경됨: 2023-11-17

패스워드 변경

☐ 사용자의 계정 패스워드 변경 허용 안 함

☒ 이 계정 비활성화 ⓘ

☒ 즉시

☐ 다음 이후:

모든 장치에서 로그아웃

○ 기본 관리자 계정 비활성화 여부 확인

이름	이메일	설명	2FA 상태	상태
admin		System default user	비활성화됨	비활성화됨
guest		Guest	비활성화됨	정상
nasec			비활성화됨	정상
user01			비활성화됨	정상

Synology-02 계정별 권한 관리

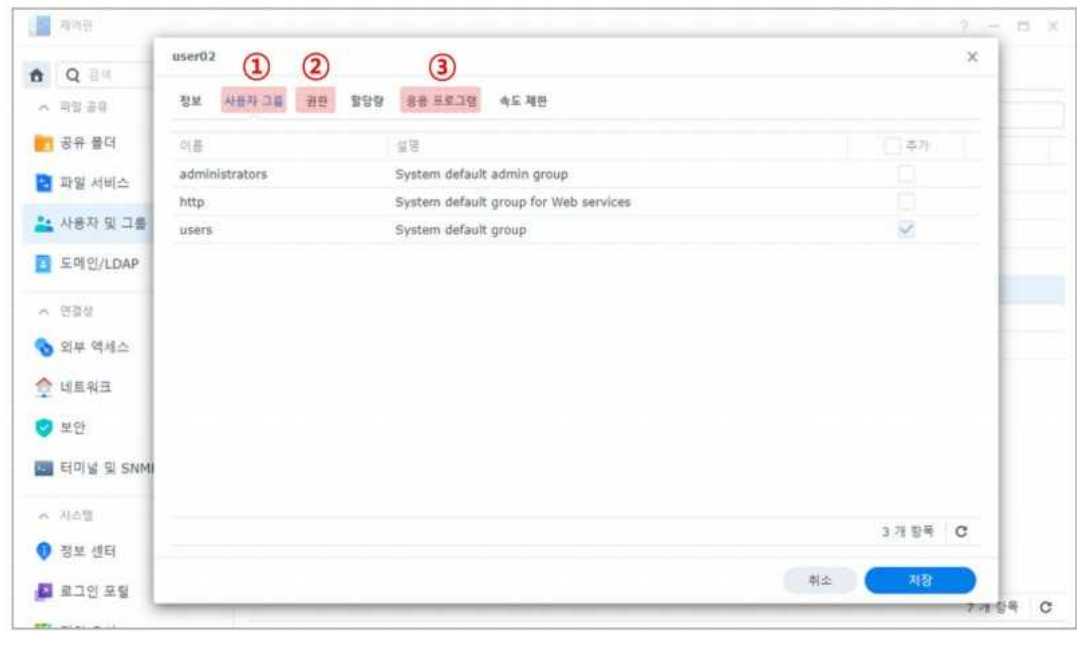
🛡️ 취약점 개요

점검 내용	• 사용자(계정)별 불필요한 권한 부여 여부 점검				
점검 목적	• 불필요하게 과도한 권한을 부여받은 사용자 계정을 통해 주요 설정 변경, 자료 유출 등을 방지하기 위함				
보안 위협	• 의도하지 않게 인가된 관리자 권한을 이용하여 NAS 장치의 주요 설정 변경, 시스템 침입 경로 노출, 자료 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우</td></tr> <tr> <td>취약</td><td>과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우</td></tr> </table>	양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우	취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우
양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우				
취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우				
참고	※ 관리자 권한은 최소한의 사용자(계정)에만 부여 ※ 업무별 목적에 맞게 적절한 권한으로 계정 부여				

🛡️ 점검 및 조치방법

○ 사용자 계정별 권한 확인

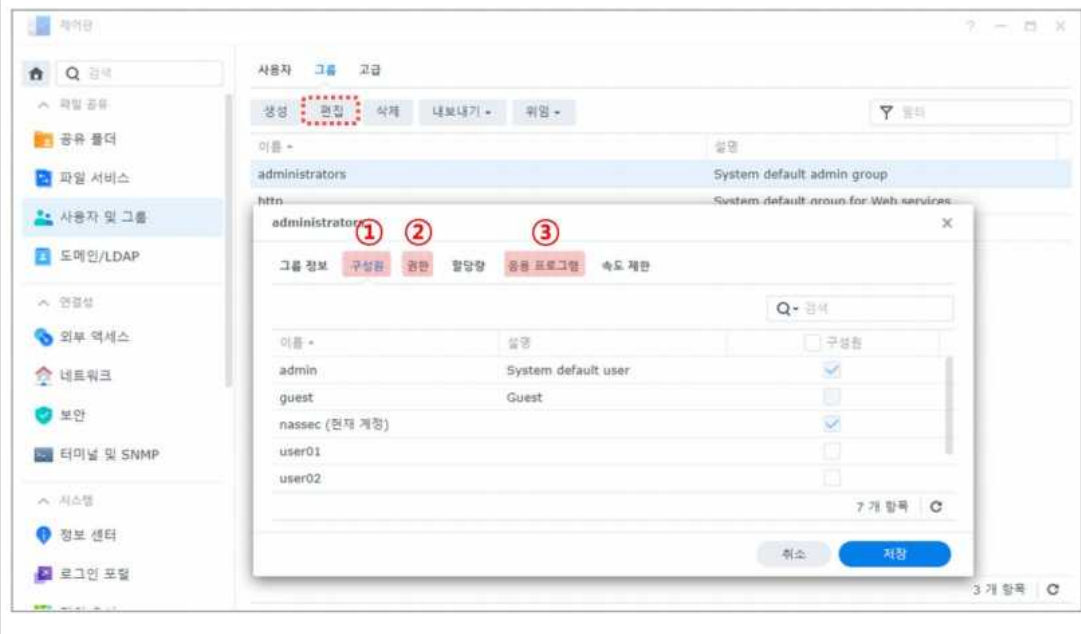
- ▶ [제어판] > [사용자 및 그룹] > [사용자] > 점검대상 계정 선택 > [편집] 메뉴를 클릭하여 부여된 권한 확인 및 불필요한 권한 회수
- ▶ 권한 점검은 ① 사용자 그룹(그룹 권한), ② 권한(접근 권한), ③ 응용 프로그램 권한 세가지 영역에서 진행하여야 함



※ 각 사용자는 기본적으로 포함된 ‘그룹 권한’을 상속받으며 사용자와 그룹 권한 사이에서 충돌이 발생한 경우 NA (액세스 없음) > RW(읽기/쓰기) > RO(읽기 전용) 순으로 최종 권한이 결정됨

○ 그룹별 기본 권한 확인

- ▶ [제어판] > [사용자 및 그룹] > [그룹] 탭에서 그룹별 기본 권한 확인 후 불필요한 권한 및 사용자 제거
- ▶ 권한 점검은 ① 구성원(사용자), ② 권한(접근 권한), ③ 응용 프로그램 권한을 점검하고, 특히 관리자 그룹 (administrators)에 불필요한 사용자가 포함되어 있는지 확인하여 관리자 권한 계정 최소화



Synology-03 불필요한 공용계정 및 휴면계정 관리

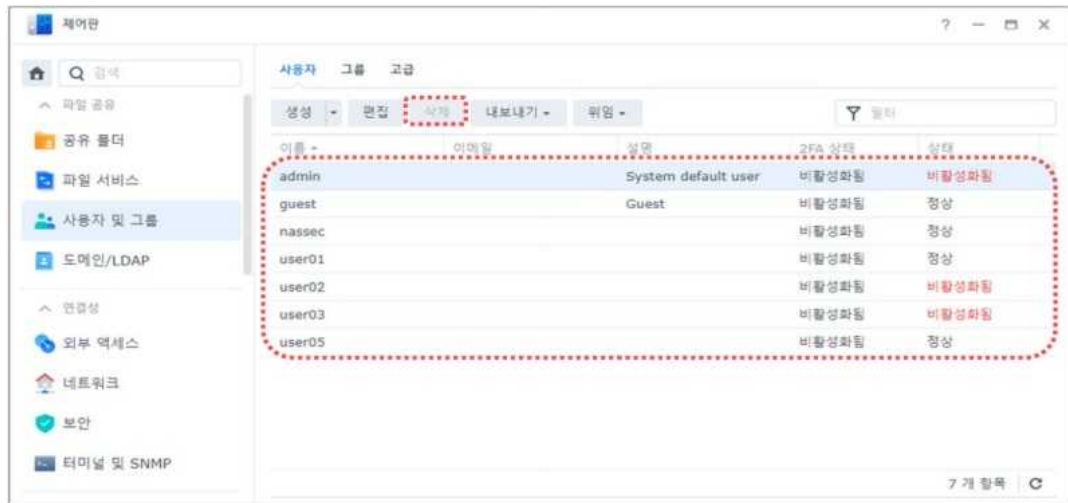
❏ 취약점 개요

점검 내용	불필요한 공용계정 및 미사용 휴면계정 존재 여부 점검				
점검 목적	- 불필요한 공용계정 및 미사용 휴면계정을 관리하여 비인가자의 접근 시도를 차단하고, 사용자별 개별 계정 부여를 통해 파일 변조, 정보 유출 등 사고 및 장애 발생에 대한 책임 추적성을 강화하기 위함 ※ 책임 추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				
보안 위협	관리되지 않는 휴면계정을 통한 비인가 접근의 위험이 존재하며, 공용계정 사용으로 인한 침해사고와 서비스 장애 발생 시 추적의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>공용계정 및 휴면계정을 관리하고 있는 경우</td></tr> <tr> <td>취약</td><td>공용계정 및 휴면계정이 관리되지 않는 경우</td></tr> </table>	양호	공용계정 및 휴면계정을 관리하고 있는 경우	취약	공용계정 및 휴면계정이 관리되지 않는 경우
양호	공용계정 및 휴면계정을 관리하고 있는 경우				
취약	공용계정 및 휴면계정이 관리되지 않는 경우				
참고	※ 계정의 공유를 금지하여야 하며, 1인 1계정 사용을 원칙으로함				

❏ 점검 및 조치방법

○ 사용자 계정 목록 확인

- ▶ [제어판] > [사용자 및 그룹] > [사용자] 탭에서 사용자 계정 목록 확인
- ▶ 사용자 확인(인터뷰), 계정 관리대장 검토 등을 통해 공용계정 및 미사용된 장기 휴면계정 여부를 확인하여 불필요한 계정 삭제 조치



※ 여러 사용자가 같은 계정을 공유하지 않도록 계정별로 필요한 권한 설정

Synology-04 패스워드 만료 기간 설정

🛡️ 취약점 개요

점검 내용	패스워드(암호)의 최대 유효 기간 설정 여부 점검				
점검 목적	패스워드(암호)의 유효 기간을 설정하여, 사용자가 패스워드를 변경하도록 강제하여 비인가자가 불법 또는 임의로 획득한 패스워드의 무단 사용을 방지하기 위함				
보안 위협	장기간 변경하지 않은 패스워드를 지속적으로 사용하는 경우, 패스워드 크래킹 공격으로 패스워드가 노출될 위험성이 커지며, 임의로 획득한 패스워드를 무단 사용할 위험이 커짐				
점검 기준	<table border="1"> <tr> <td>양호</td><td>적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)</td></tr> <tr> <td>취약</td><td>적절한 패스워드 만료 기간 설정되지 않은 경우</td></tr> </table>	양호	적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)	취약	적절한 패스워드 만료 기간 설정되지 않은 경우
양호	적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)				
취약	적절한 패스워드 만료 기간 설정되지 않은 경우				
참고	※ 암호정책: 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 패스워드 만료 기간은 90일(3개월) 이내로 설정하는 것을 권장				

🛡️ 점검 및 조치방법

○ 최대 패스워드 유효 기간 설정 점검

- ▶ [제어판] > [사용자 및 그룹] > [고급] 탭의 패스워드 만료 메뉴에서 '패스워드 만료 활성화' 체크박스 활성화 여부 및 '최대 패스워드 유효 기간(일수)' 확인

The screenshot shows the Synology Control Panel interface. On the left, the 'Control Panel' sidebar is visible with the 'User and Group' section selected. The main area shows the 'Password Policy' settings under the 'Advanced' tab. A red dashed box highlights the 'Password Policy' section, which includes the following settings:

- ☐ Password Policy Activation
- Maximum password validity (days): 30
- ☐ Minimum password validity (days): 1
- ☐ Require password change at login
- ☒ Require password change after expiration
- ☐ Require password change after expiration
- Require password change after expiration: 00 : 00
- Require password change after expiration: 1

At the bottom of the settings, there are buttons for 'Reset' and 'Apply'.

※ 최소 비밀번호 유효 기간 : 암호 변경 후 다시 암호를 변경할 수 있기 전까지 경과해야 하는 최소 날짜로 최소 기간이 설정되지 않았다면 사용자에게 익숙한 암호로 즉시 변경이 가능하여 원래 암호를 같은 날 다시 사용할 수 있으므로, 주기적인 비밀번호 변경이 무의미해 질 수 있으므로 최소 1일 이상 설정하는 것을 권장

○ 최대 비밀번호 유효 기간 설정

▶ ‘**패스워드 만료 활성화**’ 체크박스 선택 및 최대(90일 이내), 최소 유효기간(1일 이상) 설정

※ 비밀번호 사용 기간 만료 전 메시지, 만료 알림 이메일 등 비밀번호 변경을 위한 경고 메시지 제공을 권장

^ 비밀번호 만료

☒ 비밀번호 만료 활성화

최대 비밀번호 유효 기간(일수):

30

☒ 최소 비밀번호 유효 기간(일수)

1

☐ 만료 전에 사용자가 로그인할 때 비밀번호를 변경하라는 메시지 표시(일수)

1

☒ 만료 후 사용자에게 비밀번호 변경 허용

☐ 만료 알림 이메일 전송

보낸 시간

00 : 00

만료전 일 수:

Synology-05 패스워드 복잡도 설정

🛡️ 취약점 개요

점검 내용	● 사용자 계정의 비밀번호 복잡도 설정 여부 점검																
점검 목적	● 사용자 비밀번호 복잡성 관련 정책이 설정되어 있는지 점검하여 쉽게 추측 가능한 비밀번호로 인한 비인가자의 접근 차단하기 위함																
보안 위협	● 짧고 간단한 비밀번호의 경우 자동화된 비밀번호 크래킹 도구를 통한 비밀번호 공격(무작위 대입, 사전 대입, 추측 공격 등)에 의해 쉽게 유추될 수 있으므로 복잡성 설정을 통해 비밀번호를 알아낼 수 있는 평균 시간을 증가시킬 수 있도록 설정하여야 함																
점검 기준	<table><tr><td>양호</td><td>비밀번호 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)</td></tr><tr><td>취약</td><td>비밀번호 복잡도가 적절하게 설정되지 않은 경우</td></tr></table>	양호	비밀번호 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)	취약	비밀번호 복잡도가 적절하게 설정되지 않은 경우												
양호	비밀번호 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)																
취약	비밀번호 복잡도가 적절하게 설정되지 않은 경우																
참고	※ 비밀번호 복잡성 : 사용자 비밀번호 설정 시 영문(대문자, 소문자), 숫자, 특수 문자가 혼합된 비밀번호로 설정하는 방법 ※ 영문·숫자·특수문자 중 두가지 조합 시 최소 10자리 이상, 세 가지 조합 시 9자리 이상 비밀번호 규칙 설정을 권장 <table><tr><th colspan="4">비밀번호 조합 종류 및 구성 수</th></tr><tr><th>조합명</th><th>개수</th><th>조합명</th><th>개수</th></tr><tr><td>대문자</td><td>26개</td><td>숫자</td><td>10개</td></tr><tr><td>소문자</td><td>26개</td><td>특수 문자</td><td>32개</td></tr></table>	비밀번호 조합 종류 및 구성 수				조합명	개수	조합명	개수	대문자	26개	숫자	10개	소문자	26개	특수 문자	32개
비밀번호 조합 종류 및 구성 수																	
조합명	개수	조합명	개수														
대문자	26개	숫자	10개														
소문자	26개	특수 문자	32개														

🛡️ 점검 및 조치방법

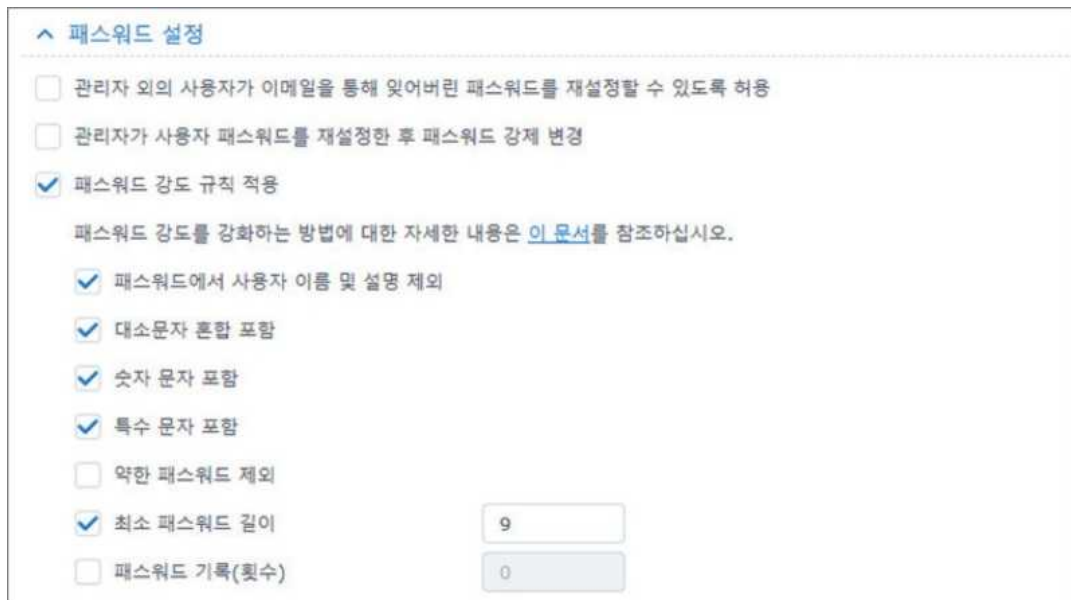
○ 패스워드 복잡도 설정 여부 및 규칙 점검

- ▶ [제어판] > [사용자 및 그룹] > [고급] 탭의 패스워드 설정 메뉴에서 '패스워드 강도 규칙 적용' 체크박스 활성화 여부 및 패스워드 강도 규칙 확인



○ 패스워드 복잡도 설정

- ▶ ‘패스워드 강도 규칙 적용’ 체크박스 선택 및 복잡도 설정(2조합 최소 10자리 이상, 3조합 9자리 이상 설정)



- ※ 패스워드에서 사용자 이름 및 설명 제외 : 사용자 이름이나 사용자 식별 정보를 포함할 수 없음
- ※ 약한 패스워드 제외 : 123456, password, qwerty 등과 같은 단순한 패스워드를 설정할 수 없음
- ※ 패스워드 기록(횟수) : 변경할 패스워드는 이전에 설정한 것과 달라야 하며, 설정한 횟수만큼 직전 패스워드를 사용할 수 없음

Synology-06 로그인 실패 횟수 제한

❗ 취약점 개요

점검 내용	로그인 실패 허용 임계값 설정 여부 점검				
점검 목적	로그인 실패 임계값이 설정되어 있는지 점검하여 비인가자의 지속적인 로그인 시도를 차단하기 위함				
보안 위협	반복되는 로그인 실패에 대한 차단이 이루어지지 않으면 자동화된 패스워드 크래킹 도구를 통한 패스워드 공격(무작위 대입, 사전 대입, 추측 공격 등)에 취약하여 사용자 패스워드가 탈취될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하, 계정 잠금 시간 10분 이상 권장)</td></tr> <tr> <td>취약</td><td>로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우</td></tr> </table>	양호	로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하, 계정 잠금 시간 10분 이상 권장)	취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우
양호	로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하, 계정 잠금 시간 10분 이상 권장)				
취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우				
참고	※ 계정 잠금 시간 : 로그인 실패로 계정이 잠기는 시간으로 관리자가 잠금 해제를 하거나 잠금 유지 시간이 경과되어야 재시도할 수 있음 ※ 로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장				

❗ 점검 및 조치방법

○ 계정 보호 활성화 여부 점검

▶ [제어판] > [보안] > [계정] 탭의 계정 보호 메뉴에서 ‘**계정 보호 활성화**’ 체크박스 활성화 여부 및 ‘**로그인 시도 횟수**’, ‘**계정 보호 취소/차단 해제(잠금 시간)**’ 설정값 확인

※ 로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장



※ Synology NAS 장비에서는 정해진 시간('다음 시간 이내' 설정) 이내에 설정한 로그인 시도 횟수를 초과하면 계정 잠금이 발동하며, 일정 시간 이후 잠금이 해제됨

○ 계정 보호 활성화 및 임계값 설정

▶ '계정 보호 활성화' 체크박스 활성화 및 임계값 설정

☒ 계정 보호 활성화

트러스트되지 않은 클라이언트

트러스트되지 않은 클라이언트가 미리 정의해 놓은 기간 이내에 로그인 실패 횟수가 너무 많을 경우 계정 보호가 촉발됩니다.

로그인 시도 횟수:

다음 시간 이내(분):

계정 보호는 미리 정의해 놓은 기간이 지난 후 취소됩니다.

계정 보호 취소(분 후):

[보호된 계정 관리](#)

트러스트된 클라이언트

트러스트된 클라이언트는 미리 정의해 놓은 기간 이내에 로그인 실패 횟수가 너무 많을 경우 차단됩니다.

로그인 시도 횟수:

다음 시간 이내(분):

클라이언트가 얼마 후에 차단이 해제될지 기간을 정의합니다.

차단 해제(분 후):

[트러스트된 클라이언트 관리](#)

※ 트러스트되지 않은 클라이언트 : 로그인 이력이 없는 클라이언트(PC)가 로그인 실패 시 해당 계정은 보호된 계정으로 격리되어 일정 시간 로그인 불가(계정 기준 잠금)

※ 트러스트된 클라이언트 : 로그인 이력이 있는 클라이언트(PC)가 로그인 실패 시 해당 IP가 차단되어 어떠한 계정으로든 로그인할 수 없으며 일정 시간 이후 차단 해제(IP 기준 잠금)

5.3 접근 관리

Synology-07 암호화 통신 및 기본 포트 변경

🛡️ 취약점 개요

점검 내용	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜 사용 및 기본 포트를 변경하고 접근하고 있는지 점검				
점검 목적	웹 또는 터미널 접근 시 데이터를 암호화하여 전송하는 HTTPS와 SSH를 사용하여 비인가자의 데이터 스니핑에 대비하고, HTTPS와 SSH의 알려진 기본 포트를 변경하여 공격자의 접근을 어렵게 하기 위함				
보안 위협	공격자가 스니핑(Sniffing)을 시도하면 계정의 ID와 패스워드가 평문으로 노출되어 계정이 탈취될 위험이 존재하며, 잘 알려진 기본 포트를 사용하는 경우, 지속적인 패스워드 크래킹 또는 해킹 공격의 대상이 될 위험이 존재함				
점검 기준	<table> <tr> <td>양호</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우</td></tr> <tr> <td>취약</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우</td></tr> </table>	양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우	취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우
양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우				
취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우				
참고	※ 스니핑(Sniffing) : 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청 장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말함				

🔒 점검 및 조치방법

○ NAS 웹 페이지 접근 시 보안 접속(HTTPS) 사용 여부 확인 ①

- ▶ [제어판] > [로그인 포털] > [DSM] 탭의 웹 서비스 메뉴에서 웹 접근을 위한 기본 포트 변경 여부 및 ‘**자동으로 HTTP 연결을 DSM 데스크톱의 HTTPS로 리다이렉션**’ 기능 활성화



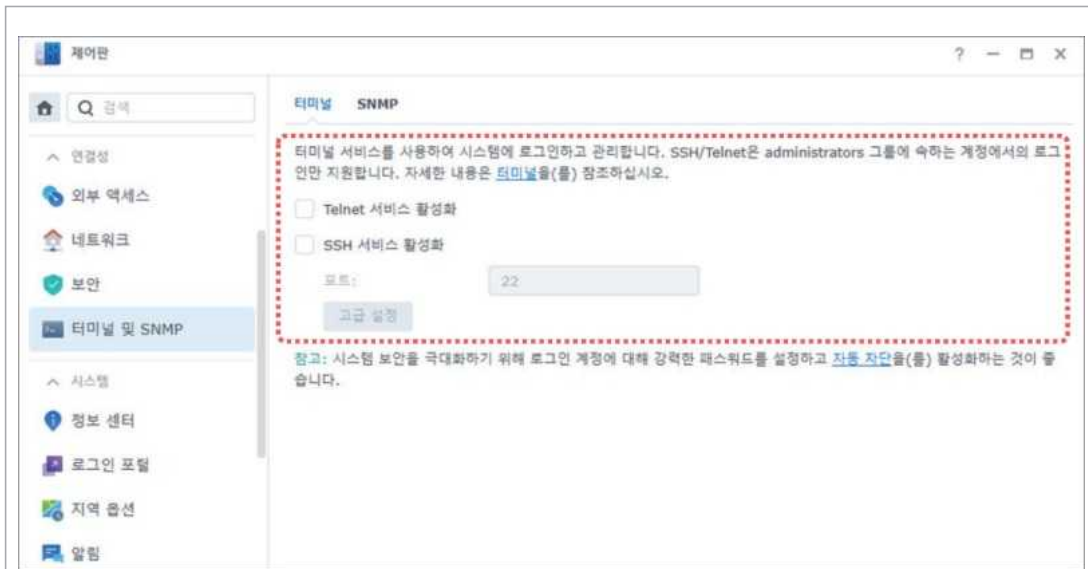
- ▶ 기본 포트 변경 및 ‘**자동으로 HTTP 연결을 DSM 데스크톱의 HTTPS로 리다이렉션**’ 기능 활성화를 통해 웹 접근 시 HTTPS 사용



- ※ Synology NAS에서는 웹 포트가 기본값으로 변경(HTTP/80→5000, HTTPS/443→5001)되어 제공되고 있으나 5000, 5001번 포트도 인터넷을 통해 쉽게 알 수 있으므로 알려지지 않은 포트로 변경하여 접속할 것을 권장
 ※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 ‘포트 포워딩’ 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

○ 터미널을 통한 원격접근 시 보안 접속(SSH) 사용 여부 확인 ②

- ▶ [제어판] > [터미널 및 SNMP] > [터미널] 탭에서 ‘**SSH 서비스 활성화**’ 체크박스 활성화 여부 및 포트 변경 여부 확인



- ▶ 터미널 접근이 불필요할 경우 체크박스를 해제하여 불필요한 서비스를 제거하고, 사용이 필요한 경우 데이터를 평문으로 전송하는 Telnet 서비스의 사용은 권장하지 않으며, 암호화된 SSH 서비스의 기본 포트를 변경하여 사용하는 것을 권장



※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

Synology-08 Session timeout 설정

🔒 취약점 개요

점검 내용	• Session timeout(자동 로그아웃) 설정 적용 여부 점검				
점검 목적	• 사용자의 부주의로 계정이 로그인된 상태로 방치되는 상황을 방지하고, 사용하지 않는 세션을 종료하여 보안성과 가용성을 높이기 위함				
보안 위협	• 사용자가 작업 중 이석하거나 불안정한 세션 종료를 했을 경우, 권한 없는 사용자가 이석한 자리에서 정책 삭제나 변경 등 악의적인 행위를 하거나 불안정한 세션 종료를 한 세션 정보를 재사용하여 인증 없이 NAS 장치에 접근할 위험이 있음				
점검 기준	<table border="1"> <tr> <td>양호</td><td>Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)</td></tr> <tr> <td>취약</td><td>Session timeout(자동 로그아웃)이 설정되지 않은 경우</td></tr> </table>	양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)	취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우
양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)				
취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우				
참고	※ Session timeout : 로컬 또는 원격에서 장비에 접속한 사용자가 일정 시간 동안 통신이 없을 시 해당 세션을 종료시키는 설정 ※ 장비에 접속하여 이행하는 업무 특성을 고려하여 최소 시간 설정				

🔒 점검 및 조치방법

🔍 Session Timeout(자동 로그아웃) 설정 확인

- ▶ [제어판] > [보안] > [보안] 탭의 로그인 설정 메뉴에서 '로그아웃 타이머(분)' 설정시간을 확인하여 적정 시간으로 설정(15분 이내로 설정할 것을 권장)



Synology-09 USB 장치 사용금지

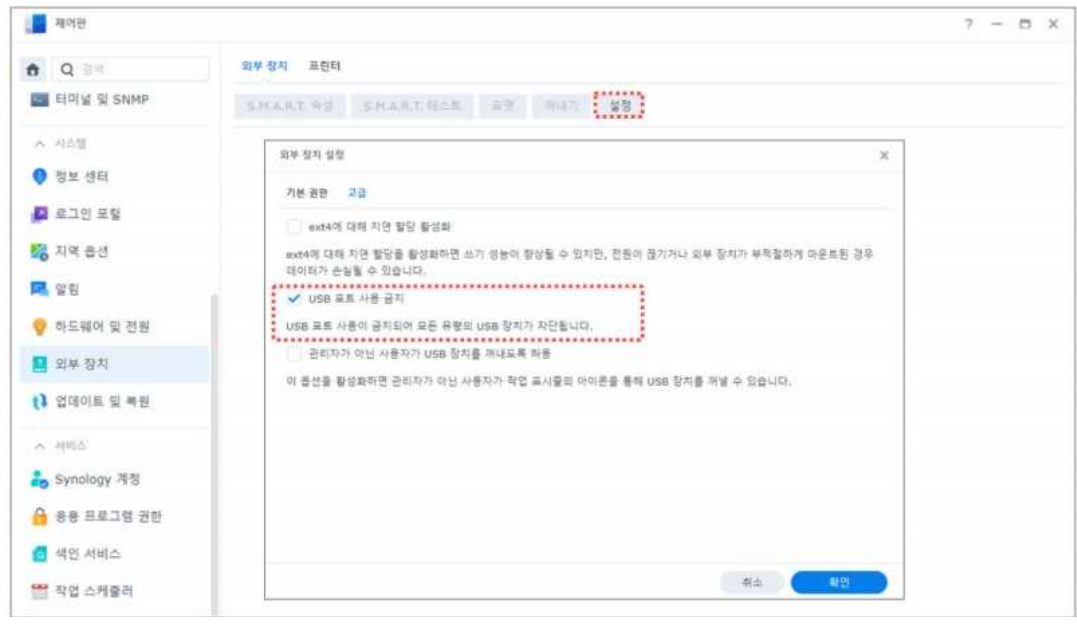
❏ 취약점 개요

점검 내용	• 이동식 저장매체(USB)의 사용금지 설정 여부 점검				
점검 목적	• NAS 장치에 USB 장치 사용을 강제적으로 제한하여, 비인가자의 물리적 접근을 통한 악성코드 감염과 데이터 유출 등의 위험을 차단하기 위함				
보안 위협	• 비인가자가 NAS 장치에 물리적 접근으로 USB를 통한 악성코드 감염, 데이터 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우</td></tr> <tr> <td>취약</td><td>USB 장치 사용금지 또는 권한이 설정되지 않은 경우</td></tr> </table>	양호	USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우	취약	USB 장치 사용금지 또는 권한이 설정되지 않은 경우
양호	USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우				
취약	USB 장치 사용금지 또는 권한이 설정되지 않은 경우				
참고	※ BAD USB : 비인가자가 USB 메모리 펌웨어의 소스 코드를 악의적인 코드로 변조하여 USB 연결 시 악성코드 자동 설치/실행되는 USB ※ 포트락(PortLock) : 데이터 유출이나 외부 침입을 방지하기 위해 입출력 포트를 물리적으로 봉인하여 통제하는 포트 잠금장치				

❏ 점검 및 조치방법

○ USB 장치 사용 금지 설정 여부 확인

- ▶ [제어판] > [외부 장치] > [외부 장치] > [설정] > [고급] 탭에서 'USB 포트 사용 금지' 체크박스 활성화 여부 확인
- ▶ USB 장치 사용이 필요한 경우 [기본 권한] 탭에서 사용자별 USB 장치 사용 권한을 부여할 수 있음



Synology-10 불필요한 공유폴더 미사용 및 암호화 활성화

❏ 취약점 개요

점검 내용	• 불필요한 공유 폴더의 존재 여부 및 암호화 활성화 여부 점검				
점검 목적	• 불필요하게 공유되고 있는 폴더가 있는지 확인하여 비인가자의 접근 가능성 차단과 이를 통한 자료 유출 방지				
보안 위협	• 관리되지 않는 불필요한 공유 폴더는 자료 유출, 악성코드 유포 경로로 활용될 수 있으며, 해당 폴더로 접근이 가능한 IP/Port가 노출되었을 경우, 비인가자에 의한 공격 대상이 될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우</td></tr> <tr> <td>취약</td><td>불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우</td></tr> </table>	양호	불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우	취약	불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우
양호	불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우				
취약	불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우				
참고	※ 암호화 활성화 : 공유 폴더를 암호화하게 되면 NAS 장치(디스크)를 도난당하거나 분실하더라도 데이터를 안전하게 보호할 수 있음				

❏ 점검 및 조치 방법

○ 공유폴더 목록 및 암호화된 폴더 확인

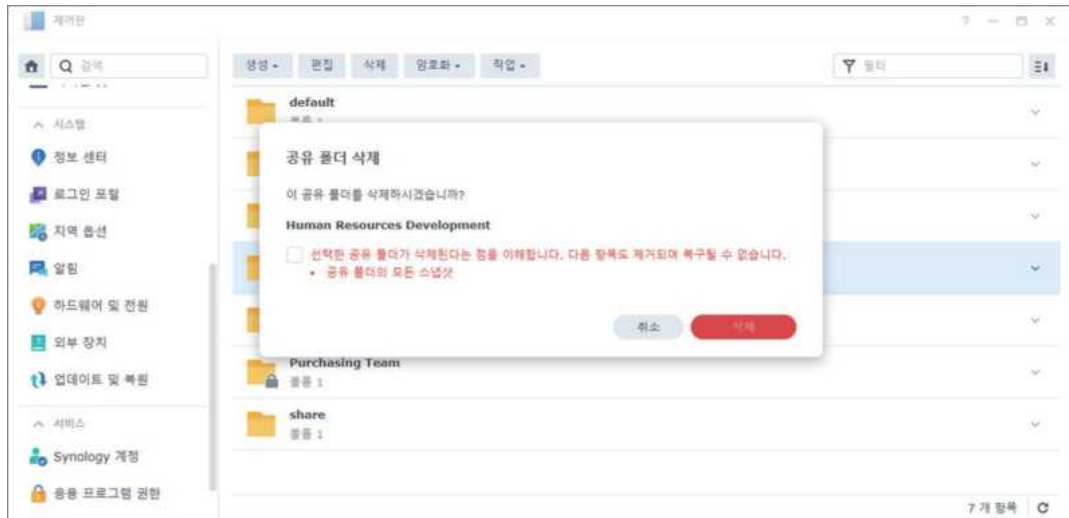
- ▶ [제어판] > [공유 폴더] 탭에서 ①**사용하지 않는 공유폴더 여부** 및 ②**중요한 폴더에 대한 암호화 적용 여부** 확인
 ※ 폴더 아이콘 우측에 자물쇠 아이콘이 있으면 암호화가 적용된 폴더



○ 불필요한 공유폴더 삭제 조치

▶ 사용하지 않는 공유 폴더는 '폴더 선택' 후 **[삭제]** 버튼을 통해 삭제 조치

※ NAS 장치에서 기본으로 제공하는 공유 폴더(default, share)를 사용하지 않는 경우 삭제하는 것을 권장



○ 중요 폴더 암호화 적용

▶ 암호화를 적용할 폴더 선택 후 [편집] > [암호화] 탭에서 '**이 공유폴더 암호화**' 체크박스 활성화 후 암호화키를 입력하여 암호화 적용



※ 암호화 키를 분실할 경우 암호화된 폴더에 접근할 수 없으므로 분실하지 않도록 주의하여야 함

Synology-11 MFA(Multi-Factor Authentication) 인증 적용 여부

❏ 취약점 개요

점검 내용	• 사용자 계정에 대한 다중인증(MFA) 설정 여부 점검				
점검 목적	• 두 가지 이상의 인증 방식을 통해 피싱, 사회 공학적 기법, 무차별 대입 공격 등과 같은 공격을 통한 비인가자의 접속을 방지하기 위함				
보안 위협	• 비인가자가 패스워드 크래킹, 크리덴셜 스테핑 등이나 피싱, 사회 공학적 기법 등을 통해 계정 정보를 탈취하게 되면, 시스템 관리자 권한으로 접속하여 보안 설정 임의 조작, 데이터 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>사용자 계정에 MFA 인증이 적용된 경우</td></tr> <tr> <td>취약</td><td>사용자 계정에 MFA 인증이 적용되지 않은 경우</td></tr> </table>	양호	사용자 계정에 MFA 인증이 적용된 경우	취약	사용자 계정에 MFA 인증이 적용되지 않은 경우
양호	사용자 계정에 MFA 인증이 적용된 경우				
취약	사용자 계정에 MFA 인증이 적용되지 않은 경우				
참고	※ 크리덴셜 스테핑 : 비인가자(공격자)가 기존에 노출된 계정 정보를 통하여 다른 플랫폼에 무작위로 대입해보며 사용자의 계정을 탈취하는 공격 ※ Multi-Factor 인증(MFA) : 사용자에게 암호 이외의 추가 정보를 입력하도록 요구하는 다중 단계 사용자 인증 방식				

❏ 점검 및 조치방법

○ MFA(Multi-Factor Authentication) 인증 적용 여부 확인

- ▶ [제어판] > [보안] > [계정] 탭의 2단계 인증 메뉴에서 '다음 사용자에게 2단계 인증 적용' 체크박스 활성화 여부 확인



※ Synology NAS 장치의 MFA 인증을 사용하기 위해서는 관리자 이메일 등록이 선행되어야 함

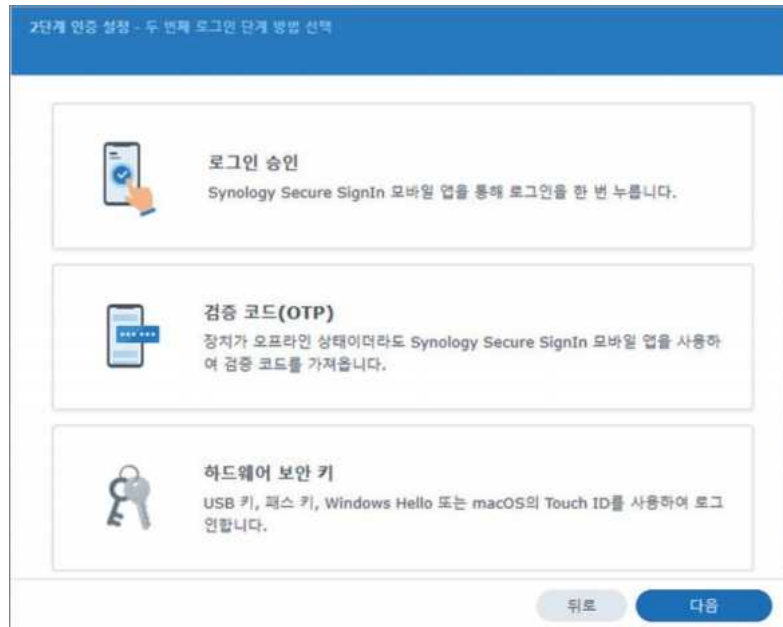
○ 관리자 이메일 등록

▶ [제어판] > [알림] > [이메일] 탭의 이메일 메뉴에서 관리자 이메일 등록

○ MFA(Multi-Factor Authentication) 인증 적용 및 인증 대상 설정

▶ [제어판] > [보안] > [계정] 탭의 2단계 인증 메뉴에서 '다음 사용자에게 2단계 인증 적용' 체크박스 활성화 및 인증 대상 설정

- ▶ 사용자는 최초 로그인 시 MFA 인증방식(로그인 승인, 검증 코드(OTP), 하드웨어 보안키)을 설정하고 사용해야 함



5.4 패치 및 보안 관리

Synology-12 보안 어드바이저 예약검사 적용

🛡️ 취약점 개요

점검 내용	● 보안 어드바이저를 설치하여 주기적인 예약검사(점검) 여부 점검				
점검 목적	● 정기적인 예약 검사를 통해 NAS 장치의 장애, 설정상의 보안 취약점, 최신 업데이트 등 위험을 지속적으로 관리하기 위함				
보안 위협	● NAS 장치 내 악성코드 감염, 시스템 장애 및 경고, 취약한 설정 및 최신 업데이트 등을 적용하지 않아 시스템 장애 발생, 제로데이 공격, 악성코드 감염 등의 위험이 존재함				
점검 기준	<table><tr><td>양호</td><td>보안 어드바이저를 설치하여 정기 예약검사를 설정하여 실행하고 있는 경우</td></tr><tr><td>취약</td><td>보안 어드바이저가 설치되어 있지 않거나, 예약검사 일정을 설정하지 않은 경우</td></tr></table>	양호	보안 어드바이저를 설치하여 정기 예약검사를 설정하여 실행하고 있는 경우	취약	보안 어드바이저가 설치되어 있지 않거나, 예약검사 일정을 설정하지 않은 경우
양호	보안 어드바이저를 설치하여 정기 예약검사를 설정하여 실행하고 있는 경우				
취약	보안 어드바이저가 설치되어 있지 않거나, 예약검사 일정을 설정하지 않은 경우				
참고	※ 보안 어드바이저 : Synology에서 제공하는 DSM용 보안 응용 프로그램으로 맬웨어, 네트워크, 시스템, 업데이트, 계정 등에 대한 보안 진단을 통해 사용자에게 보안 권고를 해주는 자가진단도구 보안 어드바이저 개요 결과 로그인 분석 고급 ! 위험성 주의를 요하는 보안 위험을 찾았습니다. 2 일 안에 조치하십시오. 스캔 보고서 생성 🌐 맬웨어 시스템에서 맬웨어가 발견되지 않았습니다. 🟢 🖥️ 시스템 DSM이(가) 잘 작동 중입니다. 🟢 👤 계정 1 계정 설정은 보안이 취약합니다. 🔴 🏠 네트워크 네트워크 구성이 양호합니다. 🟢 🔄 업데이트 DSM 버전이 최신 상태입니다. 3개의 패키지가 최신 상태가 아닙니다. 🟡				

🔍 점검 및 조치방법

○ 보안 어드바이저 예약검사 설정 여부 점검

- ▶ [보안 어드바이저] > [고급] 탭의 스캔 일정 메뉴에서 '정기 스캔 일정 활성화' 체크박스 활성화 여부 및 스캔 일정 확인

보안 어드바이저

수행할 검사를 정의합니다.

검사 목록 사용자 지정

스캔 일정

☒ 정기 스캔 일정 활성화

다음 일수 후 실행: 매일

작업 실행: 00 : 00

보고서 설정

저장소 위치: [선택]

☐ 월간 보고서 활성화

☐ 일일 보고서 활성화

이메일을 통해 보고서를 받으려면 먼저 [재어판](#)으로 이동하여 이메일 알림을 활성화하십시오.

Synology-13 제조사에서 제공하는 최신 업데이트 적용

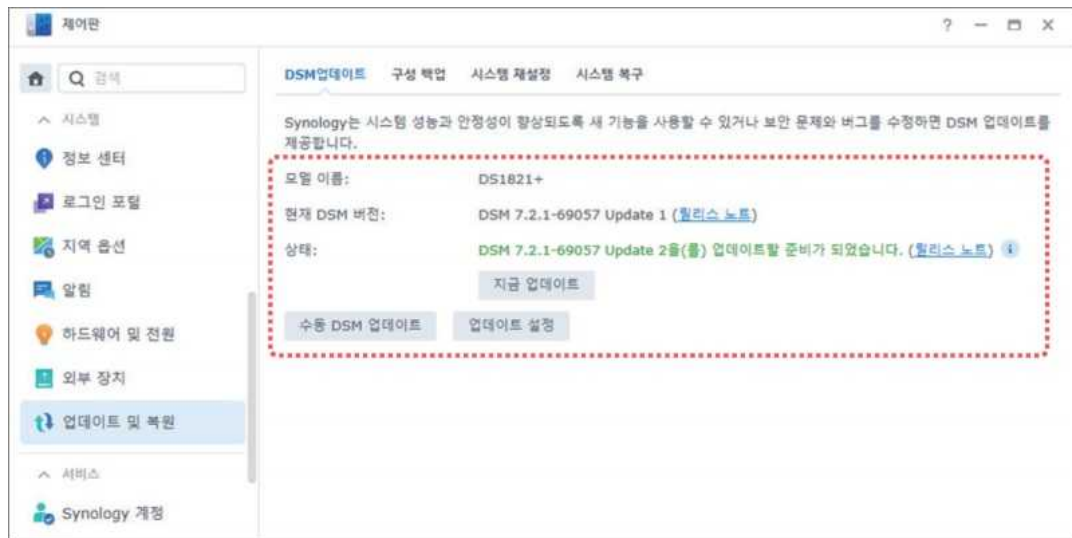
🛡️ 취약점 개요

점검 내용	• 제조사에서 제공하는 펌웨어의 최신 업데이트 여부 점검				
점검 목적	• 최신 업데이트를 적용하여 NAS 장치의 보안성과 시스템 안정성 확보				
보안 위협	• 최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 이용하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우</td></tr> </table>	양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우	취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우
양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우				
취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우				
참고	※ 펌웨어(Firmware) : 프로그래밍의 일종인 펌웨어는 하드웨어를 제어하는 소프트웨어 운영체제 프로그램으로 하드웨어 제어를 통해 하드웨어 역할을 하는 하드웨어와 소프트웨어의 중간자 역할 수행				

🛡️ 점검 및 조치방법

○ 업데이트 현황 확인

▶ [제어판] > [업데이트 및 복원] > [DSM업데이트] 탭의 최신 업데이트 상태 메시지 확인

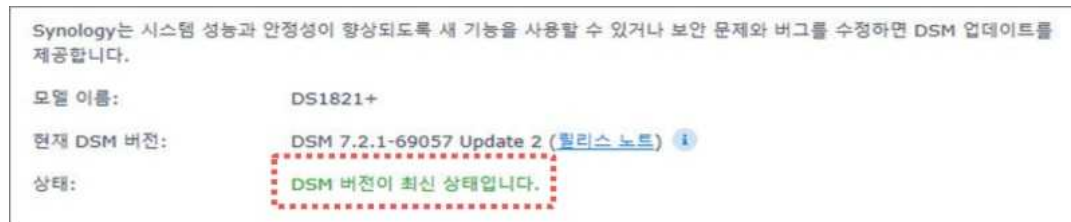


○ 최신 업데이트 적용

- ▶ NAS 장치가 인터넷 환경에 연결된 경우 '지금 업데이트' 버튼을 클릭하여 최신 업데이트를 적용하고, 폐쇄망 환경에 구축되어 인터넷 연결이 불가할 시 제조사 홈페이지에서 패치 파일을 다운로드 후 '수동 DSM 업데이트' 진행
 - ▶ 업데이트 후 시스템을 재기동해야 하는 경우가 있으므로 이를 고려하여 업데이트 설치 진행
- ※ 사용자가 시스템상에 '중요 DSM 업데이트 감지됨' 통지를 받은 경우 즉각적인 업데이트 권장

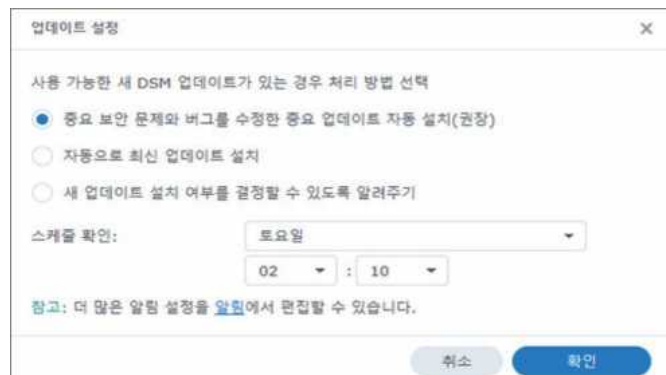


※ Synology 다운로드 센터 : <https://www.synology.com/ko-kr/support/download>



○ 자동 업데이트 설정 적용

- ▶ [제어판] > [업데이트 및 복원] > [DSM업데이트] > [업데이트 설정] 탭에서 자동 업데이트 설정 적용



- ▶ 중요도에 따라 자동 업데이트를 설정할 수 있으며, 긴급한 패치를 요구하는 보안 업데이트는 자동 설치를 권장하고, 제조사의 '릴리즈 노트'를 참고하여 업데이트에 따른 영향도를 고려하여 패치하는 것을 권장

Release Notes for DSM 7.2.1-69057 Update 2

DSM 7.2 시리즈 DSM 6.2 시리즈 All versions

Synology는 시스템 성능과 안정성이 향상되도록 새 기능을 사용할 수 있거나 보안 문제와 버그를 수정하면 DSM 업데이트를 제공합니다.

모델 이름: DS1821+

현재 DSM 버전: DSM 7.2.1-69057 Update 1 ([릴리즈 노트](#))

상태: DSM 7.2.1-69057 Update 2를(를) 업데이트할 준비가 되었습니다. ([릴리즈 노트](#))

[지금 업데이트](#)

[수동 DSM 업데이트](#) [업데이트 설정](#)

Version: 7.2.1-69057 Update 2

(2023-11-15)

Important notes

- Your Synology NAS may not notify you of this DSM update because of the following reasons. If you want to update your DSM to this version now, please [click here](#) to update it manually.
 - Your DSM is working fine without having to update. The system evaluates service statuses and system settings to determine whether it needs to update to this version.
- Depending on your Synology NAS model, this update will restart the device.

Fixed Issues

- Fixed an issue where certain models might experience abnormal shutdown after updating to DSM 7.2.1.
- Fixed an issue where files deleted locally might still exist on the Hyper Backup destination server.
- Fixed an issue where file access failed due to errors during soft link creation in Btrfs file systems.
- Fixed an issue where backing up WriteOnce shared folders in Hyper Backup might cause space consumption.
- Fixed an issue where SSD read-write cache might cause unexpected restarts of DSM on SA3200D and SA3400D.

Synology-14 백신 프로그램 설치

취약점 개요

점검 내용	백신 프로그램 활성화 여부 점검				
점검 목적	백신 프로그램을 설치하여 악성코드 감염을 예방하기 위함				
보안 위협	랜섬웨어, 웜, 트로이목마 등의 바이러스가 감염된 파일의 공유로 인하여 데이터 손실, 개인정보 유출, 시스템 손상 등과 같은 피해가 발생할 위험이 존재함				
점검 기준	<table> <tr> <td>양호</td><td>백신 프로그램을 설치하여 운영하고 있는 경우</td></tr> <tr> <td>취약</td><td>백신 프로그램을 설치하지 않은 경우</td></tr> </table>	양호	백신 프로그램을 설치하여 운영하고 있는 경우	취약	백신 프로그램을 설치하지 않은 경우
양호	백신 프로그램을 설치하여 운영하고 있는 경우				
취약	백신 프로그램을 설치하지 않은 경우				
참고	※ 바이러스(Virus) : 실행 파일의 일부분을 변형하여, 그곳에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합으로, 컴퓨터 내에 침투하여 자료를 손상시키거나, 다른 프로그램들을 파괴하여 작동할 수 없도록 하는 컴퓨터 프로그램의 한 종류 ※ 악성코드(Malware) : 바이러스(virus), 웜(worm), 트로이 목마(trojan)와 기타 유해한 컴퓨터 프로그램을 통틀어 일컫는 용어 ※ 랜섬웨어(Ransomware) : 악성코드의 일종으로 감염 시 화면이 차단되거나, 저장된 데이터를 암호화하여 데이터 복구를 위한 댓가를 요구하기도 함 ※ 웜(Worm) : 악의적인 목적을 가지고 자기 자신을 복제하여 전파시키며, 주로 네트워크 공유 폴더나 메일로 전파 ※ 트로이목마(Trojan) : 고의적으로 악의적 목적이 있는 파일, 주로 다른 악성코드나 위장된 프로그램으로 전파되거나 인터넷을 통해 다운로드 ※ 스파이웨어(Spyware) : 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어				

점검 및 조치방법

백신 프로그램 설치

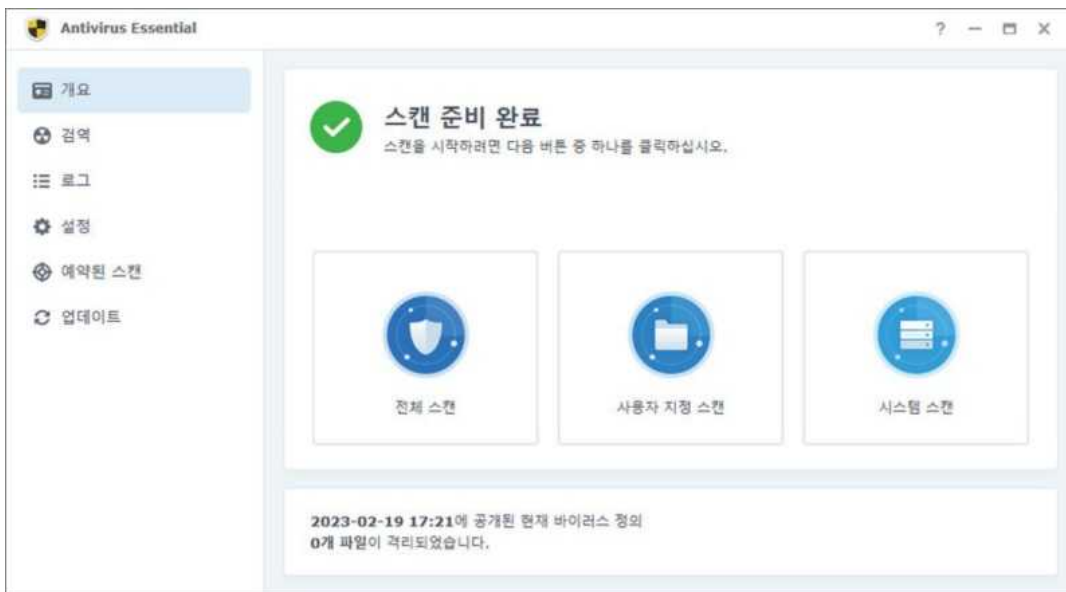
▶ Synology에서는 [패키지 센터]를 통해 NAS 장치를 위한 백신 프로그램 2종을 제공하고 있음



※ Antivirus Essential (무료) : Synology에서 직접 개발한 오픈소스 백신(ClamAV) 기반 백신 솔루션으로 DSM에 내장되어 있어 별도 라이선스 구매가 필요하지 않음

※ Antivirus by McAfee (상용) : 백신 전문 글로벌 기업인 McAfee에서 개발한 백신 솔루션으로 추가 라이선스 구매가 필요하지만 심층 보안 엔진을 기반으로 상대적으로 강력한 악성코드 탐지 기능 제공

▶ [패키지 센터] > [Antivirus Essential] 설치 및 정상 실행여부 확인



※ 본 가이드는 무료 버전인 'Antivirus Essential' 백신을 기준으로 작성되었음

Synology-15 백신 프로그램 최신 패턴 업데이트 및 예약검사 적용

❏ 취약점 개요

점검 내용	패턴 자동 업데이트 및 예약검사 설정 여부 점검				
점검 목적	설치되어 있는 백신의 최신 엔진(패턴) 적용 및 자동 업데이트 설정 여부를 점검하여 최신 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등)의 감염을 방지하기 위함				
보안 위협	백신 프로그램의 주기적인 패턴 업데이트가 적용되지 않으면, 신종 악성코드(바이러스, 웜, 랜섬웨어 등)를 탐지하지 못하여 시스템이 악성코드에 감염될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>최신 패턴 업데이트 및 예약검사 설정이 적용된 경우</td></tr> <tr> <td>취약</td><td>최신 패턴 업데이트가 미적용되어 있거나, 예약검사 설정이 되어있지 않은 경우</td></tr> </table>	양호	최신 패턴 업데이트 및 예약검사 설정이 적용된 경우	취약	최신 패턴 업데이트가 미적용되어 있거나, 예약검사 설정이 되어있지 않은 경우
양호	최신 패턴 업데이트 및 예약검사 설정이 적용된 경우				
취약	최신 패턴 업데이트가 미적용되어 있거나, 예약검사 설정이 되어있지 않은 경우				
참고	※ 패턴 : 백신 소프트웨어는 컴퓨터 바이러스들의 패턴을 정의한 뒤, 해당 패턴과 일치하는 파일은 바이러스에 감염되었다고 판단하게 되며, 새로운 형태의 바이러스를 탐지하기 위해서는 바이러스의 형태를 정의한 패턴을 업데이트해야 함				

❏ 점검 및 조치방법

○ 백신 프로그램 최신 패턴 업데이트

▶ [Antivirus Essential] > [업데이트] 탭에서 '바이러스 정의(패턴)' 업데이트 현황 확인



- ▶ NAS 장치가 인터넷 환경에 연결된 경우 ‘지금 업데이트’ 버튼을 클릭하여 최신 업데이트를 적용하고, 폐쇄망 환경에 구축되어 인터넷 연결이 불가할 시 백신사 홈페이지에서 패치 파일을 다운로드 후 ‘수동 업데이트’ 진행



※ 백신 패턴(정의) 다운로드 주소

- bytecode.cvd : <http://database.clamav.net/bytecode.cvd>
- daily.cvd : <http://database.clamav.net/daily.cvd>
- main.cvd : <http://database.clamav.net/main.cvd>

- ▶ [Antivirus Essential] > [설정] 탭의 업데이트 메뉴에서 ‘스캔하기 전에 바이러스 정의 업데이트’ 체크박스 활성화를 하여 실시간 바이러스 패턴(정의) 업데이트 적용



○ 백신 프로그램 예약검사 설정

- ▶ [Antivirus Essential] > [예약된 스캔] 탭에서 생성된 예약 스캔 목록을 확인하고, 별도 예약이 없을 경우 [생성] 버튼 클릭 후 예약 스케줄 등록



Synology-16 방화벽 기능 활성화

❏ 취약점 개요

점검 내용	• 방화벽 기능 활성화 및 정책 설정 적용 여부 점검				
점검 목적	• 방화벽 기능 활성화하고 접근통제 정책 설정을 적용하여 비인가자 IP의 무분별한 접근을 사전에 차단하고, 침해사고 발생 시 책임추적을 용이하게 하기 위함				
보안 위협	• 방화벽 설정으로 적절한 접근통제가 이루어지지 않을 경우, 불법 접근 및 데이터 유출, 서비스 거부 공격 등의 외부 공격으로부터 다양한 보안 위협에 노출될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우</td></tr> </table>	양호	방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우	취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우
양호	방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우				
취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우				
참고	※ 방화벽: 접근 제어, 패킷 필터링, 로그 및 감사 등을 지원하는 네트워크 보안 장비의 하나로, 기본적으로 출발지 IP, 목적지 IP와 Port를 사용하여 접근통제 정책을 설정함 ※ 화이트리스트 방식: 기본적으로 모든 접근을 막아놓고 액세스 허용 목록을 통해 접근 허용 대상만 따로 등록하는 방식 ※ 블랙리스트 방식: 기본적으로 모든 접근을 허용하되 특정 사람, 웹 사이트, 프로그램 등을 차단하는 액세스 거부 목록을 통해 접근하지 못하는 예외를 두는 방식				

❏ 점검 및 조치방법

❏ 방화벽 기능 활성화 여부 점검

▶ [제어판] > [보안] > [방화벽] 탭에서 '방화벽 활성화' 체크박스 선택 여부 확인



○ 방화벽 규칙(정책) 목록 확인 및 신규정책 생성(해외 IP 차단)

- ▶ [제어판] > [보안] > [방화벽] > [규칙] 탭에서 생성된 방화벽 규칙을 확인할 수 있으며, [생성] 버튼을 통해 신규 규칙(정책)을 생성할 수 있음

프로파일 편집 "default"

프로파일 이름: default

방화벽 규칙

생성 편집 삭제

모든 인터페이스

☒ 활성화됨	포트	프로토콜	소스 IP	작업
☒	모두	모두	대한민국	허용

1 개 항목

참고: "모든 인터페이스"에 일치하는 규칙이 없으면 각 인터페이스의 규칙이 일치됩니다.

참고: 규칙을 끌어다 놓아 순서를 재정렬할 수 있습니다. 맨 위에 있는 규칙이 더 높은 우선순위를 갖습니다.

※ 방화벽 규칙(정책)은 NAS 장치를 운영하는 목적에 따라 알맞게 설정하여야 하며 각 응용 프로그램 서비스, 접속 IP에 따라 규칙을 생성하여 외부 접근을 통제할 수 있다. NAS 장치를 국내에서만 사용하는 경우 해외IP 차단 규칙을 통해 불필요한 해외에서의 접근을 차단하는 것을 권장

- ▶ 해외IP 차단을 위해 '대한민국'을 제외한 모든 국가에서 접근 차단(화이트리스트 방식)
- ① [생성] 버튼을 클릭하여 '소스 IP' 항목에 '대한민국' 위치 추가 후 규칙 등록(작업:허용)

방화벽 규칙 생성

포트

☒ 모두

☐ 내장된 응용 프로그램 목록에서 선택

☐ 사용자 지정

소스 IP

☐ 모두

☐ 특정 IP

☒ 위치

작업

☒ 허용

☐ 거부

☒ 활성화됨

취소 확인

위치

대한민국

☐ 선택됨

소스

위치

KR

대한민국

취소 확인

※ 규칙1 (포트 : 모두, 소스 IP : 대한민국, 작업 : 허용)

- ▶ ② [생성] 버튼을 클릭하여 소스 IP 항목은 '모두', 작업 항목은 '거부'로 설정 후 규칙 등록
 ※ 규칙2 (포트 : 모두, 소스 IP : 모두, 작업 : 거부)

방화벽 규칙

생성 편집 삭제

모든 인터페이스

	활성화됨	포트	프로토콜	소스 IP	작업
≡	☒	모두	모두	대한민국	허용
≡	☒	모두	모두	모두	거부

※ 방화벽 규칙(정책) 목록의 상단에 위치할수록 높은 우선순위가 적용된다. 규칙 생성시 이점을 유의하여 설정하여야 한다. 위 규칙 목록에서는 '1)대한민국 허용' 규칙이 '2)모든 국가 거부' 정책보다 상단에 위치하고 있지만, 순서가 바뀌게 되면 '2)모든 국가 거부' 정책이 우선 적용된다.

Synology-17 DoS 보호 활성화

❏ 취약점 개요

점검 내용	• 서비스 거부(DoS) 보호 기능 활성화 여부 점검				
점검 목적	• 서비스 거부(DoS) 보호 기능을 활성화하여 서비스 거부 공격(Land, Ping Of Death, Syn Flooding, Smurf 등)을 방지 및 차단하기 위함				
보안 위협	• 공격자의 과도한 트래픽이나 접속 요청 등 서비스 거부 공격(Land, Ping Of Death, Syn Flooding, Smurf 등)으로 인하여 서버 접근 불가, 서비스 장애 및 시스템 교란 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>DoS 보호 기능이 활성화되어 있는 경우</td></tr> <tr> <td>취약</td><td>DoS 보호 기능이 비활성화되어 있는 경우</td></tr> </table>	양호	DoS 보호 기능이 활성화되어 있는 경우	취약	DoS 보호 기능이 비활성화되어 있는 경우
양호	DoS 보호 기능이 활성화되어 있는 경우				
취약	DoS 보호 기능이 비활성화되어 있는 경우				
참고	※ DoS(Denial Of Service) : 대량의 접속 요청이나 트래픽을 발생시켜 시스템의 리소스 고갈 등으로 시스템을 마비시키는 공격				

❏ 점검 및 조치방법

○ DoS 보호 활성화 여부 점검 및 조치

▶ [제어판] > [보안] > [보호] 탭의 서비스 거부(DoS) 보호 메뉴에서 'DoS 보호 활성화' 체크박스 활성화



5.5 로그 및 백업 관리

Synology-18 로그 관리

🔒 취약점 개요

점검 내용	• 내부 정책에 따른 적절한 시스템 로그 관리 여부 점검				
점검 목적	• 보안사고 발생 시 가시성 및 책임추적성을 확보하여 원인을 파악하기 위함				
보안 위협	• 로그 관리를 하지 않을 경우, 장애 및 침해사고 발생으로 피해 발생 시 원인 규명, 사후 추적 등 분석의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>주요 서비스 로그 활성화가 되어있는 경우</td></tr> <tr> <td>취약</td><td>주요 서비스 로그 활성화가 되어있지 않은 경우</td></tr> </table>	양호	주요 서비스 로그 활성화가 되어있는 경우	취약	주요 서비스 로그 활성화가 되어있지 않은 경우
양호	주요 서비스 로그 활성화가 되어있는 경우				
취약	주요 서비스 로그 활성화가 되어있지 않은 경우				
참고	※ 감사 로그 설정이 너무 높으면 불필요 로그가 기록되어 중요한 로그 기록과 혼동 및 시스템 성능 저하와 같은 영향을 받을 수 있으므로 법적 요구 사항과 조직의 정책·지침에 따라 원인 규명, 책임 추적을 위한 로그만 설정할 것을 권고함 ※ 책임추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				

🔒 점검 및 조치방법

○ 정상적으로 로그가 기록되고 있는지 점검

▶ [로그 센터] > [로그] 탭에서 최신 날짜, 시간까지 로그가 정상적으로 기록되고 있는지 확인

The screenshot shows the Synology Log Center interface. On the left, there's a sidebar with options like 'Overview', 'Logs', 'Alerts', 'Account Settings', 'Log Transfer', 'Log Search', and 'Log Settings'. The main area is titled 'Log Center' and has tabs for 'Overview' and 'Logs'. The 'Logs' tab is active, showing a list of logs. The logs are filtered by 'All' and show various system events. A red dashed box highlights the 'Time' column, indicating the focus on the latest log entries.

수준	로그	시간	사용자	이벤트
정보	시스템	2023-11-17 19:45:41	nassec	Package [Hyper Backup] has been succ...
정보	시스템	2023-11-17 19:45:40	SYSTEM	System successfully started [Hyper Bac...
정보	시스템	2023-11-17 19:45:28	nassec	Package [PHP 7.4] has been successfull...
정보	시스템	2023-11-17 19:45:27	SYSTEM	System successfully started [PHP 7.4].
정보	시스템	2023-11-17 18:33:51	SYSTEM	Package [Secure SignIn Service] has be...
정보	시스템	2023-11-17 18:33:51	SYSTEM	System successfully started [Secure Sig...
정보	시스템	2023-11-17 18:33:47	SYSTEM	System successfully stopped [Secure SI...
정보	시스템	2023-11-17 18:33:34	SYSTEM	System successfully registered [218.15...
정보	시스템	2023-11-17 18:33:31	SYSTEM	System successfully started [QuickConn...
정보	시스템	2023-11-17 18:33:26	SYSTEM	IP address [169.254.244.120] and subn...
정보	시스템	2023-11-17 18:33:26	SYSTEM	IP address [169.254.76.43] and subnet ...
정보	시스템	2023-11-17 18:33:20	SYSTEM	System started to boot up.
정보	시스템	2023-11-17 18:32:07	SYSTEM	System successfully stopped [QuickCon...

○ 파일 서비스 로그 기록(‘로깅’) 여부 점검

- ▶ NAS 장치에서 제공 중인 파일 서비스(SMB, AFP)를 사용 중인 경우, 파일 생성, 수정, 삭제 등의 작업에 대한 로그 기록 여부 확인
- ▶ [제어판] > [파일 서비스] > 해당 서비스(예:SMB) 탭에서 ‘전송 로그 활성화’ 체크박스 활성화 여부 점검

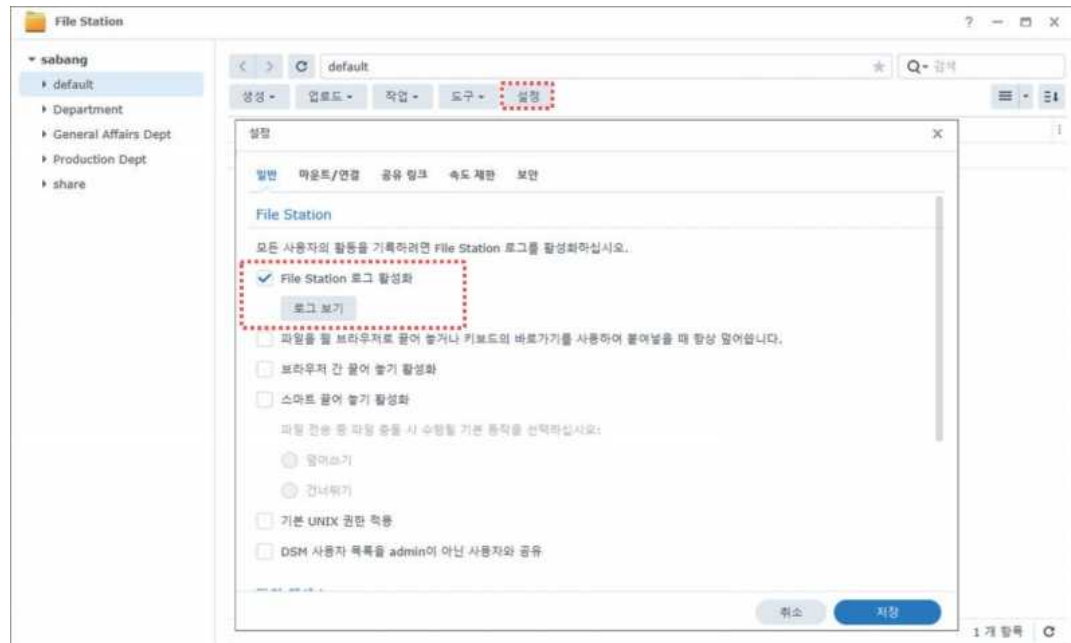


※ Synology NAS 장치에서는 여러 운영체제에서 원활한 데이터 공유를 위해 SMB, AFP, NFS, rsync와 같은 다양한 네트워크 프로토콜을 제공하고 있음

SMB (Server Message Block)	주로 Windows 환경에서 사용되는 네트워크 파일 공유 프로토콜로, 파일, 프린터 및 기타 리소스에 대한 공유 액세스 제공
AFP (Apple Filing Protocol)	Apple이 맥(MAC) 환경에서 파일 및 프린터를 공유하기 위해 개발한 프로토콜
NFS (Network File System)	유닉스 및 리눅스 환경에서 주로 사용되는 분산 파일 시스템 프로토콜로, 클라이언트 컴퓨터의 사용자가 네트워크를 통해 로컬 저장소에 있는 것처럼 파일에 접근할 수 있음
FTP (File Transfer Protocol)	파일 전송을 위해 널리 사용되는 표준 네트워크 프로토콜로 클라이언트와 서버 간에 파일을 전송하고 관리하는데 사용되지만 보안상의 이슈로 FTPS (FTP-SSL), SFTP(Secure FTP) 등으로 대체하여 사용하는 것을 권장
Rsync (Remote Sync)	원격 및 로컬 시스템 간 파일 및 디렉토리를 동기화하는 프로토콜로 주로 파일과 디렉토리를 백업할 때 사용
WebDAV (Web Distributed Authoring and Versioning)	HTTP 프로토콜을 기반으로 하는 분산 웹 저작 및 버전 관리 프로토콜 웹 서버에 저장된 파일에 직접 접근하여 읽기 및 쓰기 작업이 가능하고 파일 및 문서를 웹 상에서 공유하고 협업하는 데 사용

○ Synology File Station 로그 기록(‘로깅’) 여부 점검

- ▶ NAS 장치에 저장된 데이터의 생성, 수정, 삭제 등의 작업에 대한 로그 기록 여부 확인
- ▶ [File Station] > [설정] > [일반] 탭에서 ‘**전송 로그 활성화**’ 체크박스 활성화 여부 점검



※ File Station : Synology NAS 장치에서 제공되는 기본 애플리케이션으로 사용자가 NAS에 저장되는 파일을 쉽게 관리하고 공유할 수 있도록 지원

○ 로그 아카이브 설정

- ▶ 시스템에 저장된 로그 데이터의 무분별한 증가로 인한 저장공간 부족 현상을 해소하기 위해, 로그 아카이브 설정을 통해 특정 조건에 따른 로그 데이터 보관 규칙 설정
- ▶ [로그 센터] > [아카이브 설정] 탭의 아카이브 규칙 메뉴에서 아카이브 규칙 설정(NAS 저장공간을 고려하여 충분한 크기로 설정하는 것을 권장)

The screenshot shows the 'Log Center' interface with the 'Archive Settings' tab selected. The 'Archive Rules' section is highlighted with a red dashed box. It contains the following settings:

- 아카이브용 저장소 대상** (Archive Storage Target): 대상 (Target) is set to '공유 볼륨을 선택하십시오' (Select shared volume). 위치 선택 (Select location) button is present.
- 아카이브 규칙** (Archive Rules):
 - 다음 이벤트가 발생하면 현재 로그 데이터베이스를 아카이브합니다: (Archive current log database when the following event occurs:)
 - 데이터베이스 크기 초과 (Database size exceeded): 3 GB
 - 로그 수가 다음 보다 큼 (Log count greater than next): 10,000,000 (천만)
 - 로그 시간이 다음보다 오래되었습니다: (Log time exceeded next): 1개월
- 아카이브 형식** (Archive Format):
 - 추가 아카이브 설정을 위한 다음 옵션을 활성화합니다. (Activate the following options for additional archive settings.)
 - 기본 형식 이외에 텍스트 형식으로 로그를 아카이브합니다 (Archive logs in text format in addition to the basic format)
 - 로그 아카이브 압축 (Log archive compression)
 - 장치에 따라 별개로 로그 아카이브 (Archive logs separately by device)

※ 아카이브 규칙에 정의된 기준(크기, 로그 수, 기간)에 도달하게 되면 자동으로 로그가 백업되며, 아카이브 규칙을 설정하지 않으면 이전 로그 기록부터 삭제하면서 새로운 로그가 기록된다.

Synology-19 백업 관리

취약점 개요

점검 내용	NAS 장치에 저장된 데이터 백업 여부 점검						
점검 목적	장애 및 보안사고 발생 시 피해로부터 신속한 복구를 하기 위해 중요자료에 대한 2차 백업 (클라우드, 외부 저장매체, 스냅샷 등)을 설정하고 있는지 점검하여 자료 손실에 대비한 대응체계 점검						
보안 위협	NAS 장치에 저장된 데이터를 노리는 랜섬웨어 및 해킹 공격으로 인한 데이터 변조, 유출, 암호화의 위험이 존재함						
점검 기준	<table border="1"> <tr> <td>양호</td><td>주기적인 백업 관리를 이행하고 있는 경우</td></tr> <tr> <td>취약</td><td>주기적인 백업 관리를 이행하지 않는 경우</td></tr> </table>	양호	주기적인 백업 관리를 이행하고 있는 경우	취약	주기적인 백업 관리를 이행하지 않는 경우		
양호	주기적인 백업 관리를 이행하고 있는 경우						
취약	주기적인 백업 관리를 이행하지 않는 경우						
참고	※ NAS 장치에서 데이터 백업 종류 <table border="1"> <tr> <td>외부 저장매체 활용</td><td>네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식</td></tr> <tr> <td>외부 저장소 동기화</td><td>클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음</td></tr> <tr> <td>스냅샷(Snapshot) 기능 활용</td><td>제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함</td></tr> </table> ※ 백업 방식별 장·단점을 고려하여 데이터 백업을 진행하고, 중요한 데이터일수록 다중 백업을 적용하여 복구 신뢰성을 확보하여야 함	외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식	외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음	스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함
외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식						
외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음						
스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함						

🔍 점검 및 조치방법

- Synology NAS 장치에서는 2차 백업을 위해 [패키지 센터]에서 다양한 솔루션을 제공하고 있으며, 사용자 환경에 맞는 백업 방식 및 매체를 선정하여 백업을 진행하여야 함

서비스명	설명
 Hyper Backup	• 로컬 폴더를 포함하여 외부 서버, 다른 Synology NAS, 클라우드 서비스 (Amazon S3, Google Drive 등) 등 다양한 백업 대상에 대한 지원 • 복원 시점을 선택하여 파일 또는 시스템을 이전 상태로 복원할 수 있음 • 데이터 압축 및 암호화를 지원하여 보안성 강화
 Active Backup for Business	• Windows 및 Linux 서버, VMware 및 Hyper-V 가상 머신 등 다양한 플랫폼에 대한 전체 이미지 백업 제공 • 중앙 집중식 관리 및 모니터링을 통해 다수의 클라이언트를 효과적으로 관리할 수 있음 • 파일 및 애플리케이션 복원, 메일 서버 복원 등 다양한 복원 옵션 제공
 Cloud Sync	• 파일 및 폴더 수준의 동기화와 백업 지원 • 다양한 기기 간에 파일을 동기화할 수 있으며, 버전 관리를 통해 파일의 이전 버전을 복원할 수 있음
 Drive Backup Server	• Synology Drive에서 생성된 데이터를 안전하게 백업 • 파일, 폴더 및 버전을 선택적으로 백업할 수 있으며, 다중 버전의 파일 복원 및 파일 히스토리 조회 지원
 USB Copy	• 외부 USB 드라이브와 Synology NAS간에 저장된 데이터 복사기능 지원 • 사용자가 정의한 스케줄에 따라 주기적으로 자동 백업을 수행할 수 있음 • 다중 USB 디바이스와의 백업 지원
 Rsync Backup	• Rsync 프로토콜을 사용하여 리모트 서버와의 데이터를 동기화 제공 • 파일 또는 폴더 레벨의 백업 및 복원이 가능하며, 사용자가 정의한 주기로 자동 백업을 설정할 수 있음
 Snapshot Replication	• Btrfs 파일 시스템에서 지원하는 스냅샷을 활용한 블록 레벨의 백업 제공 • 효율적인 스냅샷 관리를 통해 스냅샷 크기를 최적화하고 공간을 절약할 수 있음 • 빠른 백업과 복원 속도 제공

Synology-20 NTP 서버 연동

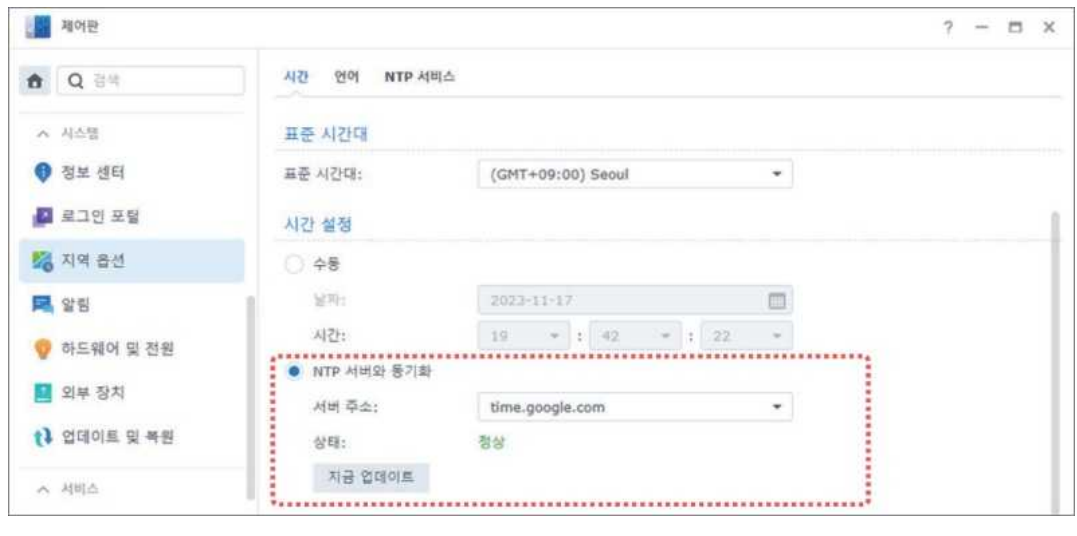
🛡️ 취약점 개요

점검 내용	• NTP 서버 연동 설정 적용 여부 점검
점검 목적	• 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과 관계 파악에 도움을 주고 로그 자체의 신뢰성을 확보하기 위함
보안 위협	• 시스템 간 시간 동기화 미흡으로 보안사고 및 장애 발생 시 로그에 대한 신뢰도 확보 미흡
점검 기준	양호 취약 NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우 NTP 서버와 연동되어 있지 않은 경우
참고	※ NTP(Network Time Protocol) : 네트워크를 통해 컴퓨터 시스템 간의 시간을 정확하게 유지 시켜주기 위한 네트워크 프로토콜. ※ Public NTP 서버 : 글로벌 IT 기업(Google, Microsoft), 비영리 단체(ntppool.org) 등에서 제공하고 있는 공개된 NTP 서버로 국내에서는 주요 통신사(LG유플러스, KT 등)에서 제공하고 있음

🛡️ 점검 및 조치방법

○ NTP 서버 연동 여부 점검

▶ [제어판] > [지역 옵션] > [시간] 탭에서 'NTP 서버와 동기화' 설정 여부 및 상태 확인



- ▶ NAS 장치가 폐쇄망 환경에서 운영되는 경우 별도 NTP 서버를 구축하여 내부 시스템 간 시간 동기화를 권장하며, [NTP 서비스] 탭에서 '**NTP 서비스 활성화**' 체크를 통해 NAS장치를 NTP 서버로 설정하여 운영할 수 있음



5.6 서비스 관리

Synology-21 불필요한 서비스 사용 금지

❖ 취약점 개요

점검 내용	• 사용하지 않는 서비스 활성화 여부 점검				
점검 목적	• 불필요한 서비스 활성화로 인한 시스템 성능 저하 및 잠재적인 보안 취약점 노출 위험을 예방하기 위해 불필요한 서비스 활성화 여부 점검				
보안 위험	• NAS 장치에서 제공되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침입의 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 서비스 사용이 비활성화된 경우</td></tr> <tr> <td>취약</td><td>불필요한 서비스 사용이 활성화된 경우</td></tr> </table>	양호	불필요한 서비스 사용이 비활성화된 경우	취약	불필요한 서비스 사용이 활성화된 경우
양호	불필요한 서비스 사용이 비활성화된 경우				
취약	불필요한 서비스 사용이 활성화된 경우				
참고	※ 서비스 사용이 필요한 경우에도 서비스 오남용 방지를 위해 계정(또는 그룹)별 사용 권한을 부여하여 필수 계정만 사용할 수 있도록 통제하는 것을 권장				

❖ 점검 및 조치방법

○ 불필요한 서비스 활성화 여부 점검 및 조치

- ▶ [제어판]에서 각 서비스에 대한 활성화 여부 확인 및 사용하지 않는 서비스 비활성화

서비스명	점검 방법
SMB	[제어판] > [파일 서비스] > [SMB]
AFP	[제어판] > [파일 서비스] > [AFP]
NFS	[제어판] > [파일 서비스] > [NFS]
FTP	[제어판] > [파일 서비스] > [FTP]
rsync	[제어판] > [파일 서비스] > [rsync]
Bonjour	[제어판] > [파일 서비스] > [고급]
SSDP	[제어판] > [파일 서비스] > [고급]
TFTP	[제어판] > [파일 서비스] > [고급]
Telnet	[제어판] > [터미널 및 SNMP] > [터미널]
SSH	[제어판] > [터미널 및 SNMP] > [터미널]
SNMP	[제어판] > [터미널 및 SNMP] > [SNMP]

- ▶ 위 서비스 목록 중 사용하지 않는 서비스가 활성화된 경우 ‘서비스 활성화’ 체크 해제하고, 사용이 필요한 경우 <Synology-02 계정별 권한관리> 항목을 참고하여 서비스별 사용 권한을 부여하여 이용하는 것을 권장



Synology-22 안전한 SNMP 서비스 사용

취약점 개요

점검 내용	안전한 SNMP 서비스 사용을 위한 보안 설정 점검								
점검 목적	- SNMP 서비스 사용 시 안전한 버전(V3) 사용을 권장 - V3 미만 버전의 SNMP 서비스를 사용하려면 유추하기 어려운 Community String을 설정하여 네트워크상에서 비인가자에게 시스템 정보가 노출되지 않도록 하여야 함								
보안 위협	SNMPv1, SNMPv2 버전을 사용할 때 Public, Private와 같은 디폴트 Community String이 변경되지 않고 그대로 사용될 경우, 이 String을 악용하여 환경설정 파일 열람 및 수정을 통한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 Dos공격까지 다양한 형태의 공격이 가능								
점검 기준	<table border="1"> <tr> <td>양호</td><td>SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우</td></tr> <tr> <td>취약</td><td>유추하기 쉬운 Community String이 설정된 경우</td></tr> </table>	양호	SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우	취약	유추하기 쉬운 Community String이 설정된 경우				
양호	SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우								
취약	유추하기 쉬운 Community String이 설정된 경우								
참고	※ SNMP(Simple Network Management Protocol) 프로토콜 : 네트워크 상태 및 성능을 모니터링하고 관리하기 위한 표준 프로토콜로 네트워크 장비, 서버, 프린터 등과 같은 장치의 구성 정보 수집 및 원격 모니터링을 제공 ※ SNMP 프로토콜 버전 <table border="1"> <thead> <tr> <th>버전</th><th>설명</th></tr> </thead> <tbody> <tr> <td>SNMPv1</td><td>SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약</td></tr> <tr> <td>SNMPv2c (SNMPv2)</td><td>일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시</td></tr> <tr> <td>SNMPv3</td><td>사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음</td></tr> </tbody> </table>	버전	설명	SNMPv1	SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약	SNMPv2c (SNMPv2)	일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시	SNMPv3	사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음
버전	설명								
SNMPv1	SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약								
SNMPv2c (SNMPv2)	일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시								
SNMPv3	사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음								

🔒 점검 및 조치방법

🔍 SNMP(Simple Network Management Protocol) 서비스 사용 버전 확인

① SNMPv3 사용

- ▶ NMS(Network Management) 솔루션에서 지원하는 SNMP 서비스 버전을 확인하여 SNMPv3를 지원하는 경우 해당 버전을 사용할 것을 권장('SNMPv3 서비스' 활성화)
- ▶ [제어판] > [터미널 및 SNMP] > [SNMP] 탭에서 사용하지 않는 'SNMPv1, SNMPv2c 서비스'는 체크 해제

② SNMPv1, SNMPv2c 사용

- ▶ SNMPv3를 지원하지 않아 SNMPv1, SNMPv2c 버전을 사용해야 하는 경우 public, private 같은 디폴트 값을 사용하지 않고, 유추하기 어려운 Community String값을 설정하여 이용하여야 함
- ▶ [제어판] > [터미널 및 SNMP] > [SNMP] 탭에서 'SNMPv1, SNMPv2c 서비스 활성화' 및 안전한 커뮤니티 값 설정

Synology-23 안전한 FTP 서비스 사용

취약점 개요

점검 내용	FTP 서비스 이용 시 안전한 설정을 유지하고 있는지 점검										
점검 목적	보안에 취약한 FTP 서비스 사용은 지양하고, FTP 서비스 사용이 필요한 경우 암호화된 파일 전송 프로토콜(FTPS, SFTP)을 사용하여 안전한 데이터 전송을 하기 위함										
보안 위협	FTP는 파일을 전송하기 위한 프로토콜로 계정과 패스워드를 암호화하지 않고 평문 전송하여 네트워크 스니핑 등의 위협으로부터 계정 정보 및 모든 전송 데이터에 대한 침해사고 가능성이 존재함										
점검 기준	<table border="1"> <tr> <td>양호</td><td>FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우</td></tr> <tr> <td>취약</td><td>FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우</td></tr> </table>	양호	FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우	취약	FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우						
양호	FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우										
취약	FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우										
참고	※ 파일 전송 프로토콜(FTP) 버전 <table border="1"> <thead> <tr> <th>버전</th><th>설명</th></tr> </thead> <tbody> <tr> <td>FTP (File Transfer Protocol)</td><td>기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)</td></tr> <tr> <td>SFTP (SSH File Transfer Protocol)</td><td>SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)</td></tr> <tr> <td>FTPS (FTP Secure)</td><td>FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)</td></tr> <tr> <td>FTPES (FTP over Explicit TLS/SSL)</td><td>FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)</td></tr> </tbody> </table> * SSL(Secure Sockets Layer) : 웹에서 데이터를 안전하게 전송하기 위해 사용되는 프로토콜 * TLS(Transport Layer Security) : SSL의 후속 프로토콜로, SSL 3.0의 보안 취약점을 보완하고 개선된 버전	버전	설명	FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)	SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)	FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)	FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)
버전	설명										
FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)										
SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)										
FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)										
FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)										

점검 및 조치방법

FTP 서비스 설정 확인

- ▶ [제어판] > [파일 서비스] > [FTP] 탭에서 **FTP 서비스 실행 여부**, **기본 포트 변경 여부**, **FTPS(또는 SFTP) 사용 여부** 등 점검

안전한 FTP 서비스 사용 설정

- ▶ **FTP 서비스를 사용하지 않는 경우** 서비스 중단
- ▶ **FTP 서비스 사용이 필요한 경우** 데이터 암호화를 제공하는 **FTPS, SFTP 프로토콜**을 사용하고, **기본 포트는 알려지지 않은 포트로 변경하여** 사용할 것을 권장

※ 기본 포트 : FTPS(21), SFTP(22)

The screenshot shows the Windows Control Panel with the 'FTP / FTPS' and 'SFTP' settings. In the 'FTP / FTPS' section, the 'FTP 서비스 활성화(암호화 없음)' checkbox is unchecked, and the 'FTP SSL/TLS 암호화 서비스(FTPS) 활성화' checkbox is checked. The '시간 초과' (Timeout) is set to 300 seconds. The 'FTP 서비스의 포트 번호 설정' (FTP service port number setting) is set to 1021. In the 'SFTP' section, the 'SFTP 서비스 활성화' checkbox is checked, and the '포트 번호' (Port number) is set to 1022.

※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

- ▶ [제어판] > [파일 서비스] > [FTP] > [고급 설정] 탭에서 '**FTP 파일 전송 로그 활성화**' 체크박스를 활성화하여 로그 가시성 확보
- ▶ '**익명 FTP 활성화**'가 설정되어 있는 경우 해제하여 익명 사용자의 접속을 차단하여야 함

※ 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 함

※ Anonymous FTP(익명 FTP) : 파일 전송을 위해서는 원칙적으로 상대방 컴퓨터를 사용할 수 있는 계정이 필요하나 누구든지 계정 없이도 anonymous 또는 ftp라는 로그인 명과 임의의 비밀번호를 사용하여 FTP를 실행할 수 있음

고급 설정

전송 설정

☒ FTP 파일 전송 로그 활성화

로그 보기

로그 내보내기 ▾

보안 설정

☐ 사용자 루트 디렉토리 변경

사용자 선택

☐ 익명 FTP 활성화

사용자는 "anonymous" 사용자 이름을 사용하여 FTP를 통해 공유 폴더에 접근할 수 있습니다.
"Anonymous FTP/WebDAV" 사용자가 공유 폴더에 대한 올바른 접근 권한을 할당 받도록 확인하십시오.



QNAP NAS 보안가이드

6.1 진단 항목	80
6.2 계정 관리	82
6.3 접근 관리	93
6.4 패치 및 보안 관리	104
6.5 로그 및 백업 관리	116
6.6 서비스 관리	121

06

06

QNAP NAS
보안 가이드

6.1 진단 항목

항목 분류	항목 코드	항목명
계정 관리	QNAP-01	기본 관리자 계정(default) 사용금지
	QNAP-02	계정별 권한 관리
	QNAP-03	불필요한 공용계정 및 휴면계정 관리
	QNAP-04	패스워드 만료 기간 설정
	QNAP-05	패스워드 복잡도 설정
	QNAP-06	로그인 실패 횟수 제한
접근 관리	QNAP-07	암호화 통신 및 기본포트 변경
	QNAP-08	Session Timeout 설정
	QNAP-09	USB 장치 사용금지
	QNAP-10	불필요한 공유폴더 미사용 및 암호화 활성화
	QNAP-11	MFA(Multi-Factor Authentication) 인증 적용 여부
	QNAP-12	UPnP 포트 포워딩 비활성화
패치 및 보안관리	QNAP-13	보안 카운셀러 보안점검 예약검사 적용
	QNAP-14	제조사에서 제공하는 최신 업데이트 적용
	QNAP-15	백신 프로그램 설치
	QNAP-16	백신 프로그램 최신 패턴 업데이트 및 예약검사 적용
	QNAP-17	방화벽 기능 활성화
로그 및 백업 관리	QNAP-18	로그 관리
	QNAP-19	백업 관리
	QNAP-20	NTP 서버 연동
서비스 관리	QNAP-21	불필요한 서비스 사용 금지
	QNAP-22	안전한 SNMP 서비스 사용
	QNAP-23	안전한 FTP 서비스 사용

23개 항목



유의사항

본 가이드는 NAS 취약점 평가항목에 대한 이해를 돕기 위해 항목설명, 점검기준, 점검방법, 대응방안을 제시하며 취약점 조치에 활용할 수 있습니다. 다만 일반적인 권고사항이므로 운영환경과 시스템에 미치는 영향을 검토하여 적용하여야 합니다.

※ 본 가이드 작성 기준은 QNAP NAS 장비의 GUI 기반으로 작성되었으며, 타제품 사용 시 각 항목에 해당하는 설정 탭의 모양, 설명, 현황 등이 제품에 따라 상이할 수 있으므로 각 제조사의 사용자 매뉴얼을 참고하여 본 가이드 안내에 따라 보안 설정할 것을 권고 드립니다.

6.2 계정 관리

QNAP-01 기본 관리자계정(default) 사용금지

❗ 취약점 개요

점검 내용	• 제조사가 생성한 기본 관리자계정(default) 사용 여부 점검										
점검 목적	• 이미 알려진 default 계정을 이용한 계정 접속 시도 및 탈취를 예방하기 위해 기본 관리자 계정의 비활성화 여부 점검										
보안 위협	• 공격자가 알려진 Default 계정 정보를 이용하여 무차별 대입 공격(Brute Force Attack), 사전 공격(Dictionary attack), 혼합 공격(Hybrid Attack), 레인보우 테이블 공격(Rainbow Table Attack) 등 패스워드 크래킹 공격을 통해 계정이 도용될 수 있으며, 이를 통해 시스템 가용성 훼손, 자료 유출 등의 위험이 존재함										
점검 기준	<table border="1"> <tr> <td>양호</td><td>기본 관리자계정(admin)를 사용하지 않는 경우</td></tr> <tr> <td>취약</td><td>기본 관리자계정(admin)를 사용하는 경우</td></tr> </table>	양호	기본 관리자계정(admin)를 사용하지 않는 경우	취약	기본 관리자계정(admin)를 사용하는 경우						
양호	기본 관리자계정(admin)를 사용하지 않는 경우										
취약	기본 관리자계정(admin)를 사용하는 경우										
참고	※ SQNAP NAS의 기본계정(default) : admin, guest ※ 대표적인 패스워드 크래킹 공격 <table border="1"> <thead> <tr> <th>서비스명</th><th>점검 방법</th></tr> </thead> <tbody> <tr> <td>무차별 대입 공격 (Brute Force Attack)</td><td>모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격</td></tr> <tr> <td>사전 공격 (Dictionary attack)</td><td>자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격</td></tr> <tr> <td>혼합 공격 (Hybrid Attack)</td><td>사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격</td></tr> <tr> <td>레인보우 테이블 공격 (Rainbow Table Attack)</td><td>해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격</td></tr> </tbody> </table>	서비스명	점검 방법	무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격	사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격	혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격	레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격
서비스명	점검 방법										
무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격										
사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격										
혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격										
레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격										

점검 및 조치방법

○ 제조사에서 제공된 기본 관리자계정(admin) 활성화 여부 확인

▶ [제어판] > [권한] > [사용자] 탭에서 admin 계정 상태 확인



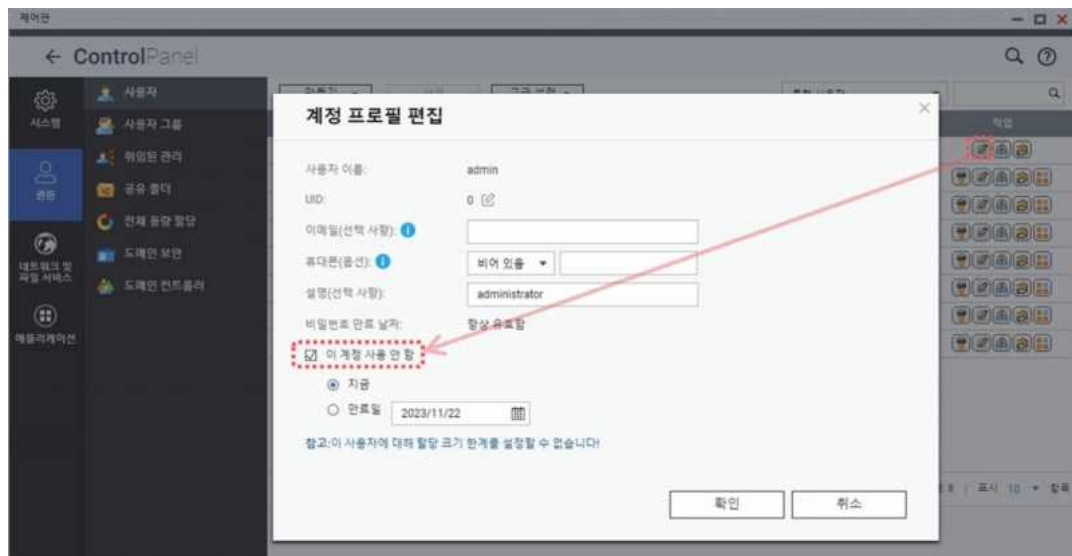
○ 새 관리자 계정 생성

- ▶ admin 계정 상태가 '사용'인 경우 비활성화를 위해 관리자 계정으로 사용할 신규 관리자 생성
- ▶ [제어판] > [권한] > [사용자] > [만들기] > [사용자 만들기] 기능을 통해 신규 관리자 생성 및 사용자 그룹에 'administrators (관리자 그룹)' 권한 부여



○ 기본 관리자 계정 비활성화

- ▶ 위 항목에서 신규 생성한 관리자 계정으로 로그인 후 기본 관리자계정(admin) 비활성화 진행
- ▶ [제어판] > [권한] > [사용자] > admin 계정 선택 > 작업그룹의 '계정 프로필 편집' 메뉴를 클릭하여 '이 계정 사용 안 함' 체크박스 선택 후 저장



○ 기본 관리자 계정 비활성화 여부 확인

■	사용자 이름	설명	할당	상태	작업
☐	admin	administrator	-	사용 안 함	  

QNAP-02 계정별 권한 관리

🛡️ 취약점 개요

점검 내용	• 사용자(계정)별 불필요한 권한 부여 여부 점검				
점검 목적	• 불필요하게 과도한 권한을 부여받은 사용자 계정을 통해 주요 설정 변경, 자료 유출 등을 방지하기 위함				
보안 위협	• 의도하지 않게 인가된 관리자 권한을 이용하여 NAS 장치의 주요 설정 변경, 시스템 침입 경로 노출, 자료 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우</td></tr> <tr> <td>취약</td><td>과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우</td></tr> </table>	양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우	취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우
양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우				
취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우				
참고	※ 관리자 권한은 최소한의 사용자(계정)에만 부여 ※ 업무별 목적에 맞게 적절한 권한으로 계정 부여				

🛡️ 점검 및 조치방법

○ 사용자 계정별 권한 확인

- ▶ [제어판] > [권한] > [사용자] > 점검대상 계정 선택 > 작업 그룹의 권한 관련 설정을 선택하여 부여된 권한 확인 및 불필요한 권한 회수
- ▶ 사용자 그룹 권한 점검 
- 불필요한 관리자 그룹(administrators) 권한 부여 여부 점검

사용자 그룹 편집

사용자 이름: nasuser1

☐

그룹 이름

☐

administrators

☒

everyone

▶ 공유폴더 접근 권한 점검

공유 폴더 권한 편집

✕

사용자 이름: nasuser1 Q

폴더 이름	미리보기	RO	RW	Deny
Container	액세스 거부	☐	☐	☐
Multimedia	읽기 전용	☐	☐	☐
Public	읽기 전용	☐	☐	☐
test3	액세스 거부	☐	☐	☐

※ 각 사용자는 기본적으로 포함된 '그룹 권한'을 상속받으며 사용자와 그룹 권한 사이에서 충돌이 발생한 경우 Deny (액세스 거부) > RW(읽기/쓰기) > RO(읽기 전용) 순으로 최종 권한이 결정됨

▶ 애플리케이션 사용 권한 점검

- 사용자 계정별 불필요한 서비스 권한 부여 여부 점검

애플리케이션 권한 편집

✕

사용자: nasuser1

서비스 이름	권한 부여
네트워크 서비스	☐
Apple 네트워크	☒
FTP 서버	☐
Microsoft 네트워크	☐
WebDAV	☒
애플리케이션	☒
File Station	☒

○ 그룹별 기본 권한 확인

- ▶ [제어판] > [권한] > [사용자 그룹] 탭에서 그룹별 기본 권한 확인 후 불필요한 권한 및 사용자 제거
- ▶ 특히 일반 사용자 그룹에 관리자 그룹과 동일 또는 유사한 권한 수준이 부여되어 있는지 확인하여 불필요한 권한은 회수

QNAP-03 불필요한 공용계정 및 휴면계정 관리

🛡️ 취약점 개요

점검 내용	불필요한 공용계정 및 미사용 휴면계정 존재 여부 점검				
점검 목적	- 불필요한 공용계정 및 미사용 휴면계정을 관리하여 비인가자의 접근 시도를 차단하고, 사용자별 개별 계정 부여를 통해 파일 변조, 정보 유출 등 사고 및 장애 발생에 대한 책임 추적성을 강화하기 위함 ※ 책임 추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				
보안 위협	관리되지 않는 휴면계정을 통한 비인가 접근의 위험이 존재하며, 공용계정 사용으로 인한 침해사고와 서비스 장애 발생 시 추적의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>공용계정 및 휴면계정을 관리하고 있는 경우</td></tr> <tr> <td>취약</td><td>공용계정 및 휴면계정이 관리되지 않는 경우</td></tr> </table>	양호	공용계정 및 휴면계정을 관리하고 있는 경우	취약	공용계정 및 휴면계정이 관리되지 않는 경우
양호	공용계정 및 휴면계정을 관리하고 있는 경우				
취약	공용계정 및 휴면계정이 관리되지 않는 경우				
참고	※ 계정의 공유를 금지하여야 하며, 1인 1계정 사용을 원칙으로함				

🛡️ 점검 및 조치방법

○ 사용자 계정 목록 확인

- ▶ [제어판] > [권한] > [사용자] 탭에서 사용자 계정 목록 확인
- ▶ 사용자 확인(인터뷰), 계정 관리대장 검토 등을 통해 공용계정 및 미사용된 장기 휴면계정 여부를 확인하여 불필요한 계정 삭제 조치

The screenshot shows the QNAP ControlPanel interface for user management. The left sidebar contains navigation options like '시스템' (System), '사용자' (Users), '권한' (Permissions), '공유 폴더' (Shared Folders), '전체 용량 할당' (Total Capacity Allocation), '도메인 보안' (Domain Security), '도메인 컨트롤러' (Domain Controller), and '백업/복원' (Backup/Restore). The main area displays a table of users with columns for '선택' (Select), '사용자 이름' (Username), '성명' (Full Name), '활동' (Status), '상태' (Role), and '작업' (Actions). The table lists users: admin (administrator, Not used, Administrator), user (User, Used, User), nuser1 through nuser5 (all Used, User), and nuser6 (Used, User). A red dashed box highlights the user list area.

QNAP-04 패스워드 만료 기간 설정

❏ 취약점 개요

점검 내용	패스워드(암호)의 최대 유효 기간 설정 여부 점검				
점검 목적	패스워드(암호)의 유효 기간을 설정하여, 사용자가 패스워드를 변경하도록 강제하여 비인가자가 불법 또는 임의로 획득한 패스워드의 무단 사용을 방지하기 위함				
보안 위협	장기간 변경하지 않은 패스워드를 지속적으로 사용하는 경우, 패스워드 크래킹 공격으로 패스워드가 노출될 위험성이 커지며, 임의로 획득한 패스워드를 무단 사용할 위험이 커짐				
점검 기준	<table border="1"> <tr> <td>양호</td><td>적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)</td></tr> <tr> <td>취약</td><td>적절한 패스워드 만료 기간 설정되지 않은 경우</td></tr> </table>	양호	적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)	취약	적절한 패스워드 만료 기간 설정되지 않은 경우
양호	적절한 패스워드 만료 기간 설정된 경우(90일 이내 권장)				
취약	적절한 패스워드 만료 기간 설정되지 않은 경우				
참고	※ 암호정책: 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 패스워드 만료 기간은 90일(3개월) 이내로 설정하는 것을 권장				

❏ 점검 및 조치방법

○ 최대 패스워드 유효 기간 설정 점검

- ▶ [제어판] > [시스템] > [보안] > [비밀번호 정책] 탭의 암호 만료 메뉴에서 '사용자가 정기적으로 암호를 변경해야 함' 체크박스 활성화 여부 및 '최대 비밀번호 사용 기간(일)' 설정 기간 확인



○ 최대 패스워드 유효 기간 설정

- ▶ ‘사용자가 정기적으로 암호를 변경해야 함’ 체크박스 선택 및 최대 비밀번호 사용 기간(90일 이내) 설정

암호 변경

☒ 사용자가 정기적으로 암호를 변경해야 함

최대 비밀번호 사용 기간(일)

☒ 암호 만료 일주일 전에 사용자에게 알림 이메일 전송 ⓘ

참고: ‘사용자가 정기적으로 암호를 변경해야 함’을 활성화하면 ‘사용자의 암호 변경 허용 안 함’이 비활성화됩니다.

※ ‘암호 만료 일주일 전에 사용자에게 알림 이메일 전송’을 활성화하여 사용자에게 경고 메시지를 제공을 권장하며, 이메일 전송을 위해서는 먼저 ‘제어판 > 시스템 > 알림센터’ 탭에서 ‘SMTP 서버 설정’을 구성하여야 함

QNAP-05 패스워드 복잡도 설정

🔒 취약점 개요

점검 내용	• 사용자 계정의 패스워드 복잡도 설정 여부 점검																
점검 목적	• 사용자 패스워드 복잡성 관련 정책이 설정되어 있는지 점검하여 쉽게 추측 가능한 패스워드로 인한 비인가자의 접근 차단하기 위함																
보안 위협	• 짧고 간단한 패스워드의 경우 자동화된 패스워드 크래킹 도구를 통한 패스워드 공격(무작위 대입, 사전 대입, 추측 공격 등)에 의해 쉽게 유추될 수 있으므로 복잡성 설정을 통해 패스워드를 알아낼 수 있는 평균 시간을 증가시킬 수 있도록 설정하여야 함																
점검 기준	<table><tr><td>양호</td><td>패스워드 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)</td></tr><tr><td>취약</td><td>패스워드 복잡도가 적절하게 설정되지 않은 경우</td></tr></table>	양호	패스워드 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)	취약	패스워드 복잡도가 적절하게 설정되지 않은 경우												
양호	패스워드 복잡도가 적절하게 설정된 경우(2조합 10자리 이상, 3조합 9자리 이상)																
취약	패스워드 복잡도가 적절하게 설정되지 않은 경우																
참고	※ 패스워드 복잡성 : 사용자 패스워드 설정 시 영문(대문자, 소문자), 숫자, 특수 문자가 혼합된 패스워드로 설정하는 방법 ※ 영문·숫자·특수문자 중 두가지 조합 시 최소 10자리 이상, 세 가지 조합 시 9자리 이상 패스워드 규칙 설정을 권장 <table><tr><th colspan="4">패스워드 조합 종류 및 구성 수</th></tr><tr><th>조합명</th><th>개수</th><th>조합명</th><th>개수</th></tr><tr><td>대문자</td><td>26개</td><td>숫자</td><td>10개</td></tr><tr><td>소문자</td><td>26개</td><td>특수 문자</td><td>32개</td></tr></table>	패스워드 조합 종류 및 구성 수				조합명	개수	조합명	개수	대문자	26개	숫자	10개	소문자	26개	특수 문자	32개
패스워드 조합 종류 및 구성 수																	
조합명	개수	조합명	개수														
대문자	26개	숫자	10개														
소문자	26개	특수 문자	32개														

🔒 점검 및 조치방법

○ 패스워드 복잡도 설정 여부 및 규칙 점검

- ▶ [제어판] > [시스템] > [보안] > [비밀번호 정책] 탭의 암호 길이 메뉴에서 패스워드 복잡도 설정 여부 확인



○ 비밀번호 복잡도 설정

- ▶ 비밀번호 복잡도 설정(2조합 최소 10자리 이상, 3조합 9자리 이상 설정)

암호 길이

다음 기준을 적용하여 암호 보안을 강화합니다.

다음 문자를 포함합니다:

☒ 영문자:

☒ 숫자

☒ 특수 문자

☒ 3회 이상 연속으로 반복되는 문자를 포함하지 않아야 함

☒ 연관된 사용자 이름 또는 반대 순서의 이름과 동일하지 않아야 함

☒ 최소 길이:

QNAP-06 로그인 실패 횟수 제한

❗ 취약점 개요

점검 내용	• 로그인 실패 허용 임계값 설정 여부 점검				
점검 목적	• 로그인 실패 임계값이 설정되어 있는지 점검하여 비인가자의 지속적인 로그인 시도를 차단하기 위함				
보안 위험	• 반복되는 로그인 실패에 대한 차단이 이루어지지 않으면 자동화된 패스워드 크래킹 도구를 통한 패스워드 공격(무작위 대입, 사전 대입, 추측 공격 등)에 취약하여 사용자 패스워드가 탈취될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하 권장)</td></tr> <tr> <td>취약</td><td>로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우</td></tr> </table>	양호	로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하 권장)	취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우
양호	로그인 실패 횟수 제한 설정이 적절하게 설정된 경우 (실패 횟수 5회 이하 권장)				
취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우				
참고	※ 계정 잠금 시간 : 로그인 실패로 계정이 잠기는 시간으로 관리자가 잠금 해제를 하거나 잠금 유지 시간이 경과되어야 재시도할 수 있음 ※ 로그인 실패 횟수는 5회 이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장				

❗ 점검 및 조치방법

○ 계정 보호 활성화 여부 점검

- ▶ [제어판] > [시스템] > [보안] > [계정 액세스 보호] 탭에서 'HTTP(S)' 활성화 여부 및 실패한 로그인 시도 설정 횟수 확인

※ 실패한 로그인 시도는 5회 이하로 설정할 것을 권장



※ HTTP(S) 설정은 관리자 웹 접근 시도에 대한 설정이며, HTTP(S) 외에도 사용하는 서비스의 계정 잠금 임계값을 설정할 수 있음

6.3 접근 관리

QNAP-07 암호화 통신 및 기본 포트 변경

🛡️ 취약점 개요

점검 내용	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜 사용 및 기본 포트를 변경하고 접근하고 있는지 점검				
점검 목적	웹 또는 터미널 접근 시 데이터를 암호화하여 전송하는 HTTPS와 SSH를 사용하여 비인가자의 데이터 스니핑에 대비하고, HTTPS와 SSH의 알려진 기본 포트를 변경하여 공격자의 접근을 어렵게 하기 위함				
보안 위협	공격자가 스니핑(Sniffing)을 시도하면 계정의 ID와 패스워드가 평문으로 노출되어 계정이 탈취될 위험이 존재하며, 잘 알려진 기본 포트를 사용하는 경우, 지속적인 패스워드 크래킹 또는 해킹 공격의 대상이 될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우</td></tr> <tr> <td>취약</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우</td></tr> </table>	양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우	취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우
양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우				
취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우				
참고	※ 스니핑(Sniffing) : 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청 장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말함				

🔍 점검 및 조치방법

🔴 NAS 웹 페이지 접근 시 보안 접속(HTTPS) 사용 여부 확인 ①

- ▶ [제어판] > [시스템] > [일반 설정] > [시스템 관리] 탭에서 '보안 연결(HTTPS) 사용', '강제 보안 연결(HTTPS)만 해당' 활성화 여부 및 기본 포트 변경 여부 점검

※ 기본 포트 : HTTP(80), HTTPS(443)



- ▶ '보안 연결(HTTPS) 사용', '강제 보안 연결(HTTPS)만 해당' 기능을 활성화하고, 기본 포트는 알려지지 않은 포트 번호로 변경하여 사용할 것을 권장



※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

○ 터미널을 통한 원격접근 시 보안 접속(SSH) 사용 여부 확인 ②

- ▶ [제어판] > [네트워크 및 파일 서비스] > [Telnet/SSH] 탭에서 'SSH 연결 허용' 활성화 여부 및 기본 포트 변경 여부 확인



- ▶ 터미널 접근 이용이 불필요한 경우 해당 설정을 해제하고, 사용이 필요한 경우 데이터를 평문으로 전송하는 Telnet 서비스의 사용은 권장하지 않으며, 암호화된 SSH 서비스의 기본 포트를 변경하여 사용하는 것을 권장

☐ 텔넷 연결 허용 (admin 계정만이 원격으로 로그인할 수 있습니다.)

포트 번호: 13131

☒ SSH 연결 허용 (관리자만 원격으로 로그인할 수 있습니다.)

포트 번호: 10022

☐ SFTP 활성화

액세스 권한 편집

※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

QNAP-08 Session timeout 설정

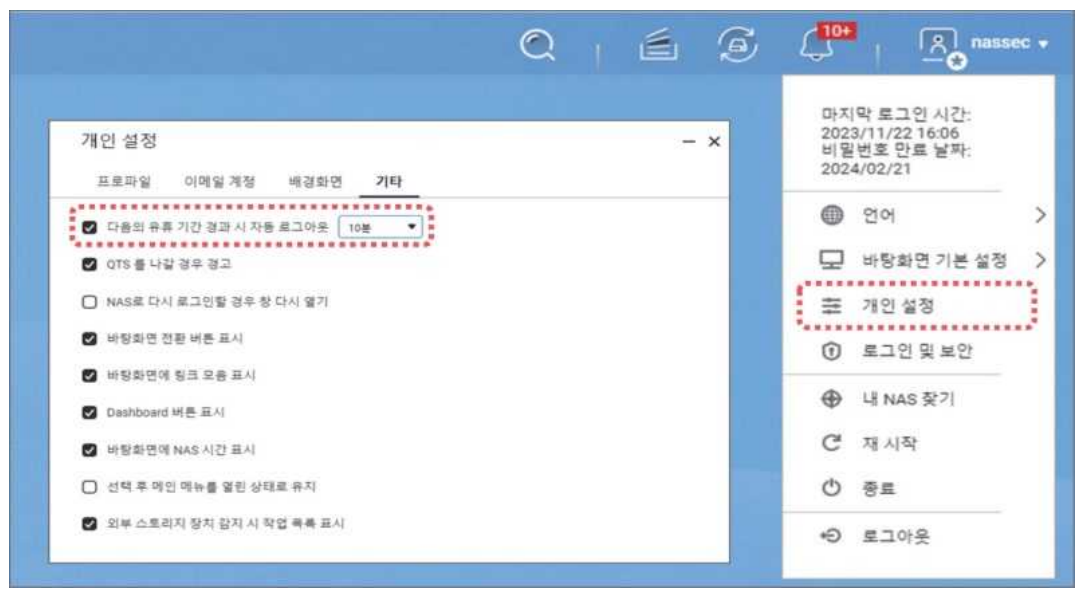
🔒 취약점 개요

점검 내용	• Session timeout(자동 로그아웃) 설정 적용 여부 점검				
점검 목적	• 사용자의 부주의로 계정이 로그인된 상태로 방치되는 상황을 방지하고, 사용하지 않는 세션을 종료하여 보안성과 가용성을 높이기 위한				
보안 위협	• 사용자가 작업 중 이석하거나 불안정한 세션 종료를 했을 경우, 권한 없는 사용자가 이석한 자리에서 정책 삭제나 변경 등 악의적인 행위를 하거나 불안정한 세션 종료를 한 세션 정보를 재사용하여 인증 없이 NAS 장치에 접근할 위험이 있음				
점검 기준	<table border="1"> <tr> <td>양호</td><td>Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)</td></tr> <tr> <td>취약</td><td>Session timeout(자동 로그아웃)이 설정되지 않은 경우</td></tr> </table>	양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)	취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우
양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)				
취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우				
참고	※ Session timeout : 로컬 또는 원격에서 장비에 접속한 사용자가 일정 시간 동안 통신이 없을 시 해당 세션을 종료시키는 설정 ※ 장비에 접속하여 이행하는 업무 특성을 고려하여 최소 시간 설정				

🔒 점검 및 조치방법

○ Session Timeout(자동 로그아웃) 시간 확인 및 권장 설정

- ▶ 관리자 웹 페이지에서 계정 ID를 클릭 후 [개인 설정] > [기타] 탭에서 '다음 유효기간 경과 시 자동 로그아웃' 시간 설정(15분 이내로 설정할 것을 권장)



QNAP-09 USB 장치 사용금지

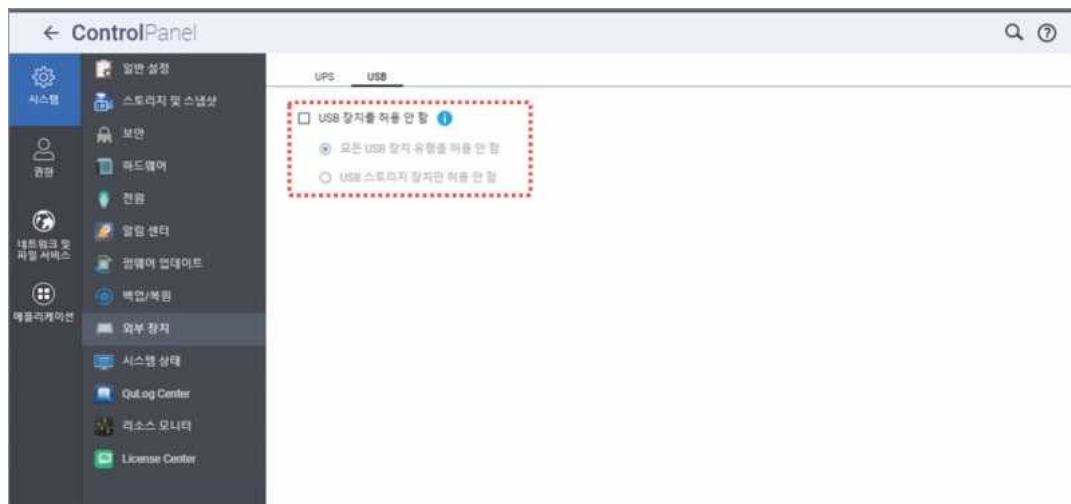
🔒 취약점 개요

점검 내용	• 이동식 저장매체(USB)의 사용금지 설정 여부 점검				
점검 목적	• NAS 장치에 USB 장치 사용을 강제적으로 제한하여, 비인가자의 물리적 접근을 통한 악성코드 감염과 데이터 유출 등의 위험을 차단하기 위한				
보안 위협	• 비인가자가 NAS 장치에 물리적 접근으로 USB를 통한 악성코드 감염, 데이터 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우</td></tr> <tr> <td>취약</td><td>USB 장치 사용금지 또는 권한이 설정되지 않은 경우</td></tr> </table>	양호	USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우	취약	USB 장치 사용금지 또는 권한이 설정되지 않은 경우
양호	USB 장치 사용금지 설정(또는 포트락 설치)이 되어 있거나, USB 장치 사용 권한이 적절하게 부여된 경우				
취약	USB 장치 사용금지 또는 권한이 설정되지 않은 경우				
참고	※ BAD USB : 비인가자가 USB 메모리 펌웨어의 소스 코드를 악의적인 코드로 변조하여 USB 연결 시 악성코드 자동 설치/실행되는 USB ※ 포트락(PortLock) : 데이터 유출이나 외부 침입을 방지하기 위해 입출력 포트를 물리적으로 봉인하여 통제하는 포트 잠금장치				

🔒 점검 및 조치방법

○ USB 장치 사용금지 설정 여부 점검

- ▶ [제어판] > [시스템] > [외부 장치] > [USB] 탭에서 'USB 장치를 허용 안 함' 활성화 여부 확인 및 권장 설정 (권장: USB 장치 사용금지)



QNAP-10 불필요한 공유폴더 미사용 및 암호화 활성화

❏ 취약점 개요

점검 내용	• 불필요한 공유 폴더의 존재 여부 및 암호화 활성화 여부 점검				
점검 목적	• 불필요하게 공유되고 있는 폴더가 있는지 확인하여 비인가자의 접근 가능성 차단과 이를 통한 자료 유출 방지				
보안 위협	• 관리되지 않는 불필요한 공유 폴더는 자료 유출, 악성코드 유포 경로로 활용될 수 있으며, 해당 폴더로 접근이 가능한 IP/Port가 노출되었을 경우, 비인가자에 의한 공격 대상이 될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우</td></tr> <tr> <td>취약</td><td>불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우</td></tr> </table>	양호	불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우	취약	불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우
양호	불필요한 공유 폴더를 제거하고, 중요 폴더에 대한 암호화가 적용된 경우				
취약	불필요한 공유 폴더가 존재하거나 중요 폴더에 암호화가 적용되지 않은 경우				
참고	※ 암호화 활성화 : 공유 폴더를 암호화하게 되면 NAS 장치(디스크)를 도난당하거나 분실하더라도 데이터를 안전하게 보호할 수 있음				

❏ 점검 및 조치 방법

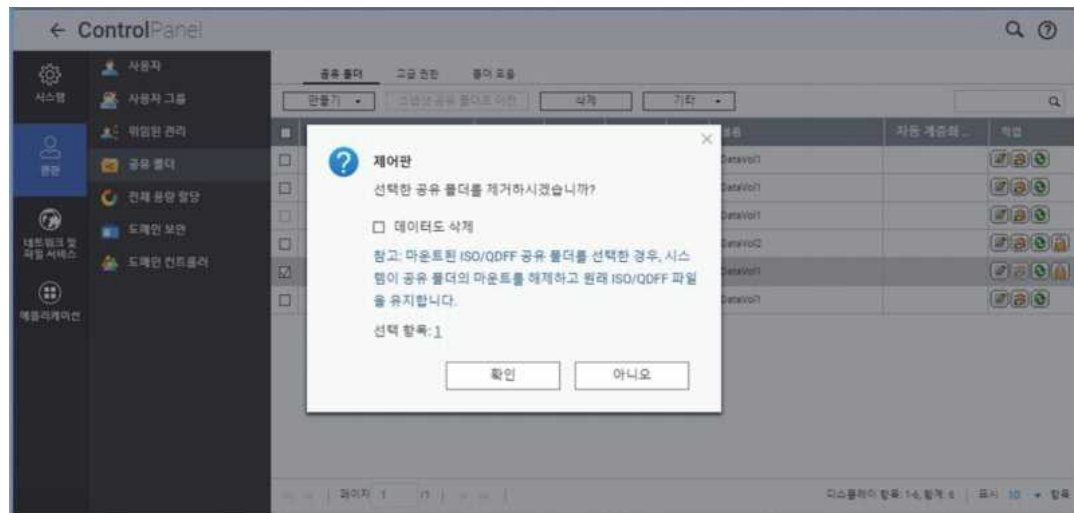
○ 공유폴더 목록 및 암호화된 폴더 확인

- ▶ [제어판] > [권한] > [공유폴더] 탭에서 ①**사용하지 않는 공유폴더 여부** 및 ②**중요한 폴더에 대한 암호화 적용 여부** 확인

※ 폴더 우측에 작업 컬럼에 자물쇠 아이콘이 있으면 암호화가 적용된 폴더

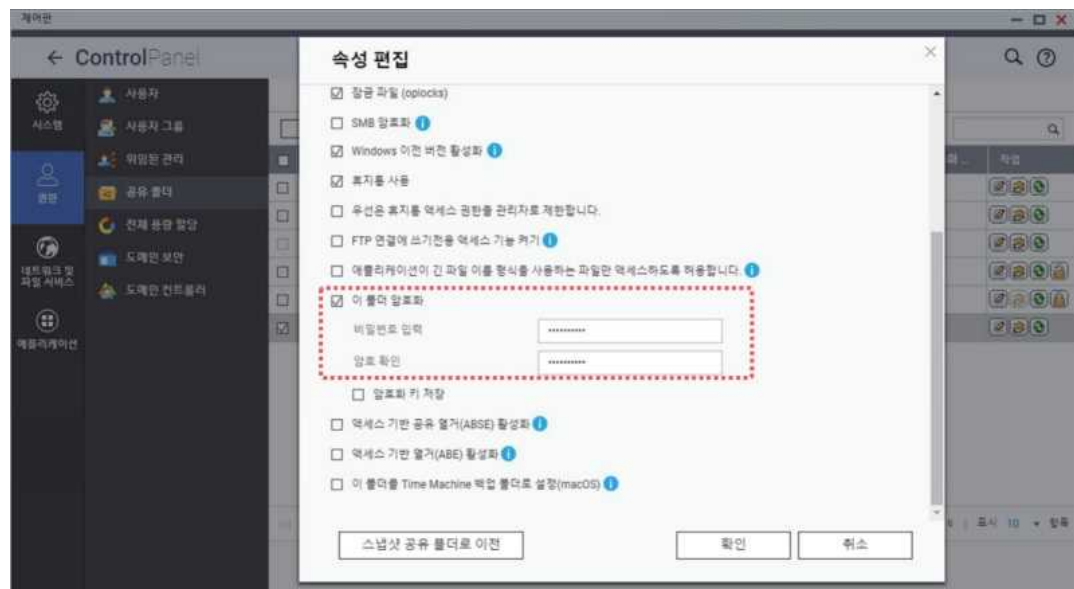


○ 불필요한 공유폴더 삭제 조치



○ 중요 폴더 암호화 적용

- ▶ 암호화를 적용할 폴더 선택 후 [속성 편집] 탭에서 ‘이 공유폴더 암호화’ 활성화 및 암호키를 입력하여 폴더 암호화 적용



※ 암호키를 분실할 경우 암호화된 폴더에 접근할 수 없으므로 분실하지 않도록 주의하여야 함

QNAP-11 MFA(Multi-Factor Authentication) 인증 적용 여부

❗ 취약점 개요

점검 내용	사용자 계정에 대한 다중인증(MFA) 설정 여부 점검				
점검 목적	두 가지 이상의 인증 방식을 통해 피싱, 사회 공학적 기법, 무차별 대입 공격 등과 같은 공격을 통한 비인가자의 접속을 방지하기 위함				
보안 위협	비인가자가 패스워드 크래킹, 크리덴셜 스테핑 등이나 피싱, 사회 공학적 기법 등을 통해 계정 정보를 탈취하게 되면, 시스템 관리자 권한으로 접속하여 보안 설정 임의 조작, 데이터 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>사용자 계정에 MFA 인증이 적용된 경우</td></tr> <tr> <td>취약</td><td>사용자 계정에 MFA 인증이 적용되지 않은 경우</td></tr> </table>	양호	사용자 계정에 MFA 인증이 적용된 경우	취약	사용자 계정에 MFA 인증이 적용되지 않은 경우
양호	사용자 계정에 MFA 인증이 적용된 경우				
취약	사용자 계정에 MFA 인증이 적용되지 않은 경우				
참고	※ 크리덴셜 스테핑 : 비인가자(공격자)가 기존에 노출된 계정 정보를 통하여 다른 플랫폼에 무작위로 대입해보며 사용자의 계정을 탈취하는 공격 ※ Multi-Factor 인증(MFA) : 사용자에게 암호 이외의 추가 정보를 입력하도록 요구하는 다중 단계 사용자 인증 방식				

❗ 점검 및 조치방법

○ 2단계 인증(2SV) 활성화 여부 점검

▶ [제어판] > [시스템] > [보안] > [2단계 인증] 탭에서 사용자 계정별 2단계 인증 적용 여부(상태) 확인

ControlPanel

하위/가부 목록 | IP 액세스 보호 | 계정 액세스 보호 | SSL 인증서 및 개인 키 | 비밀번호 정책 | **2단계 인증**

2단계 인증

2단계 인증(2SV)은 사용자가 NAS에 로그인할 때마다 추가로 일회성 보안 코드를 요구함으로써 사용자 계정에 추가적인 보호 계층을 더해줍니다. 특정 사용자 및 그룹에 대해 2단계 인증을 실시할 수 있습니다.

참고: 그룹 내 그룹과 사용자 간에 '2SV 실시' 구성이 일관되지 않을 수 있습니다. 사용자에 대한 최종 2SV 상태를 확인하려면 '상태'를 참조하십시오.

2SV 실시	사용자 이름	성명	상태
☐	admin	administrator	사용 안함
☐	user		사용 안함
☐	nasuser1		사용 안함
☐	nasuser2		사용 안함
☐	nasuser3		사용 안함

디스플레이 항목: 1-4, 항목: 8 | 표시: 10 | 항목

▶ 2단계 인증을 적용할 사용자 계정 선택 후 '적용' 버튼 클릭

☒ 2SV 설치	사용자 이름	설명	상태
☒	nasuser3		사용 안함
☒	nasuser4		사용 안함
☒	nasuser5		사용 안함
☒	nassec		사용 안함
☒	nasadmin		사용 안함

적용

○ 2단계 인증(2SV) 추가설정(개별 사용자 계정 로그인 시)

▶ 2단계 인증의 최종 활성화는 각 사용자 계정의 최초 로그인 시 복구 이메일 설정, 인증 방법 선택 등 추가 설정을 진행해야 하며, 제조사에서 제공하는 'QNAP Authenticator' 모바일 앱을 통해 완료할 수 있음

인증 방법 선택:

- ☒ 보안 코드(TOTP)
인증 앱에서 보안 코드 받기(모바일 장치를 NAS에 연결하지 않아도 됩니다.)
- ☐ QR 코드
"QNAP Authenticator" 모바일 앱으로 QR 코드 스캔
- ☐ 로그인 승인
모바일 장치로 로그인 요청 승인
- ☐ 온라인 인증 코드
모바일 장치로 인증 코드 받기

시작

QNAP NAS68F505

< nasadmin

인증 앱에서 생성한 보안 코드(TOTP)를 입력하십시오.

02:54

☐ 이 장치에서 다시 인증하지 않음

다음

[다른 방법 시도](#)

QNAP-12 UPnP 포트 포워딩 비활성화

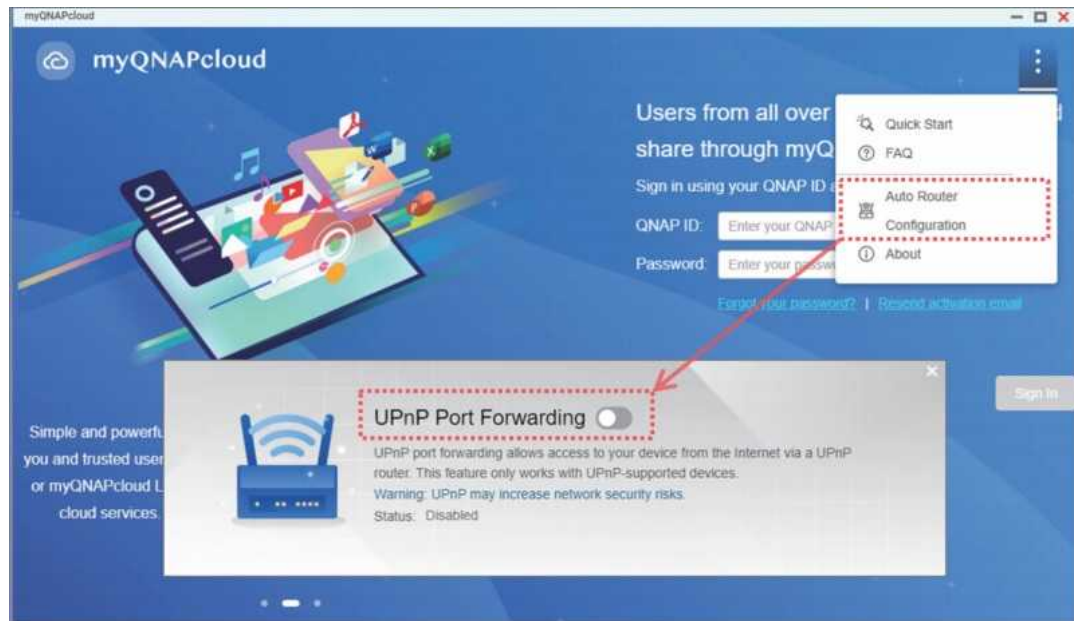
취약점 개요

점검 내용	제조사에서 제공하는 UPnP(Universal Plug and Play) 기능 사용 여부 점검				
점검 목적	UPnP의 특성상 외부에서 내부 네트워크에 연결된 장치를 확인할 수 있는 취약점이 존재하여 UPnP를 통한 내부 공격을 사전 예방하기 위함				
보안 위협	UPnP를 통해 사용자의 내부 LAN을 검색하여 내부에서 사용 중인 여러 주변 장치가 공격에 노출될 위험이 존재하며, 비인가자가 인가된 단말기기로 가장해 UPnP에 요청을 전송하면 연결된 모든 장치의 정보 노출의 위험이 존재함				
점검 기준	<table> <tr> <td>양호</td><td>UPnP 기능이 비활성화되어 있는 경우</td></tr> <tr> <td>취약</td><td>UPnP 기능이 활성화되어 있는 경우</td></tr> </table>	양호	UPnP 기능이 비활성화되어 있는 경우	취약	UPnP 기능이 활성화되어 있는 경우
양호	UPnP 기능이 비활성화되어 있는 경우				
취약	UPnP 기능이 활성화되어 있는 경우				
참고	※ UPnP(Universal Plug and Play) : 자동으로 포트를 구성하는 프로토콜로, 포트 포워딩을 자동으로 설정해 네트워크 내 응용프로그램과 장치들을 서로 연결할 수 있도록 함. 주변 장치를 빠르게 연결할 수 있는 편의성을 제공해 주지만 보안에 취약함 ※ 포트포워딩(port forwarding) : 컴퓨터 네트워크 상에서 패킷이 방화벽이나 라우터 같은 네트워크 게이트를 지날 때 IP 주소와 포트 번호 결합의 통신 요청을 다른 곳으로 넘겨주는 네트워크 주소 변환을 해주는 기능				

🔍 점검 및 조치방법

○ UPnP 포트포워딩 활성화 여부 점검

- ▶ [myQNAPcloud] 앱 실행 > 우측상단 설정(:) 모양 클릭 > [Auto Router Configuration] 탭에서 UPnP 활성화 여부 확인 및 해제



※ 최근 QNAP에서는 데이터 보안을 유지하기 위해 UPnP 기능을 비활성화하여 출고하고 있음. 단, 장비 모델별 설정값이 상이할 수 있으므로 반드시 해당 메뉴를 통해 활성화 여부 점검을 권장함

6.4 패치 및 보안 관리

QNAP-13 보안 카운셀러 보안점검 예약검사 적용

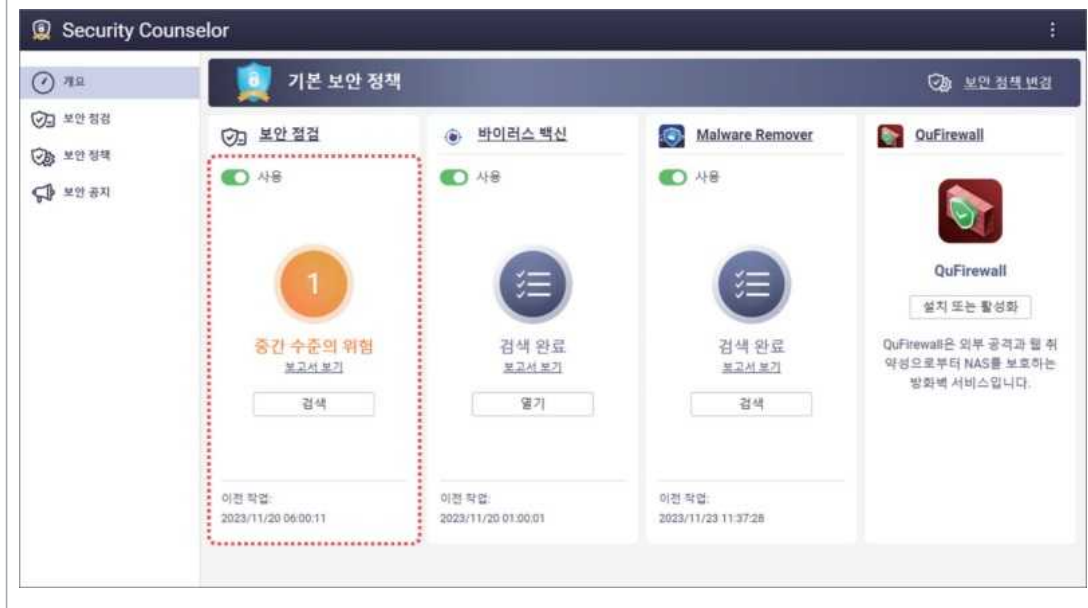
❶ 취약점 개요

점검 내용	• 보안 카운셀러를 통한 정기 예약검사(보안 점검) 활성화 여부 점검
점검 목적	• 정기적인 예약 검사를 통해 NAS 장치의 장애, 설정상의 보안 취약점, 최신 업데이트 등 위험을 지속적으로 관리하기 위함
보안 위협	• NAS 장치 내 악성코드 감염, 시스템 장애 및 경고, 취약한 설정 및 최신 업데이트 등을 적용하지 않아 시스템 장애 발생, 제로데이 공격, 악성코드 감염 등의 위험이 존재함
점검 기준	양호 취약
참고	※ 보안 카운셀러 : QNAP NAS 장치에서 제공되는 보안 프로그램으로 장치의 보안 상태를 주기적으로 모니터링하고 필요한 보안 권고사항 알려주어 효과적으로 보안관리를 할 수 있는 자가진단도구

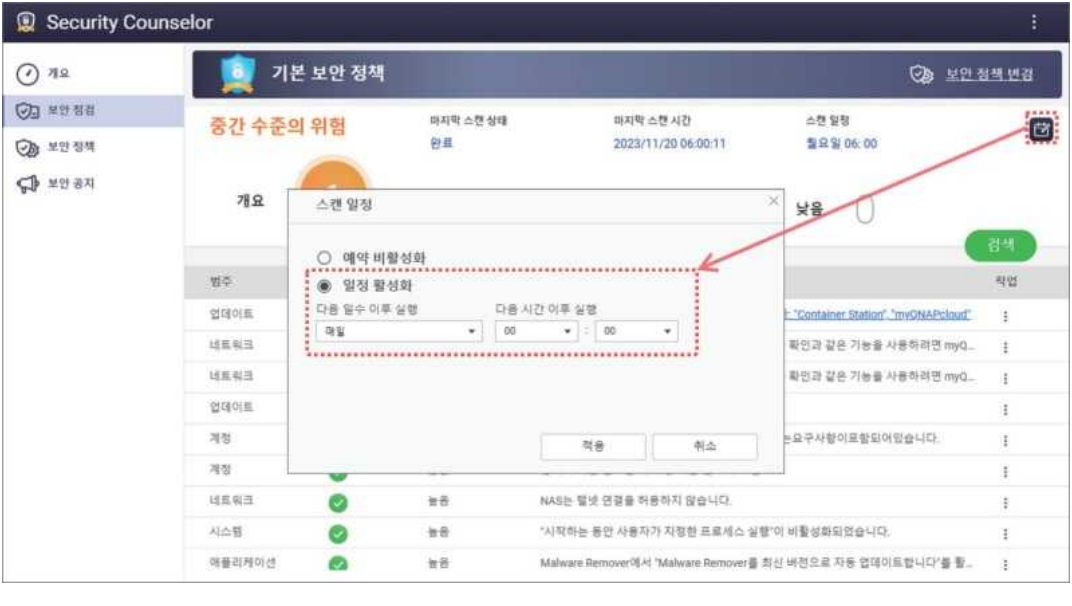
❷ 점검 및 조치방법

○ 보안 카운셀러 사용 및 예약검사 설정 여부 점검

▶ [Security Counselor] 앱 실행 후 '보안 점검' 기능 사용 여부 점검



▶ [보안 점검] 탭의 우측  모양(스캔 설정)을 클릭 후 예약검사 일정 등록



Security Counselor 기본 보안 정책 화면. 중앙에 '스캔 일정' 팝업이 표시되어 예약 검사 설정을 할 수 있다. 팝업에는 '예약 비활성화'와 '일정 활성화' 옵션이 있으며, '일정 활성화'가 선택되어 있다. '다음 일수 이후 실행'과 '다음 시간 이후 실행'을 선택할 수 있는 드롭다운 메뉴와 시간 설정 필드가 있다. 오른쪽 상단에는 '모양(스캔 설정)' 아이콘이 빨간 선과 화살표로 강조되어 있다.

QNAP-14 제조사에서 제공하는 최신 업데이트 적용

❏ 취약점 개요

점검 내용	• 제조사에서 제공하는 펌웨어의 최신 업데이트 여부 점검				
점검 목적	• 최신 업데이트를 적용하여 NAS 장치의 보안성과 시스템 안정성 확보				
보안 위협	• 최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 이용하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우</td></tr> </table>	양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우	취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우
양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우				
취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우				
참고	※ 펌웨어(Firmware) : 프로그래밍의 일종인 펌웨어는 하드웨어를 제어하는 소프트웨어 운영체제 프로그램으로 하드웨어 제어를 통해 하드웨어 역할을 하는 하드웨어와 소프트웨어의 중간자 역할 수행				

❏ 점검 및 조치방법

○ 업데이트 현황 확인

▶ [제어판] > [시스템] > [펌웨어 업데이트] 탭에서 최신 업데이트 적용 여부 확인



○ 최신 업데이트 적용

▶ 새로운 펌웨어 업데이트가 있는 경우 최신 업데이트 적용

※ 업데이트 시 시스템을 재기동해야 하는 경우가 있으므로 진행 중인 작업이 있는 경우 이를 고려하여 업데이트 진행



- ▶ NAS 장치가 인터넷 연결이 없는 내부망 환경에 구축된 경우 제조사 홈페이지에서 업데이트 패치 파일 다운로드 후 [수동 설치] 탭에서 수동 업데이트 진행



※ QNAP 다운로드 센터 : <https://www.qnap.com/ko-kr/download>

○ 최신 업데이트 적용 확인



QNAP-15 백신 프로그램 설치

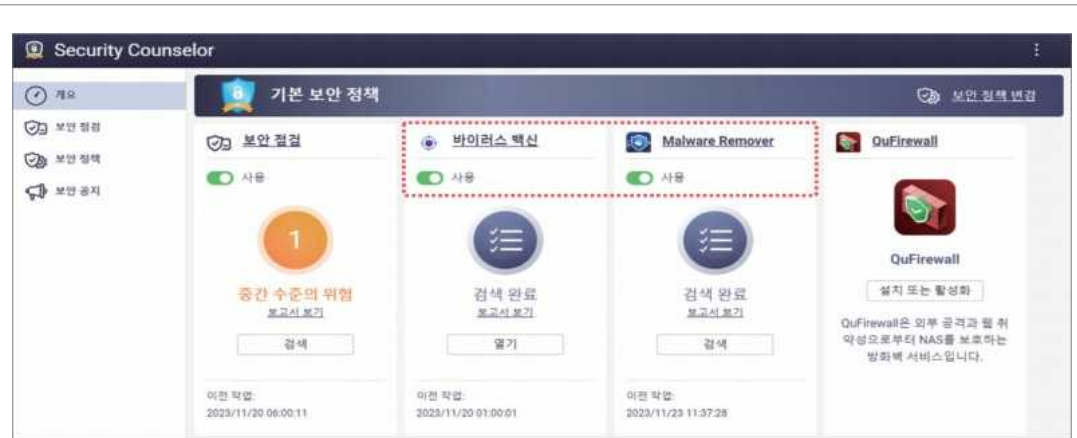
🛡️ 취약점 개요

점검 내용	• 백신 프로그램 활성화 여부 점검				
점검 목적	• 백신 프로그램을 설치하여 악성코드 감염을 예방하기 위함				
보안 위협	• 랜섬웨어, 웜, 트로이목마 등의 바이러스가 감염된 파일의 공유로 인하여 데이터 손실, 개인정보 유출, 시스템 손상 등과 같은 피해가 발생할 위험이 존재함				
점검 기준	<table> <tr> <td>양호</td><td>백신 프로그램을 설치하여 운영하고 있는 경우</td></tr> <tr> <td>취약</td><td>백신 프로그램을 설치하지 않은 경우</td></tr> </table>	양호	백신 프로그램을 설치하여 운영하고 있는 경우	취약	백신 프로그램을 설치하지 않은 경우
양호	백신 프로그램을 설치하여 운영하고 있는 경우				
취약	백신 프로그램을 설치하지 않은 경우				
참고	※ 바이러스(Virus) : 실행 파일의 일부분을 변형하여, 그곳에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합으로, 컴퓨터 내에 침투하여 자료를 손상시키거나, 다른 프로그램들을 파괴하여 작동할 수 없도록 하는 컴퓨터 프로그램의 한 종류 ※ 악성코드(Malware) : 바이러스(virus), 웜(worm), 트로이 목마(trojan)와 기타 유해한 컴퓨터 프로그램을 통틀어 일컫는 용어 ※ 랜섬웨어(Ransomware) : 악성코드의 일종으로 감염 시 화면이 차단되거나, 저장된 데이터를 암호화하여 데이터 복구를 위한 댓가를 요구하기도 함 ※ 웜(Worm) : 악의적인 목적을 가지고 자기 자신을 복제하여 전파시키며, 주로 네트워크 공유 폴더나 메일로 전파 ※ 트로이목마(Trojan) : 고의적으로 악의적 목적이 있는 파일, 주로 다른 악성코드나 위장된 프로그램으로 전파되거나 인터넷을 통해 다운로드 ※ 스파이웨어(Spyware) : 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어				

🛡️ 점검 및 조치방법

● 백신 프로그램 사용 여부 확인

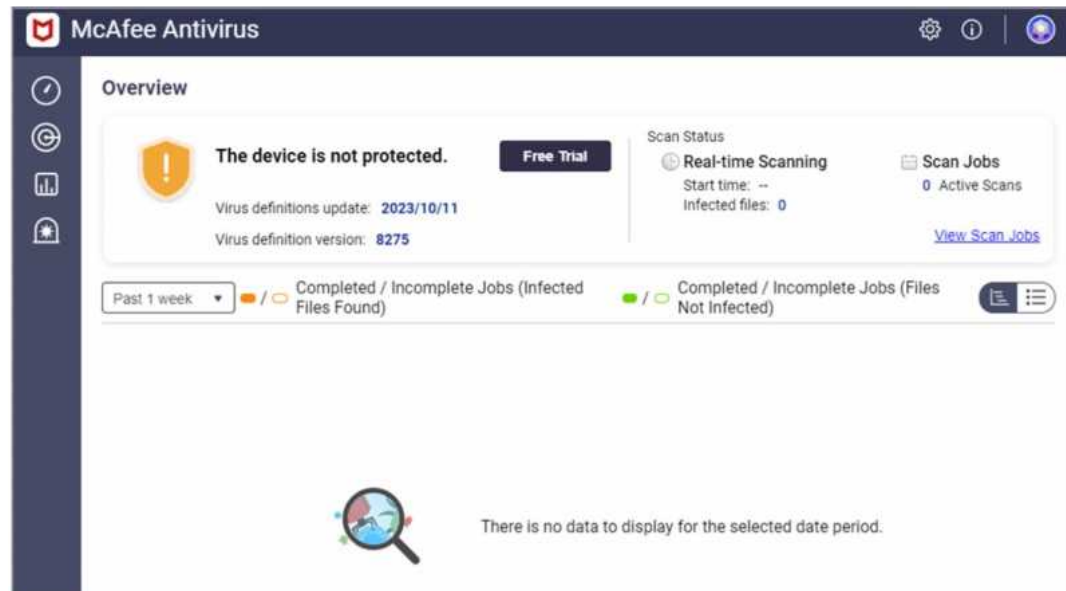
- ▶ QNAP NAS 장치에서는 악성코드 탐지를 위해 2종의 보안 프로그램을 제공하고 있으며, 두 가지 도구를 함께 사용하여 종합적인 보안을 통해 NAS 장치를 보호할 수 있음
- ▶ [보안 카운셀러] 앱 > [개요] 탭에서 ‘바이러스 백신’, ‘Malware Remover’ 사용 여부 점검



※ 바이러스 백신 (Virus Scanner) : 주로 바이러스 및 악성코드에 중점을 두고 파일 시스템을 스캔하며, 파일의 시그니처와 행동 패턴을 분석하여 악성코드를 탐지한다.

※ Malware Remover : 악성코드를 포함한 스파이웨어, 애드웨어 등 다양한 악성 소프트웨어를 대상으로 하며, 정의된 악성코드 패턴을 기반으로 스캔을 수행한다.

▶ 고급 백신 필요 시 유료 백신(McAfee)도 라이선스 비용을 지급하고 이용할 수 있음



※ Antivirus by McAfee (상용) : 백신 전문 글로벌 기업인 McAfee에서 개발한 백신 솔루션으로 추가 라이선스 구매가 필요하지만 심층 보안 엔진을 기반으로 상대적으로 강력한 악성코드 탐지 기능 제공

QNAP-16 백신 프로그램 최신 패턴 업데이트 및 예약검사 적용

❏ 취약점 개요

점검 내용	• 패턴 자동 업데이트 및 예약검사 설정 여부 점검
점검 목적	• 설치되어 있는 백신의 최신 엔진(패턴) 적용 및 자동 업데이트 설정 여부를 점검하여 최신 악성코드(바이러스, 웜, 랜섬웨어, 스파이웨어 등)의 감염을 방지하기 위함
보안 위협	• 백신 프로그램의 주기적인 패턴 업데이트가 적용되지 않으면, 신종 악성코드(바이러스, 웜, 랜섬웨어 등)를 탐지하지 못하여 시스템이 악성코드에 감염될 위험이 존재함
점검 기준	양호 최신 패턴 업데이트 및 예약검사 설정이 적용된 경우 취약 최신 패턴 업데이트가 미적용되어 있거나, 예약검사 설정이 되어있지 않은 경우
참고	※ 패턴 : 백신 소프트웨어는 컴퓨터 바이러스들의 패턴을 정의한 뒤, 해당 패턴과 일치하는 파일은 바이러스에 감염되었다고 판단하게 되며, 새로운 형태의 바이러스를 탐지하기 위해서는 바이러스의 형태를 정의한 패턴을 업데이트해야 함

❏ 점검 및 조치방법

○ 백신 프로그램 최신 패턴 업데이트

① 바이러스 백신(Virus Scanner)

- ▶ [제어판] > [애플리케이션] > [바이러스 백신] > [개요] 탭에서 바이러스 백신 상태를 확인하여 최신상태 ('업데이트 완료')가 아닌 경우 하단 '지금 업데이트' 버튼으로 최신 업데이트 적용



- ▶ NAS 장치가 내부망 환경에 구축되어 인터넷 연결이 불가할 시 백신社 홈페이지에서 패치 파일을 다운로드 후 '수동 업데이트' 진행

※ 백신 패턴(정의) 다운로드 주소

- bytecode.cvd : <http://database.clamav.net/bytecode.cvd>
- daily.cvd : <http://database.clamav.net/daily.cvd>
- main.cvd : <http://database.clamav.net/main.cvd>

② Malware Remover

▶ [Malware Remover] 앱 > [설정] 탭에서 '멀웨어 정의 업데이트 후 즉시 스캔' 활성화



○ 백신 프로그램 예약검사 설정

① 바이러스 백신(Virus Scanner)



▶ [제어판] > [애플리케이션] > [바이러스 백신] > [스캔 작업] 탭에서 '스캔 작업 추가' 버튼 클릭 후 예약 검사 일정 등록

② Malware Remover

▶ [Malware Remover] 앱 > [설정] 탭에서 '예약 스캔 활성화' 적용 후 스캔 일정 등록



QNAP-17 방화벽 기능 활성화

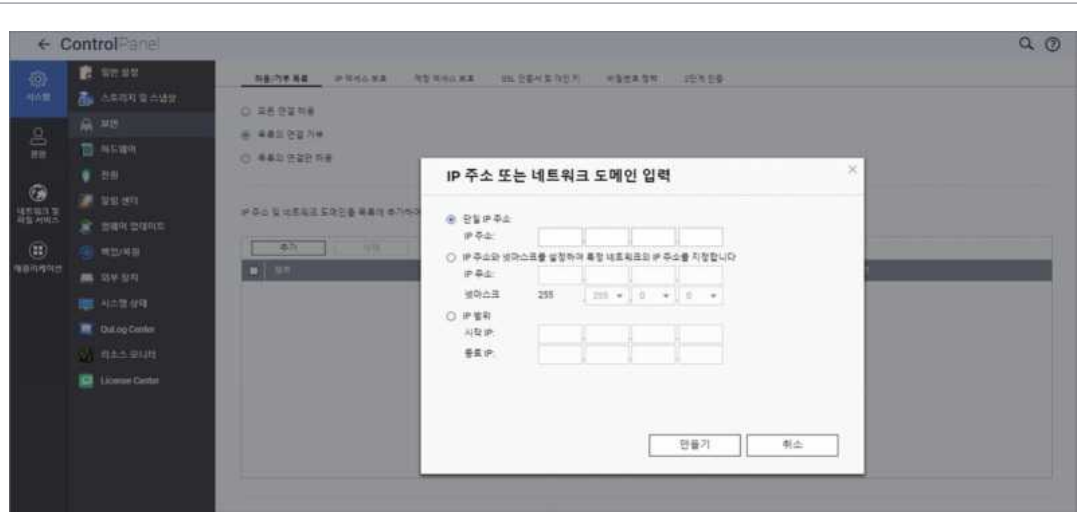
🔒 취약점 개요

점검 내용	• 방화벽 기능 활성화 및 정책 설정 적용 여부 점검				
점검 목적	• 방화벽 기능 활성화하고 접근통제 정책 설정을 적용하여 비인가자 IP의 무분별한 접근을 사전에 차단하고, 침해사고 발생 시 책임추적을 용이하게 하기 위함				
보안 위협	• 방화벽 설정으로 적절한 접근통제가 이루어지지 않을 경우, 불법 접근 및 데이터 유출, 서비스 거부 공격 등의 외부 공격으로부터 다양한 보안 위협에 노출될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우</td></tr> </table>	양호	방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우	취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우
양호	방화벽을 활성화하여 접근통제 정책을 적용하고 있는 경우				
취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우				
참고	※ 방화벽 : 접근 제어, 패킷 필터링, 로그 및 감사 등을 지원하는 네트워크 보안 장비의 하나로, 기본적으로 출발지 IP, 목적지 IP와 Port를 사용하여 접근통제 정책을 설정함 ※ 화이트리스트 방식 : 기본적으로 모든 접근을 막아놓고 액세스 허용 목록을 통해 접근 허용 대상만 따로 등록하는 방식 ※ 블랙리스트 방식 : 기본적으로 모든 접근을 허용하되 특정 사람, 웹 사이트, 프로그램 등을 차단하는 액세스 거부 목록을 통해 접근하지 못하는 예외를 두는 방식				

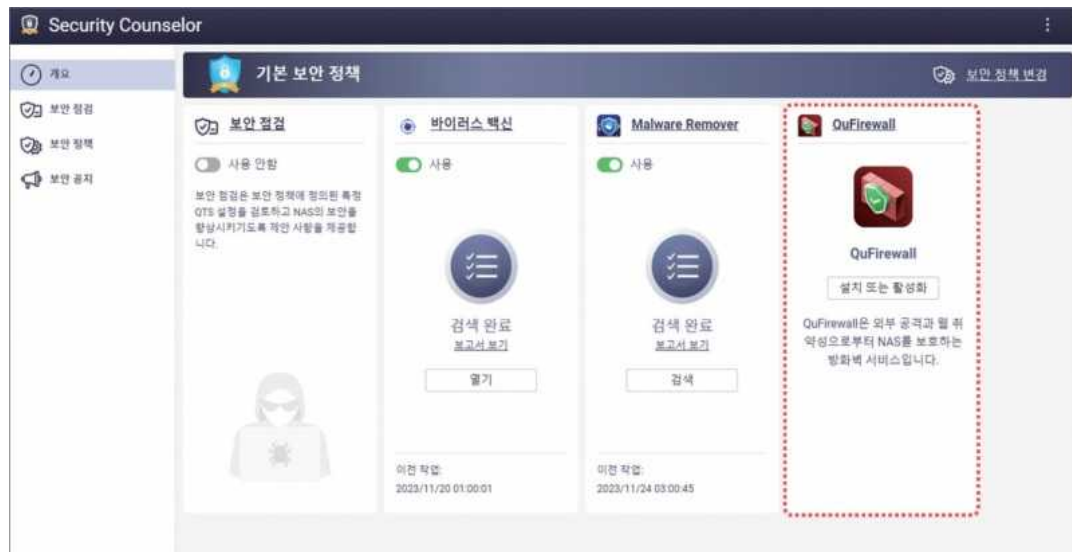
🔒 점검 및 조치방법

○ 방화벽 기능 활성화 여부 점검

- ▶ QNAP NAS 장치에서는 IP 기반 접근 제어 설정을 위해 제어판의 허용/거부 목록 설정 또는 방화벽 앱을 통한 설정 두 가지 방식을 제공하고 있음
- ※ [제어판] > [시스템] > [보안] > [허용/거부 목록]
- ▶ 단 제어판 허용/거부 목록 설정을 통한 방식은 IP 주소(또는 대역)으로만 접근 제어 설정이 가능하여 특정 국가 단위의 정책 설정은 제공하지 않음

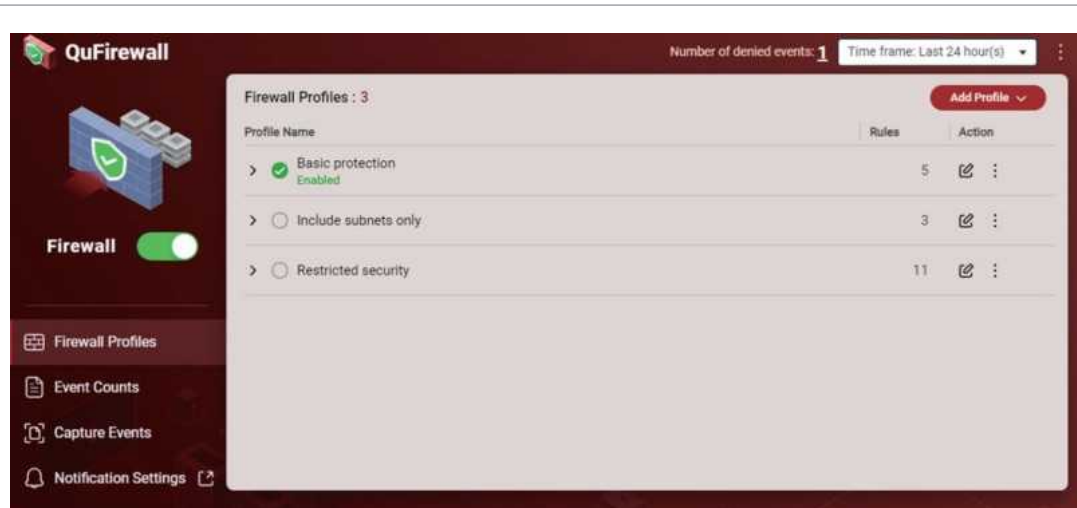


▶ 따라서 앱 센터 또는 보안 카운셀러 앱에서 방화벽 앱(QuFirewall)을 설치하여 이용하는 것을 권장



○ 방화벽 신규 정책 생성(해외 IP 차단)

▶ QuFirewall 앱에서는 세 가지 기본 정책 세트(Profile)를 제공하고 있으며 'Basic Protection'에 특정 국가만 접근을 허용하는 정책을 포함하고 있음



※ 기본 제공 정책(Profile)

- Basic protection : NAS 장치를 사용하는 특정 국가만 접근을 허용하는 정책
- Include subnets only : 로컬 네트워크에서만 접근을 허용하는 정책
- Restricted security : 로컬 네트워크에서만 QTS 웹 및 앱 접근을 허용하고, 외부에서는 VPN을 통해서만 접근을 허용하는 정책 및 앱 접근을 허용하고, 외부에서는 VPN을 통해서만 접근을 허용하는 정책

- ▶ 특정 국가에 대한 접근 제어를 위해서는 기본 제공 정책에 추가하거나 신규정책을 생성하여 국가 단위의 접근 제어를 설정할 수 있음

※ 기본 제공 정책은 화이트 리스트 방식(허용 목록을 제외한 모든 접근을 차단)을 적용하고 있어 해당 국가에 대한 허용 정책을 추가

Add Rule

Permission: ☒ Allow ☐ Deny

Interface: All

Source:

- ☐ Any
- ☐ IP: Select an IP category ☐ Use IPv6 address
- ☐ Domain
- ☒ Region: South Korea (1 regions selected)

Protocol: ☒ Any ☐ TCP ☐ UDP ☐ ICMP

Apply Cancel

※ 방화벽 규칙(정책)은 NAS 장치를 운영하는 목적에 따라 알맞게 설정하여야 하며 각 응용 프로그램 서비스, 접속 IP에 따라 규칙을 생성하여 외부 접근을 통제할 수 있다. NAS 장치를 국내에서만 사용하는 경우 해외IP 차단 규칙을 통해 불필요한 해외에서의 접근을 차단하는 것을 권장

6.5 로그 및 백업 관리

QNAP-18 로그 관리

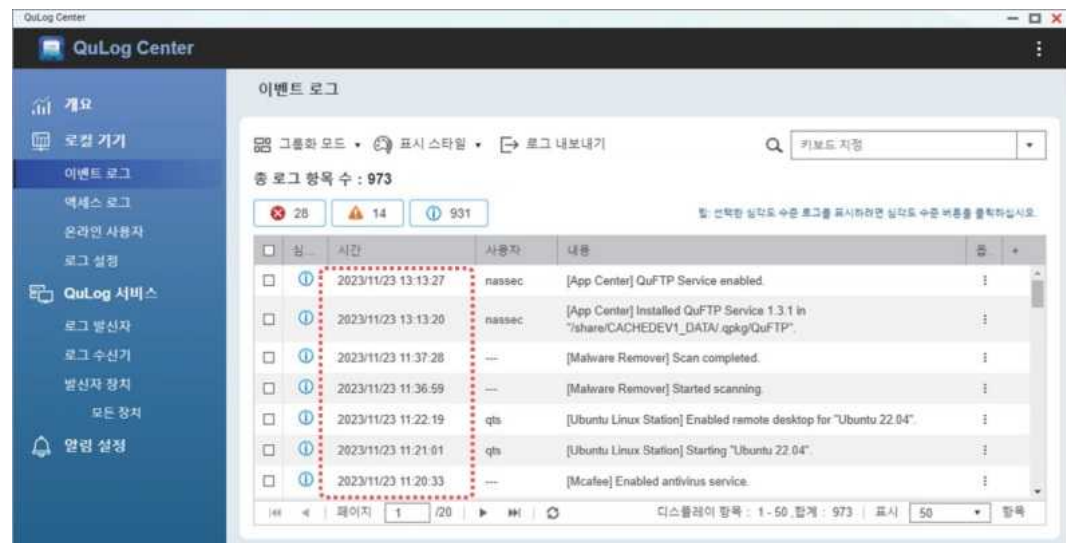
❏ 취약점 개요

점검 내용	• 내부 정책에 따른 적절한 시스템 로그 관리 여부 점검				
점검 목적	• 보안사고 발생 시 가시성 및 책임추적성을 확보하여 원인을 파악하기 위함				
보안 위협	• 로그 관리를 하지 않을 경우, 장애 및 침해사고 발생으로 피해 발생 시 원인 규명, 사후 추적 등 분석의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>주요 서비스 로그 활성화가 되어있는 경우</td></tr> <tr> <td>취약</td><td>주요 서비스 로그 활성화가 되어있지 않은 경우</td></tr> </table>	양호	주요 서비스 로그 활성화가 되어있는 경우	취약	주요 서비스 로그 활성화가 되어있지 않은 경우
양호	주요 서비스 로그 활성화가 되어있는 경우				
취약	주요 서비스 로그 활성화가 되어있지 않은 경우				
참고	※ 감사 로그 설정이 너무 높으면 불필요 로그가 기록되어 중요한 로그 기록과 혼동 및 시스템 성능 저하와 같은 영향을 받을 수 있으므로 법적 요구 사항과 조직의 정책·지침에 따라 원인 규명, 책임 추적을 위한 로그만 설정할 것을 권고함 ※ 책임추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				

❏ 점검 및 조치방법

○ 정상적으로 로그가 기록되고 있는지 점검

- ▶ [QuLog Center] 앱 > [로컬 기기] > [이벤트 로그], [액세스 로그] 탭에서 최근 시간까지 정상적으로 로그가 기록되고 있는지 확인



- ※ 이벤트 로그 : 시스템 또는 응용 프로그램에서 발생하는 이벤트에 대한 기록(시스템의 시작 또는 종료, 오류 메시지, 보안 이벤트 등)을 담고 있는 로그 파일
- ※ 액세스 로그 : 시스템이나 서비스에 접근한 사용자 또는 장치에 대한 정보(사용자 계정, IP 주소, 접근 시간, 접근한 파일 또는 리소스, 접근 유형 등)를 기록한 로그 파일

○ 액세스 로그 대상 서비스 설정

- ▶ [QuLog Center] 앱 > [로컬 기기] > [로그 설정] 탭의 ‘**액세스 로그 설정**’ 메뉴에서 액세스 로그를 기록할 서비스 설정

연결 유형

로그할 연결을 선택합니다.

☒ HTTP/HTTPS	☒ SSH/SFTP	☐ iSCSI
☒ FTP	☐ AFP (Mac)	☐ RADIUS
☒ Telnet	☐ SMB	☐ WebDAV
☐ NFS ⓘ		

○ 로그 아카이브 설정

- ▶ 시스템에 저장된 로그 데이터의 무분별한 증가로 인한 저장공간 부족 현상을 해소하기 위해, 로그 아카이브 설정을 통해 특정 조건에 따른 로그 데이터 보관 규칙 설정
- ▶ [QuLog Center] 앱 > [로컬 기기] > [로그 설정] 탭의 ‘**이벤트 로그 설정**’, ‘**액세스 로그 설정**’ 메뉴에서 로그 보존 설정
- ※ NAS 장치의 저장공간을 고려하여 충분한 크기로 설정하는 것을 권장

QuLog Center

로그 설정

이벤트 로그 설정 액세스 로그 설정 이벤트 표시등

여기에서는 데이터베이스 크기, 로그 언어를 설정하고 이벤트 로그에서 모든 데이터를 삭제할 수 있습니다.

일반 설정

로그 보존 설정을 구성합니다. 로그 항목 수가 지정된 임계값에 도달하면 QuLog Center에서 가장 오래된 항목을 자동으로 삭제하여 새 항목을 위한 공간을 마련합니다.

대상: DataVault

최대 항목 수: 5백만

로그 보존 시간: 최근 180 일

☒ 데이터베이스 한계에 도달한 후에는 로그 항목을 지정된 위치에 보관하고 이동하십시오.

대상 폴더: /Container/container-status 찾기

- ※ 로그 데이터 저장소를 별도로 지정하지 않으면 정의된 기준(항목 수, 보존 기간)에 도달하게 되었을 때 이전 로그 기록을 삭제하면서 새로운 로그가 기록된다.

QNAP-19 백업 관리

취약점 개요

점검 내용	NAS 장치에 저장된 데이터 백업 여부 점검						
점검 목적	장애 및 보안사고 발생 시 피해로부터 신속한 복구를 하기 위해 중요자료에 대한 2차 백업 (클라우드, 외부 저장매체, 스냅샷 등)을 설정하고 있는지 점검하여 자료 손실에 대비한 대응체계 점검						
보안 위협	NAS 장치에 저장된 데이터를 노리는 랜섬웨어 및 해킹 공격으로 인한 데이터 변조, 유출, 암호화의 위험이 존재함						
점검 기준	<table border="1"> <tr> <td>양호</td><td>주기적인 백업 관리를 이행하고 있는 경우</td></tr> <tr> <td>취약</td><td>주기적인 백업 관리를 이행하지 않는 경우</td></tr> </table>	양호	주기적인 백업 관리를 이행하고 있는 경우	취약	주기적인 백업 관리를 이행하지 않는 경우		
양호	주기적인 백업 관리를 이행하고 있는 경우						
취약	주기적인 백업 관리를 이행하지 않는 경우						
참고	※ NAS 장치에서 데이터 백업 종류 <table border="1"> <tr> <td>외부 저장매체 활용</td><td>네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식</td></tr> <tr> <td>외부 저장소 동기화</td><td>클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음</td></tr> <tr> <td>스냅샷(Snapshot) 기능 활용</td><td>제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함</td></tr> </table> ※ 백업 방식별 장·단점을 고려하여 데이터 백업을 진행하고, 중요한 데이터일수록 다중 백업을 적용하여 복구 신뢰성을 확보하여야 함	외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식	외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음	스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함
외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식						
외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음						
스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함						

🔒 점검 및 조치방법

- QNAP NAS 장치에서는 HBS3(Hybrid Backup Sync) 앱을 통해 다양한 데이터 백업 방식을 지원하고 있으며 사용자 환경에 맞는 백업 방식 및 매체를 선정하여 백업을 진행하여야 함

지원앱	백업 방식	설명
 HBS3 (Hybrid Backup Sync)	RTRR (Real-Time Remote Replication)	• RTRR 방식은 실시간 원격 복제 방식으로 NAS에서 다른 NAS로 데이터를 백업할 수 있음 • 또한 실시간으로 변경 사항을 원격 NAS에 복제
	Rsync 백업	• Rsync는 원격 서버와의 데이터 동기화를 지원하는 프로토콜로, 다른 Rsync 호환 서버와 동기화를 통해 데이터를 백업 할 수 있음
	클라우드 백업	• Amazon S3, Google Drive, Dropbox 등 다양한 클라우드 서비스와 통합하여 클라우드 저장소에 데이터를 백업할 수 있음
	USB 백업 및 외부 디스크 복제	• 외부 USB 디바이스를 NAS에 연결하거나 외부 디스크에 데이터를 복제하여 물리적인 저장 매체에 안전하게 데이터를 백업 할 수 있음
 스토리지 및 스냅샷	Snapshot 기능 활용	• 스냅샷 기능을 이용하여 특정 시점의 데이터를 보호할 수 있음. 데이터가 삭제되거나 수정된 경우 되돌리기 기능을 이용하여 신속하게 데이터를 복원할 수 있음

QNAP-20 NTP 서버 연동

❗ 취약점 개요

점검 내용	• NTP 서버 연동 설정 적용 여부 점검
점검 목적	• 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과 관계 파악에 도움을 주고 로그 자체의 신뢰성을 확보하기 위함
보안 위협	• 시스템 간 시간 동기화 미흡으로 보안사고 및 장애 발생 시 로그에 대한 신뢰도 확보 미흡
점검 기준	양호 취약 NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우 NTP 서버와 연동되어 있지 않은 경우
참고	※ NTP(Network Time Protocol) : 네트워크를 통해 컴퓨터 시스템 간의 시간을 정확하게 유지 시켜주기 위한 네트워크 프로토콜. ※ Public NTP 서버 : 글로벌 IT 기업(Google, Microsoft), 비영리 단체(ntppool.org) 등에서 제공하고 있는 공개된 NTP 서버로 국내에서는 주요 통신사(LG유플러스, KT 등)에서 제공하고 있음

❗ 점검 및 조치방법

○ NTP 서버 연동 여부 점검

▶ [제어판] > [시스템] > [일반 설정] > [시간] 탭에서 '시간 서버와 자동으로 동기화' 설정 및 연결 테스트 진행



▶ NAS 장치가 내부망 환경에서 운영되는 경우 별도 NTP 서버를 구축하여 내부 시스템 간 시간 동기화를 권장하며, [시스템] > [애플리케이션] > [NTP 서버] 탭에서 NAS 장치를 NTP 서버로 구성하여 운영할 수 있음

6.6 서비스 관리

QNAP-21 불필요한 서비스 사용 금지

🔒 취약점 개요

점검 내용	• 사용하지 않는 서비스 활성화 여부 점검				
점검 목적	• 불필요한 서비스 활성화로 인한 시스템 성능 저하 및 잠재적인 보안 취약점 노출 위험을 예방하기 위해 불필요한 서비스 활성화 여부 점검				
보안 위험	• NAS 장치에서 제공되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침입의 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 서비스 사용이 비활성화된 경우</td></tr> <tr> <td>취약</td><td>불필요한 서비스 사용이 활성화된 경우</td></tr> </table>	양호	불필요한 서비스 사용이 비활성화된 경우	취약	불필요한 서비스 사용이 활성화된 경우
양호	불필요한 서비스 사용이 비활성화된 경우				
취약	불필요한 서비스 사용이 활성화된 경우				
참고	※ 서비스 사용이 필요한 경우에도 서비스 오남용 방지를 위해 계정(또는 그룹)별 사용 권한을 부여하여 필수 계정만 사용할 수 있도록 통제하는 것을 권장				

🔒 점검 및 조치방법

○ 불필요한 서비스 활성화 여부 확인

▶ QNAP에서 제공하는 각 서비스에 대한 활성화 여부 확인

서비스명	점검 방법
웹 서버	[제어판] > [애플리케이션] > [웹 서버] 탭
가상호스트	[제어판] > [애플리케이션] > [웹 서버] 탭
LDAP	[제어판] > [애플리케이션] > [LDAP 서버] 탭
syslog	[제어판] > [애플리케이션] > [Syslog 서버] 탭
RADIUS	[제어판] > [애플리케이션] > [RADIUS 서버] 탭
TFTP	[제어판] > [애플리케이션] > [TFTP 서버] 탭
NTP 서버	[제어판] > [애플리케이션] > [NTP 서버] 탭
파일 서비스(SMB, AFP, NFS, WebDAV)	[제어판] > [네트워크 및 파일 서비스] > [Win/Mac/NFS/WebDAV] 탭
터미널 서비스(Telnet, SSH)	[제어판] > [네트워크 및 파일 서비스] > [Telnet/SSH] 탭
SNMP	[제어판] > [네트워크 및 파일 서비스] > [SNMP] 탭
UPnP	[제어판] > [네트워크 및 파일 서비스] > [서비스 발견] 탭
Bonjour	[제어판] > [네트워크 및 파일 서비스] > [서비스 발견] 탭

- ▶ 위 서비스 목록 중 사용하지 않는 서비스가 활성화된 경우 각 서비스 탭에서 비활성화 조치

웹 서버

가상 호스트

웹 서버

이 기능을 활성화하면 웹페이지 파일을 Web 공유 네트워크에 올려 웹사이트에 게시할 수 있습니다.

☐ 웹 서버 활성화

포트 번호:

80

QNAP-22 안전한 SNMP 서비스 사용

취약점 개요

점검 내용	안전한 SNMP 서비스 사용을 위한 보안 설정 점검								
점검 목적	- SNMP 서비스 사용 시 안전한 버전(V3) 사용을 권장 - V3 미만 버전의 SNMP 서비스를 사용하려면 유추하기 어려운 Community String을 설정하여 네트워크상에서 비인가자에게 시스템 정보가 노출되지 않도록 하여 함								
보안 위협	SNMPv1, SNMPv2 버전을 사용할 때 Public, Private와 같은 디폴트 Community String이 변경되지 않고 그대로 사용될 경우, 이 String을 악용하여 환경설정 파일 열람 및 수정을 통한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 Dos공격까지 다양한 형태의 공격이 가능								
점검 기준	<table> <tr> <td>양호</td><td>SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우</td></tr> <tr> <td>취약</td><td>유추하기 쉬운 Community String이 설정된 경우</td></tr> </table>	양호	SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우	취약	유추하기 쉬운 Community String이 설정된 경우				
양호	SNMPv3를 사용하거나 유추하기 어려운 Community String이 설정된 경우								
취약	유추하기 쉬운 Community String이 설정된 경우								
참고	※ SNMP(Simple Network Management Protocol) 프로토콜 : 네트워크 상태 및 성능을 모니터링하고 관리하기 위한 표준 프로토콜로 네트워크 장비, 서버, 프린터 등과 같은 장치의 구성 정보 수집 및 원격 모니터링을 제공 ※ SNMP 프로토콜 버전 <table> <tr> <th>버 전</th><th>설 명</th></tr> <tr> <td>SNMPv1</td><td>SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약</td></tr> <tr> <td>SNMPv2c (SNMPv2)</td><td>일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시</td></tr> <tr> <td>SNMPv3</td><td>사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음</td></tr> </table>	버 전	설 명	SNMPv1	SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약	SNMPv2c (SNMPv2)	일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시	SNMPv3	사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음
버 전	설 명								
SNMPv1	SNMP의 최초 버전으로 Community String라는 간단한 패스워드를 통해 데이터를 전송하며, Community String값이 평문으로 전송되기 때문에 보안에 취약								
SNMPv2c (SNMPv2)	일부 기능 추가 및 Community String을 암호화하여 전달하는 방식으로 개선하여 SNMPv2가 출시되었지만, 사용하는 방식이 복잡하다는 문제점으로 인해 다시 평문으로 전달하는 방식으로 회귀되어 SNMPv2c으로 재출시								
SNMPv3	사용자 인증 및 데이터 암호화를 지원하는 가장 안전한 버전으로 널리 권장되고 있으나, v3 버전을 지원하지 않은 솔루션들이 일부 있음								

점검 및 조치방법

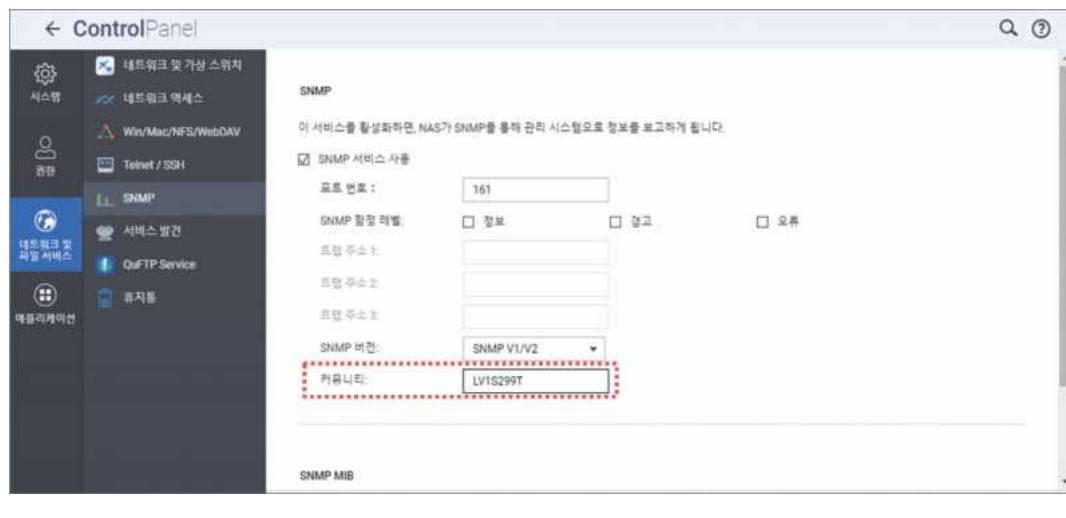
SNMP(Simple Network Management Protocol) 서비스 버전 확인

① SNMPv3 사용 시

- ▶ NMS(Network Management) 솔루션에서 지원하는 SNMP 서비스 버전을 확인하여 SNMPv3를 지원하는 경우 해당 버전을 사용할 것을 권장

② SNMPv1, SNMPv2c 사용 시

- ▶ SNMPv3를 지원하지 않아 SNMPv1, SNMPv2c 버전을 사용해야 하는 경우 public, private 같은 디폴트 값을 사용하지 않고, 유추하기 어려운 Community String값을 설정하여 이용하여야 함
- ▶ [제어판] > [네트워크 및 파일 서비스] > [SNMP] 탭에서 안전한 커뮤니티 값 설정



QNAP-23 안전한 FTP 서비스 사용

취약점 개요

점검 내용	FTP 서비스 이용 시 안전한 설정을 유지하고 있는지 점검										
점검 목적	보안에 취약한 FTP 서비스 사용은 지양하고, FTP 서비스 사용이 필요한 경우 암호화된 파일 전송 프로토콜(FTPS, SFTP)을 사용하여 안전한 데이터 전송을 하기 위함										
보안 위협	FTP는 파일을 전송하기 위한 프로토콜로 계정과 패스워드를 암호화하지 않고 평문 전송하여 네트워크 스니핑 등의 위협으로부터 계정 정보 및 모든 전송 데이터에 대한 침해사고 가능성이 존재함										
점검 기준	<table border="1"> <tr> <td>양호</td><td>FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우</td></tr> <tr> <td>취약</td><td>FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우</td></tr> </table>	양호	FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우	취약	FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우						
양호	FTP 서버 서비스를 사용하지 않거나, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하고 있는 경우										
취약	FTP 서버 서비스를 사용하고 있고, 암호화된 전송 프로토콜(FTPS, SFTP)을 사용하지 않는 경우										
참고	※ 파일 전송 프로토콜(FTP) 버전 <table border="1"> <thead> <tr> <th>버전</th><th>설명</th></tr> </thead> <tbody> <tr> <td>FTP (File Transfer Protocol)</td><td>기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)</td></tr> <tr> <td>SFTP (SSH File Transfer Protocol)</td><td>SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)</td></tr> <tr> <td>FTPS (FTP Secure)</td><td>FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)</td></tr> <tr> <td>FTPES (FTP over Explicit TLS/SSL)</td><td>FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)</td></tr> </tbody> </table> * SSL(Secure Sockets Layer) : 웹에서 데이터를 안전하게 전송하기 위해 사용되는 프로토콜 * TLS(Transport Layer Security) : SSL의 후속 프로토콜로, SSL 3.0의 보안 취약성을 보완하고 개선된 버전	버전	설명	FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)	SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)	FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)	FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)
버전	설명										
FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)										
SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)										
FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)										
FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)										

🔍 점검 및 조치방법

○ FTP 서비스 설정 확인

- ▶ [QuFTP Service] 앱 실행 > [FTP 서버] > [시스템] 탭에서 FTP 서비스 실행 여부, 기본 포트 변경 여부, 안전한 FTPES(또는 SFTP) 서비스 사용 여부 등을 확인



○ 안전한 FTP 서비스 사용 설정

- ▶ FTP 서비스를 사용하지 않는 경우 서비스 사용 중단('FTP 서버 활성화' 체크 해제)
- ▶ FTP 서비스 사용이 필요한 경우 데이터 암호화를 제공하는 FTPES, SFTP 프로토콜을 사용하고, 기본 포트는 알려지지 않은 포트로 변경하여 사용할 것을 권장

※ 기본 포트 : FTPES(21), SFTP(22)



- ▶ SFTP 서비스 사용은 [제어판] > [네트워크 및 파일 서비스] > [Telnet/SSH] 탭에서 설정할 수 있음



※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

- ▶ 하단 추가기능 메뉴에서 '익명 액세스 사용'이 설정되어있는 경우 해제하여 익명 사용자의 접속을 차단하여야 함

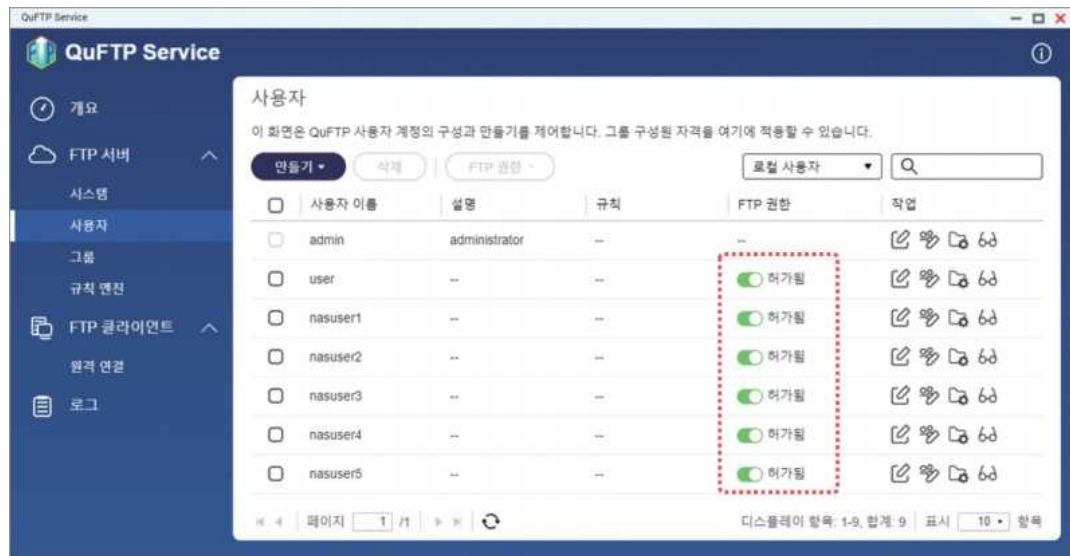


※ Anonymous FTP(익명 FTP)를 사용 시 anonymous 계정으로 로그인 후 디렉터리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 함

※ Anonymous FTP(익명 FTP) : 파일 전송을 위해서는 원칙적으로 상대방 컴퓨터를 사용할 수 있는 계정이 필요하나 누구든지 계정 없이도 anonymous 또는 ftp라는 로그인 명과 임의의 비밀번호를 사용하여 FTP를 실행할 수 있음

○ FTP 서비스 사용자 권한 부여

- ▶ [QuFTP Service] 앱 실행 > [FTP 서버] > [사용자] 탭에서 FTP 서비스 사용이 필요한 사용자에게만 권한을 부여하여 불필요한 사용자 권한 회수



ipTIME NAS 보안가이드

7.1 진단 항목	130
7.2 계정 관리	132
7.3 접근 관리	138
7.4 패치 및 보안 관리	143
7.5 로그 및 백업 관리	148
7.6 서비스 관리	154

07

07

ipTIME NAS
보안 가이드

7.1 진단 항목

항목 분류	항목 코드	항목명
계정 관리	iptime-01	기본 관리자 계정(default) 사용금지
	iptime-02	계정별 권한 관리
	iptime-03	공용계정 및 휴면계정 관리
	iptime-04	로그인 실패 횟수 제한
접근 관리	iptime-05	암호화 통신 및 기본포트 변경
	iptime-06	Session Timeout 설정
	iptime-07	불필요한 공유폴더 비활성화
패치 및 보안관리	iptime-08	제조사에서 제공하는 최신 업데이트 적용
	iptime-09	악성 스크립트 접근 방지(CSRF) 적용
	iptime-10	방화벽 기능 활성화
로그 및 백업 관리	iptime-11	로그 관리
	iptime-12	백업 관리
	iptime-13	NTP 서버 연동
서비스 관리	iptime-14	불필요한 서비스 사용 금지
	iptime-15	안전한 FTP 서비스 사용
15개 항목		



유의사항

본 가이드는 NAS 취약점 평가항목에 대한 이해를 돕기 위해 항목설명, 점검기준, 점검방법, 대응방안을 제시하며 취약점 조치에 활용할 수 있습니다. 다만 일반적인 권고사항이므로 운영환경과 시스템에 미치는 영향을 검토하여 적용하여야 합니다.

※ 본 가이드 작성 기준은 **ipTIME NAS 장비의 GUI 기반으로 작성되었으며, 타제품 사용 시 각 항목에 해당하는 설정 탭의 모양, 설명, 현황 등이 제품에 따라 상이할 수 있으므로 각 제조사의 사용자 매뉴얼을 참고하여 본 가이드 안내에 따라 보안 설정할 것을 권고 드립니다.**

7.2 계정 관리

iptime-01 기본 관리자계정(default) 사용금지

취약점 개요

점검 내용	제조사가 생성한 기본 관리자계정(default) 사용 여부 점검										
점검 목적	이미 알려진 default 계정을 이용한 계정 접속 시도 및 탈취를 예방하기 위해 기본 관리자 계정의 비활성화 여부 점검										
보안 위협	공격자가 알려진 Default 계정 정보를 이용하여 무차별 대입 공격(Brute Force Attack), 사전 공격(Dictionary attack), 혼합 공격(Hybrid Attack), 레인보우 테이블 공격(Rainbow Table Attack) 등 패스워드 크래킹 공격을 통해 계정이 도용될 수 있으며, 이를 통해 시스템 가용성 훼손, 자료 유출 등의 위험이 존재함										
점검 기준	<table border="1"> <tr> <td>양호</td><td>기본 관리자계정(admin)를 사용하지 않는 경우</td></tr> <tr> <td>취약</td><td>기본 관리자계정(admin)를 사용하는 경우</td></tr> </table>	양호	기본 관리자계정(admin)를 사용하지 않는 경우	취약	기본 관리자계정(admin)를 사용하는 경우						
양호	기본 관리자계정(admin)를 사용하지 않는 경우										
취약	기본 관리자계정(admin)를 사용하는 경우										
참고	※ ipTIME NAS의 기본계정(default) : admin ※ 대표적인 패스워드 크래킹 공격 <table border="1"> <thead> <tr> <th>서비스명</th><th>점검 방법</th></tr> </thead> <tbody> <tr> <td>무차별 대입 공격 (Brute Force Attack)</td><td>모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격</td></tr> <tr> <td>사전 공격 (Dictionary attack)</td><td>자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격</td></tr> <tr> <td>혼합 공격 (Hybrid Attack)</td><td>사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격</td></tr> <tr> <td>레인보우 테이블 공격 (Rainbow Table Attack)</td><td>해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격</td></tr> </tbody> </table>	서비스명	점검 방법	무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격	사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격	혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격	레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격
서비스명	점검 방법										
무차별 대입 공격 (Brute Force Attack)	모든 가능한 패스워드 조합을 시도하여 암호를 찾는 공격										
사전 공격 (Dictionary attack)	자주 사용하는 단어나 문장, 생일 등을 사전(Dictionary)으로 미리 만들어 놓고 이를 대입해 패스워드를 알아내는 공격										
혼합 공격 (Hybrid Attack)	사전 공격과 무차별 대입 공격의 특징을 혼합하여 사용하는 공격										
레인보우 테이블 공격 (Rainbow Table Attack)	해시 함수를 사용하여 암호를 저장하는 시스템에서 미리 계산된 해시값과 관련된 암호를 검색하는 공격										

점검 및 조치방법

○ 제조사에서 제공된 기본 관리자계정(admin) 활성화 여부 확인

▶ [폴더/사용자 관리] > [사용자 관리] 탭에서 admin 계정 상태 확인

The screenshot shows the '사용자 관리' (User Management) tab. On the left, a sidebar lists various system settings. The main area displays a table of users: admin, user01, user02, user03, user04, and user05. Below the table, the 'admin' user's details are shown. The '계정 사용' (Account Status) section has two radio buttons: '사용' (selected) and '사용안함' (disabled). A red dashed box highlights these buttons, and a red arrow points to the '사용' button. Other fields include '사용자 ID' (admin), '암호' (password), '암호 재입력' (confirm password), '용량제한 대상그룹' (usage limit target group), '폴더' (folder), '이름' (name), '이메일 주소' (email address), and '설명' (description).

○ 새 관리자 계정 생성

▶ admin 계정이 사용 중인 경우 비활성화를 위해 관리자 계정으로 사용할 신규 관리자 생성

▶ [폴더/사용자 관리] > [사용자 관리] 탭에서 '새 사용자' 클릭 후 신규 관리자계정 생성

The screenshot shows the '사용자 관리' (User Management) tab with the '새 사용자' (New User) button highlighted in the top right corner by a red arrow. Below the user list, the '새 사용자' form is displayed. The '계정 사용' (Account Status) section has two radio buttons: '사용' (selected) and '사용안함' (disabled). A red dashed box highlights this section. Other fields include '사용자 ID' (nasec), '암호' (password), '암호 재입력' (confirm password), '용량제한 대상그룹' (usage limit target group), '폴더' (folder), '이름' (name), '이메일 주소' (email address), and '설명' (description). The '관리자 권한' (Administrator Privileges) checkbox is checked.

○ 기본 관리자 계정 비활성화

- ▶ ②항에서 신규 생성한 관리자 계정으로 로그인 후 기본 관리자계정(admin) 비활성화 진행
- ▶ [폴더/사용자 관리] > [사용자 관리] 탭에서 'admin' 계정 선택 후 '사용안함' 선택

The screenshot shows a user management form with the following fields and values:

Field	Value
계정 사용 *	☐ 사용 ☒ 사용안함
사용자 ID *	admin
암호 *	*****
암호 재입력 *	*****
용량제한 대상그룹	사용안함
홈 폴더	사용안함
이름	admin
이메일 주소	admin123456789@gmail.com
설명	admin

Additional options on the right:

- ☒ 관리자 권한
- ☐ 암호 재설정

iptime-02 계정별 권한 관리

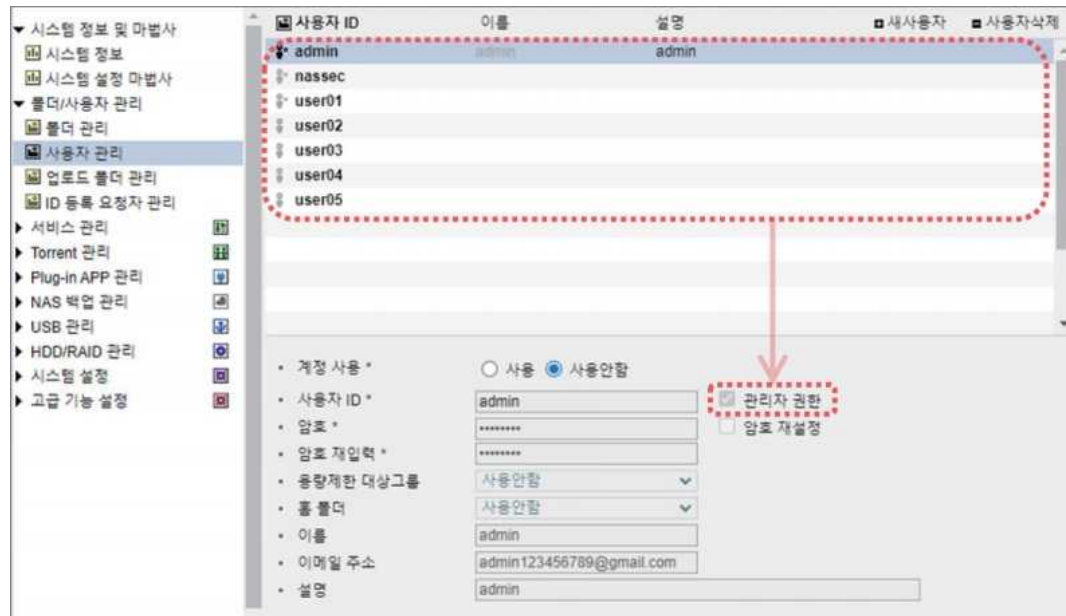
❖ 취약점 개요

점검 내용	• 사용자(계정)별 불필요한 권한 부여 여부 점검				
점검 목적	• 불필요하게 과도한 권한을 부여받은 사용자 계정을 통해 주요 설정 변경, 자료 유출 등을 방지하기 위함				
보안 위협	• 의도하지 않게 인가된 관리자 권한을 이용하여 NAS 장치의 주요 설정 변경, 시스템 침입 경로 노출, 자료 유출 등의 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우</td></tr> <tr> <td>취약</td><td>과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우</td></tr> </table>	양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우	취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우
양호	업무를 고려하여 적절한 권한을 부여하고, 불필요한 관리자 권한의 계정이 없는 경우				
취약	과도한 권한을 부여하거나, 불필요한 관리자 권한의 계정이 있을 경우				
참고	※ 관리자 권한은 최소한의 사용자(계정)에만 부여 ※ 업무별 목적에 맞게 적절한 권한으로 계정 부여				

❖ 점검 및 조치방법

○ 사용자 계정별 관리자 권한 부여 여부 점검

- ▶ [폴더/사용자 관리] > [사용자 관리] 탭의 사용자 계정 목록에서 불필요한 관리자 권한이 부여되었는지 확인하여 '관리자 권한' 체크박스 해제



iptime-03 불필요한 공용계정 및 휴면계정 관리

❖ 취약점 개요

점검 내용	• 불필요한 공용계정 및 미사용 휴면계정 존재 여부 점검				
점검 목적	• 불필요한 공용계정 및 미사용 휴면계정을 관리하여 비인가자의 접근 시도를 차단하고, 사용자별 개별 계정 부여를 통해 파일 변조, 정보 유출 등 사고 및 장애 발생에 대한 책임 추적성을 강화하기 위함 ※ 책임 추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				
보안 위협	• 관리되지 않는 휴면계정을 통한 비인가 접근의 위험이 존재하며, 공용계정 사용으로 인한 침해사고와 서비스 장애 발생 시 추적의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>공용계정 및 휴면계정을 관리하고 있는 경우</td></tr> <tr> <td>취약</td><td>공용계정 및 휴면계정이 관리되지 않는 경우</td></tr> </table>	양호	공용계정 및 휴면계정을 관리하고 있는 경우	취약	공용계정 및 휴면계정이 관리되지 않는 경우
양호	공용계정 및 휴면계정을 관리하고 있는 경우				
취약	공용계정 및 휴면계정이 관리되지 않는 경우				
참고	※ 계정의 공유를 금지하여야 하며, 1인 1계정 사용을 원칙으로함				

❖ 점검 및 조치방법

○ 사용자 계정 목록 확인

- ▶ [폴더/사용자 관리] > [사용자 관리] 탭의 사용자 계정 목록을 검토하여 ‘불필요한 공용계정’ 및 ‘미사용 휴면계정’ 존재 여부 확인
- ▶ 사용자 확인(인터뷰), 계정 관리대장 검토 등을 통해 공용계정 및 미사용된 장기 휴면계정 여부를 확인하여 불필요한 계정 삭제(또는 ‘사용안함’) 조치

iptime-04 로그인 실패 횟수 제한

취약점 개요

점검 내용	로그인 실패 허용 임계값 설정 여부 점검				
점검 목적	로그인 실패 임계값이 설정되어 있는지 점검하여 비인가자의 지속적인 로그인 시도를 차단하기 위함				
보안 위협	반복되는 로그인 실패에 대한 차단이 이루어지지 않으면 자동화된 패스워드 크래킹 도구를 통한 패스워드 공격(무작위 대입, 사전 대입, 추측 공격 등)에 취약하여 사용자 패스워드가 탈취될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장</td></tr> <tr> <td>취약</td><td>로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우</td></tr> </table>	양호	로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장	취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우
양호	로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장				
취약	로그인 실패 횟수 제한 설정이 없거나 적절하게 설정되지 않은 경우				
참고	※ 계정 잠금 시간 : 로그인 실패로 계정이 잠기는 시간으로 관리자가 잠금 해제를 하거나 잠금 유지 시간이 경과되어야 재시도할 수 있음 ※ 로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장				

점검 및 조치방법

로그인 제한 설정 여부 점검

- ▶ [시스템 설정] > [관리 페이지 설정] 탭의 관리 페이지 고급 설정 메뉴에서 '로그인 제한' 활성화 및 임계값 설정
- ※ 로그인 실패 횟수는 5회이하, 계정 잠금 시간은 사용자 필요에 따라 조정 권장
- ※ 자동매크로 방지를 위한 'CAPTCHA' 설정 권장

The screenshot shows the '관리 페이지 설정' (Management Page Settings) window. Under the '관리 페이지 고급 설정' (Management Page Advanced Settings) tab, the '로그인 제한' (Login Limit) section is highlighted with a red dashed box. It includes a checkbox for '로그인 제한' which is checked, and a dropdown for '로그인 실패 횟수' (Login Failure Count) set to 5. Below it, the 'CAPTCHA' section is also highlighted, with a checkbox for 'CAPTCHA' checked and a dropdown for 'CAPTCHA 표시' (CAPTCHA Display) set to '수동 입력' (Manual Input). The 'ID 등록 요청 설정' (ID Registration Request Settings) section shows a radio button for '중단' (Stop) selected, and a dropdown for '최대 등록 요청 갯수' (Maximum Number of Registration Requests) set to 50.

※ CAPTCHA : 자동 매크로를 방지하기 위해 만들어진 인증방식으로 사람은 쉽게 인식할 수 있는 텍스트, 이미지를 통해 사람과 기계를 구별하는 프로그램

7.3 접근 관리

iptime-05 암호화 통신 및 기본 포트 변경

🔒 취약점 개요

점검 내용	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜 사용 및 기본 포트를 변경하고 접근하고 있는지 점검				
점검 목적	웹 또는 터미널 접근 시 데이터를 암호화하여 전송하는 HTTPS와 SSH를 사용하여 비인가자의 데이터 스니핑에 대비하고, HTTPS와 SSH의 알려진 기본 포트를 변경하여 공격자의 접근을 어렵게 하기 위함				
보안 위협	공격자가 스니핑(Sniffing)을 시도하면 계정의 ID와 패스워드가 평문으로 노출되어 계정이 탈취될 위험이 존재하며, 잘 알려진 기본 포트를 사용하는 경우, 지속적인 패스워드 크래킹 또는 해킹 공격의 대상이 될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우</td></tr> <tr> <td>취약</td><td>NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우</td></tr> </table>	양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우	취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우
양호	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하고 기본 포트를 변경하여 사용하는 경우				
취약	NAS 장치에 접근(웹, 터미널) 시 암호화 프로토콜을 사용하지 않거나 기본 포트 그대로 사용하는 경우				
참고	※ 스니핑(Sniffing) : 스니퍼(Sniffer)는 "컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청 장치"라고 말할 수 있으며 "스니핑"이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말함				

🔒 점검 및 조치방법

○ NAS 웹 페이지 접근 시 보안 접속(HTTPS) 사용 여부 점검 ①

- ▶ [시스템 설정] > [관리자 페이지 설정] 탭에서 관리자 페이지 접속 설정 메뉴에서 'HTTP+HTTPS(일반접속+보안접속)' 체크박스 활성화 및 기본 포트(HTTP/80, HTTPS/443) 변경 여부 확인

- ▶ ‘HTTP+HTTPS(일반접속+보안접속)’ 체크박스를 활성화하여 보안 접속(HTTPS)을 사용하고, ‘기본 포트 사용’ 체크박스 해제 후 알려지지 않은 포트로 변경

※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 ‘포트 포워딩’ 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

○ 터미널을 통한 원격접근 시 보안 접속(SSH) 사용 여부 확인 ②

- ▶ [시스템 설정] > [기타 설정] > [SSH 서버] 탭에서 **SSH 서버 사용여부, 접속계정 설정여부, 기본 포트 번호 변경여부** 등을 확인

- ▶ SSH 서버를 사용하지 않는 경우 서비스를 중단
▶ SSH 서버 사용이 필요한 경우 사용이 필요한 ‘접속계정’을 설정하고 ‘**포트 번호**’를 알려지지 않은 포트로 변경하여 사용하여야 함(기본 포트 22)

※ ipTIME NAS에서는 데이터를 평문으로 전송하는 터미널 서비스인 Telnet 서비스는 제공하지 않음
※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 ‘포트 포워딩’ 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함

iptime-06 Session timeout 설정

📌 취약점 개요

점검 내용	• Session timeout(자동 로그아웃) 설정 적용 여부 점검				
점검 목적	• 사용자의 부주의로 계정이 로그인된 상태로 방치되는 상황을 방지하고, 사용하지 않는 세션을 종료하여 보안성과 가용성을 높이기 위함				
보안 위험	• 사용자가 작업 중 이석하거나 불안정한 세션 종료를 했을 경우, 권한 없는 사용자가 이석한 자리에서 정책 삭제나 변경 등 악의적인 행위를 하거나 불안정한 세션 종료를 한 세션 정보를 재사용하여 인증 없이 NAS 장치에 접근할 위험이 있음				
점검 기준	<table border="1"> <tr> <td>양호</td><td>Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)</td></tr> <tr> <td>취약</td><td>Session timeout(자동 로그아웃)이 설정되지 않은 경우</td></tr> </table>	양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)	취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우
양호	Session timeout(자동 로그아웃)이 적절하게 설정된 경우 (15분 이내로 설정할 것을 권장)				
취약	Session timeout(자동 로그아웃)이 설정되지 않은 경우				
참고	※ Session timeout : 로컬 또는 원격에서 장비에 접속한 사용자가 일정 시간 동안 통신이 없을 시 해당 세션을 종료시키는 설정 ※ 장비에 접속하여 이행하는 업무 특성을 고려하여 최소 시간 설정				

📌 점검 및 조치방법

○ Session Timeout(자동 로그아웃) 설정 확인

- ▶ [시스템 설정] > [기타 설정] > [자동 로그아웃 시간 설정] 탭에서 '자동 로그아웃' 시간이 적절하게 설정되어 있는지 확인(15분 이내로 설정하는 것을 권장)



iptime-07 불필요한 공유폴더 미사용

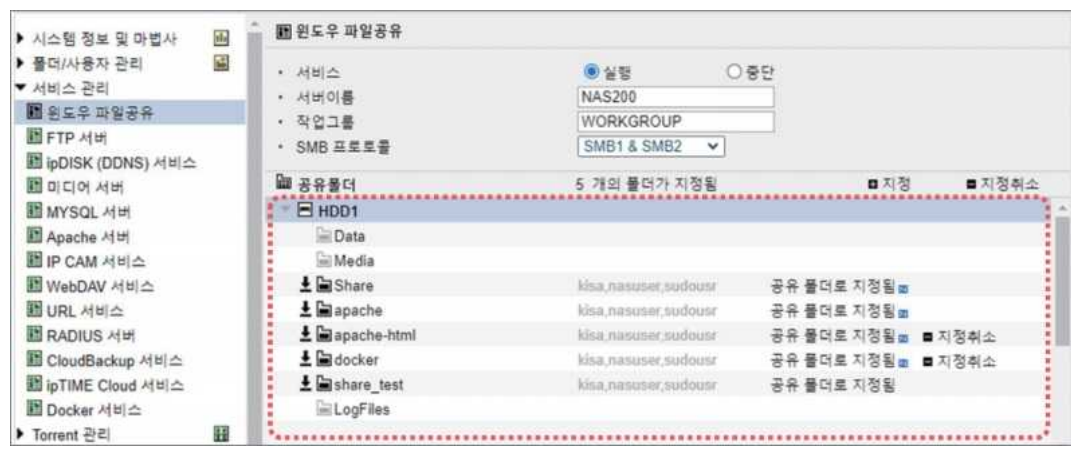
❖ 취약점 개요

점검 내용	불필요한 윈도우 공유폴더 여부 점검				
점검 목적	불필요하게 공유되고 있는 폴더가 있는지 확인하여 비인가자의 접근 가능성 차단과 이를 통한 자료 유출 방지				
보안 위협	- 관리되지 않는 불필요한 공유 폴더는 자료 유출, 악성코드 유포 경로로 활용될 수 있으며, 해당 폴더로 접근이 가능한 IP/Port가 노출되었을 경우, 비인가자에 의한 공격 대상이 될 위험이 존재함 - 윈도우 공유폴더에서 사용하는 SMB 프로토콜을 통한 취약점 공격의 주요 대상이 될 수 있음				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 공유폴더가 없을 경우</td></tr> <tr> <td>취약</td><td>불필요한 공유폴더가 존재하는 경우</td></tr> </table>	양호	불필요한 공유폴더가 없을 경우	취약	불필요한 공유폴더가 존재하는 경우
양호	불필요한 공유폴더가 없을 경우				
취약	불필요한 공유폴더가 존재하는 경우				
참고	※ SMB(Server Message Block) : 네트워크 파일 및 프린터 공유를 위한 프로토콜로, 클라이언트와 서버 간 통신을 통해 파일 및 리소스를 공유하고 접근하는 데 사용됨. 주로 Windows 기반 시스템에서 활용되며, 많은 기업에서 파일 서버 목적으로 사용하고 있음				

❖ 점검 및 조치 방법

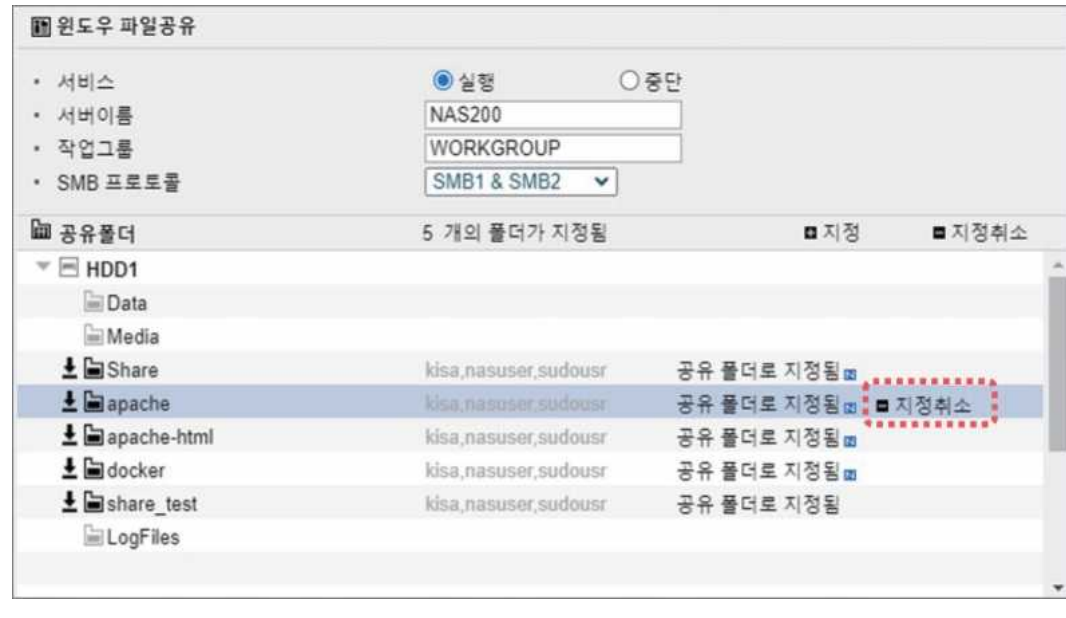
○ 윈도우 공유폴더 현황 점검

- ▶ [서비스 관리 > 윈도우 파일공유] 탭에서 파일공유 서비스 활성화 여부와 공유폴더 확인
- ▶ **윈도우 공유폴더를 사용하지 않는 경우** 서비스 비활성화(중단)



○ 불필요 공유폴더 존재 시 비활성화 또는 삭제

- ▶ [서비스 관리] > 윈도우 파일공유] 탭에서 불필요 공유폴더 ‘지정 취소’ 선택 후 저장
- ▶ 의심되는 폴더 존재 시 인터뷰를 통해 필요/불필요 공유폴더 사용 여부 확인



7.4 패치 및 보안 관리

iptime-08 제조사에서 제공하는 최신 업데이트 적용

❖ 취약점 개요

점검 내용	제조사에서 제공하는 펌웨어의 최신 업데이트 여부 점검				
점검 목적	최신 업데이트를 적용하여 NAS 장치의 보안성과 시스템 안정성 확보				
보안 위협	최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 이용하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우</td></tr> </table>	양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우	취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우
양호	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하고 있는 경우				
취약	제조사에서 제공하는 최신 펌웨어 업데이트를 적용하지 않고 있는 경우				
참고	※ 펌웨어(Firmware) : 프로그래밍의 일종인 펌웨어는 하드웨어를 제어하는 소프트웨어 운영체제 프로그램으로 하드웨어 제어를 통해 하드웨어 역할을 하는 하드웨어와 소프트웨어의 중간자 역할 수행				

❖ 점검 및 조치방법

○ 업데이트 현황 확인

▶ [시스템 설정] > [펌웨어 업그레이드] 탭에서 현재 펌웨어 버전 확인(최신 여부 확인)



○ 최신 업데이트 적용

▶ NAS 장치가 인터넷에 연결된 경우 '자동 업그레이드 실행' 기능을 통해 업데이트 진행



▶ NAS 장치가 폐쇄망 환경에 구축되어 인터넷 연결이 불가할 시 제조사 홈페이지에서 패치 파일을 다운로드 후 '수동 업그레이드' 진행

▶ 제조사 공식 홈페이지 > [고객지원] > [다운로드] 탭에서 제품 선택 후 장비의 최신 펌웨어 버전 및 업데이트 내용 확인



※ ipTIME 공식 홈페이지 : <https://iptime.com>

▶ 업데이트 후 시스템을 재기동해야 하는 경우가 있으므로 이를 고려하여 업데이트 설치 진행

iptime-09 악성 스크립트 접근 방지(CSRF) 활성화

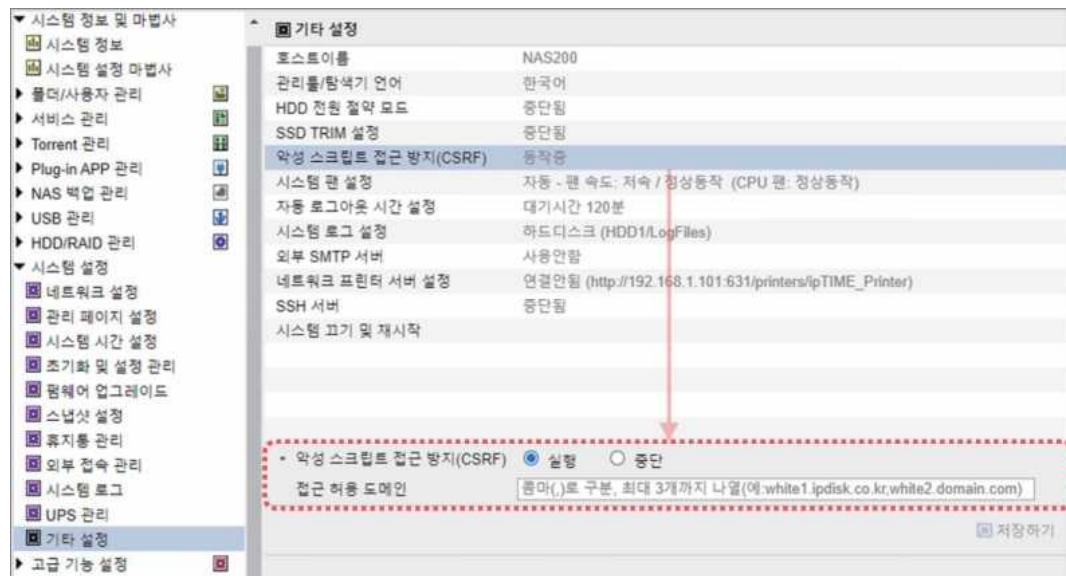
❖ 취약점 개요

점검 내용	• NAS 제조사에서 제공하는 악성 스크립트 접근 방지(CSRF) 기능 활성화 여부 점검
점검 목적	• 악성 스크립트 접근 방지(CSRF) 기능을 활성화하여 관리자 권한 탈취 등의 다양한 침해사고를 방지하기 위함
보안 위협	• 악성 스크립트 접근 방지(CSRF) 기능이 비활성화되어 있다면 일반 사용자가 로그인된 상태일 때, 특정 페이지에 악의적인 내용의 웹 요청을 통해 관리자 계정의 패스워드 변경 등으로 권한 탈취의 위험이 존재함
점검 기준	양호 악성 스크립트 접근 방지(CSRF) 기능이 활성화되어 있는 경우 취약 악성 스크립트 접근 방지(CSRF) 기능이 비활성화되어 있는 경우
참고	※ CSRF 공격(Cross Site Request Forgery) : 웹 애플리케이션에서 발생할 수 있는 보안 취약점으로 사용자가 의도하지 않은 요청을 악의적으로 공격하는 기법. 일반적으로 CSRF 공격은 사용자가 웹 애플리케이션에 로그인한 상태에서 공격자는 해당 사용자의 인증 정보를 이용하여 악의적인 요청(POST) 전송을 통해 사용자 권한 탈취

❖ 점검 및 조치방법

○ 악성 스크립트 접근 방지(CSRF) 기능 활성화 여부 확인

- ▶ [시스템 설정] > [기타 설정] 탭에서 악성 스크립트 접근 방지(CSRF) 기능 선택 후 활성화 여부 확인 후 중단되어있는 경우 해당 기능 활성화



iptime-10 방화벽 기능 활성화

🔒 취약점 개요

점검 내용	• 방화벽 기능 활성화 및 정책 설정 적용 여부 점검				
점검 목적	• 방화벽 기능 활성화하고 접근통제 정책 설정을 적용하여 비인가자 IP의 무분별한 접근을 사전에 차단하고, 침해사고 발생 시 책임추적을 용이하게 하기 위함				
보안 위협	• 방화벽 설정으로 적절한 접근통제가 이루어지지 않을 경우, 불법 접근 및 데이터 유출, 서비스 거부 공격 등의 외부 공격으로부터 다양한 보안 위협에 노출될 위험이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>방화벽이 활성화 및 별도 접근통제 정책을 적용하고 있는 경우</td></tr> <tr> <td>취약</td><td>방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우</td></tr> </table>	양호	방화벽이 활성화 및 별도 접근통제 정책을 적용하고 있는 경우	취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우
양호	방화벽이 활성화 및 별도 접근통제 정책을 적용하고 있는 경우				
취약	방화벽이 비활성화되어 있거나, 접근통제 정책을 적용하고 있지 않은 경우				
참고	※ 방화벽 : 접근 제어, 패킷 필터링, 로그 및 감사 등을 지원하는 네트워크 보안 장비의 하나로, 기본적으로 출발지 IP, 목적지 IP와 Port를 사용하여 접근통제 정책을 설정함 ※ 화이트리스트 방식 : 기본적으로 모든 접근을 막아놓고 액세스 허용 목록을 통해 접근 허용 대상만 따로 등록하는 방식 ※ 블랙리스트 방식 : 기본적으로 모든 접근을 허용하되 특정 사람, 웹 사이트, 프로그램 등을 차단하는 액세스 거부 목록을 통해 접근하지 못하는 예외를 두는 방식				

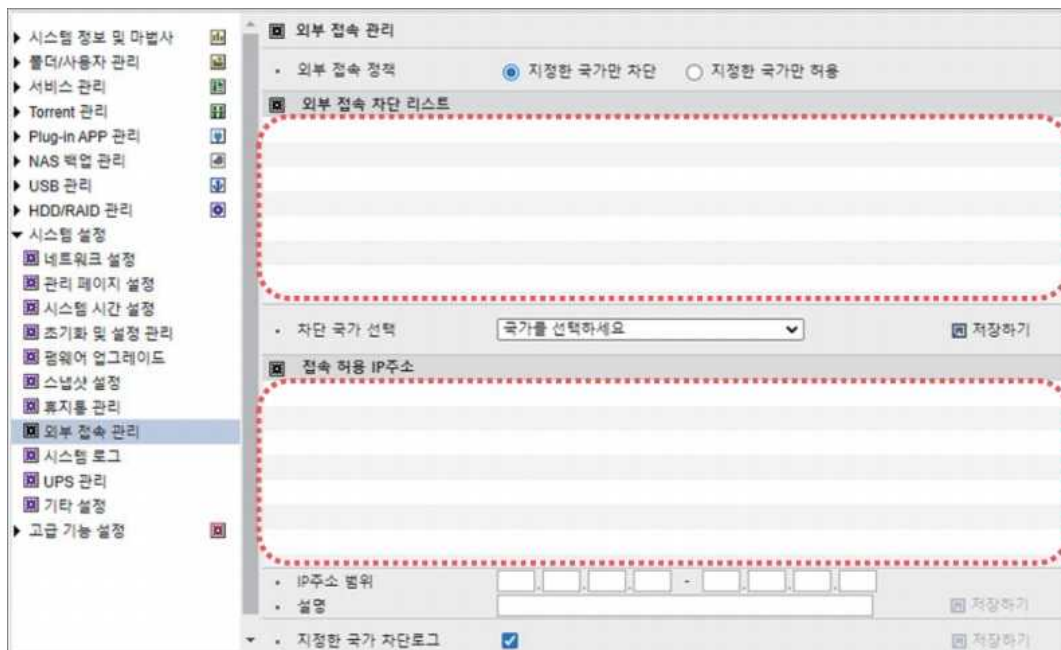
🔒 점검 및 조치방법

○ 방화벽 규칙(정책) 목록 확인 및 신규정책 생성(해외 IP 차단)

▶ [시스템 설정] > [외부 접속 관리] 탭에서 외부 접속 정책, 차단 국가, 허용 IP 등 방화벽 정책 점검

※ ipTIME NAS 장치의 방화벽 정책 방식

정책 모델	정책명	범위
블랙 리스트	지정한 국가만 차단	국가, IP 대역 단위로 설정 가능
화이트 리스트	지정한 국가만 허용	

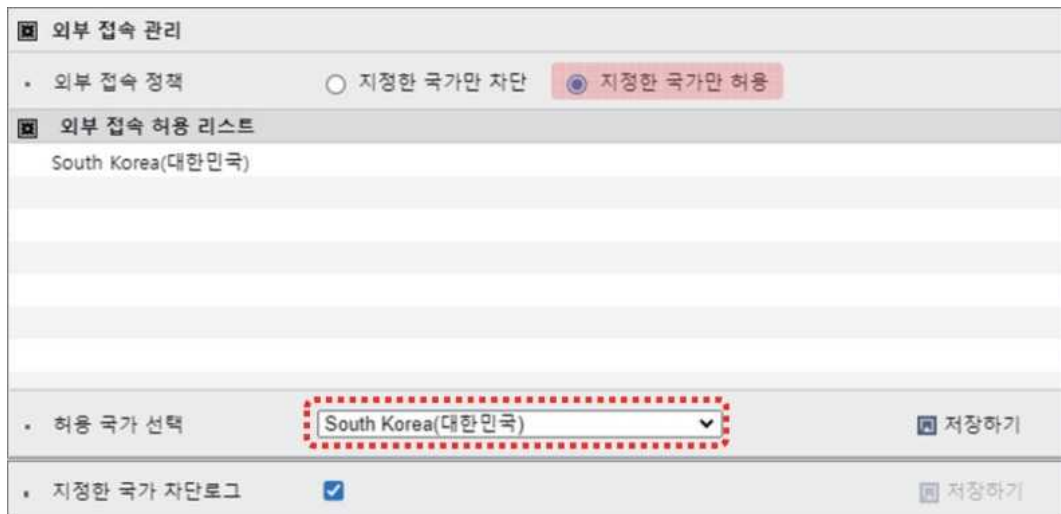


○ 신규정책 생성(해외 IP 차단)

- ▶ [시스템 설정] > [외부 접속 관리] 탭에서 '지정된 국가만 허용' 선택 후 허용 국가 선택 드롭박스 목록에서 '대한민국' 선택 후 저장

※ 하단 '지정된 국가 차단 로그' 설정을 활성화하여 외부에서 시도하는 비인가 접근에 대한 감사 로그 설정을 권장

- ▶ 하단 '접속 허용 IP 주소' 설정으로 IP 단위로 접근 정책을 설정할 수 있음



※ 방화벽 규칙(정책)은 NAS 장치를 운영하는 목적에 따라 적절하게 설정하여야 하며 각 응용 프로그램 서비스, 접속 IP에 따라 규칙을 생성하여 외부 접근을 통제할 수 있다. NAS 장치를 국내에서만 사용하는 경우 해외IP 차단 규칙을 통해 불필요한 해외에서의 접근을 차단하는 것을 권장

7.5 로그 및 백업 관리

iptime-11 로그 관리

❖ 취약점 개요

점검 내용	• 내부 정책에 따른 적절한 시스템 로그 관리 여부 점검				
점검 목적	• 보안사고 발생 시 가시성 및 책임추적성을 확보하여 원인을 파악하기 위함				
보안 위협	• 로그 관리를 하지 않을 경우, 장애 및 침해사고 발생으로 피해 발생 시 원인 규명, 사후 추적 등 분석의 어려움이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>주요 서비스 로그 활성화가 되어있는 경우</td></tr> <tr> <td>취약</td><td>주요 서비스 로그 활성화가 되어있지 않은 경우</td></tr> </table>	양호	주요 서비스 로그 활성화가 되어있는 경우	취약	주요 서비스 로그 활성화가 되어있지 않은 경우
양호	주요 서비스 로그 활성화가 되어있는 경우				
취약	주요 서비스 로그 활성화가 되어있지 않은 경우				
참고	※ 감사 로그 설정이 너무 높으면 불필요 로그가 기록되어 중요한 로그 기록과 혼동 및 시스템 성능 저하와 같은 영향을 받을 수 있으므로 법적 요구 사항과 조직의 정책·지침에 따라 원인 규명, 책임 추적을 위한 로그만 설정할 것을 권고함 ※ 책임추적성 : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙으로 시스템에 누가, 언제, 어떠한 행동을 했는지 기록하여 필요시 규칙을 위반한 행위자를 추적할 수 있음				

❖ 점검 및 조치방법

○ 정상적으로 로그가 기록되고 있는지 점검

▶ [시스템 설정] > [시스템 로그] 탭에서 로그가 정상적으로 기록되고 있는지 확인

The screenshot shows the '시스템 로그' (System Log) interface. The left sidebar has a tree view with '시스템 정보 및 마법사' (System Info & Wizard) expanded, showing '시스템 정보' (System Info), '시스템 설정 마법사' (System Setup Wizard), '폴더/사용자 관리' (Folder/User Management), '서비스 관리' (Service Management), 'Torrent 관리' (Torrent Management), 'Plug-in APP 관리' (Plug-in APP Management), 'NAS 백업 관리' (NAS Backup Management), 'USB 관리' (USB Management), 'HDD/RAID 관리' (HDD/RAID Management), '시스템 설정' (System Settings), '네트워크 설정' (Network Settings), '관리 페이지 설정' (Management Page Settings), '시스템 시간 설정' (System Time Settings), '초기화 및 설정 관리' (Reset & Settings Management), '필름웨어 업그레이드' (Firmware Upgrade), '스냅샷 설정' (Snapshot Settings), '휴지통 관리' (Trash Management), '외부 접속 관리' (External Access Management), '시스템 로그' (System Log), 'UPS 관리' (UPS Management), '기타 설정' (Other Settings), and '고급 기능 설정' (Advanced Feature Settings). The '시스템 로그' (System Log) option is selected and highlighted in blue.

The main panel shows the '시스템 로그' (System Log) tab. It has a search bar with '날짜' (Date) and '분류' (Category) filters. Below the filters is a table of logs. The table has three columns: '시간' (Time), '분류' (Category), and '설명' (Description). The logs are listed in descending order of time. The first log is from 2023.10.30 at 9:20:56, categorized as '관리 콘솔' (Management Console), with the description '[사용자:sudouser(218.153.104.54)] 관리콘솔로 로그인하였습니다.' (User:sudouser(218.153.104.54) logged in to the management console.). The second log is from 2023.10.27 at 5:27:27, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] 윈도우 파일공유 서비스가 시작되었습니다.' (User:sudouser(218.153.104.54) Windows file sharing service started.). The third log is from 2023.10.27 at 5:27:27, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] SSH 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) SSH service ended.). The fourth log is from 2023.10.27 at 5:27:27, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] FTP 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) FTP service ended.). The fifth log is from 2023.10.27 at 5:27:27, categorized as '사용자 관리' (User Management), with the description '[사용자:sudouser(218.153.104.54)] 사용자 'nasuser'의 설정을 변경하였습니다.' (User:sudouser(218.153.104.54) changed the settings of user 'nasuser'). The sixth log is from 2023.10.27 at 5:27:23, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] 윈도우 파일공유 서비스가 시작되었습니다.' (User:sudouser(218.153.104.54) Windows file sharing service started.). The seventh log is from 2023.10.27 at 5:27:23, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] SSH 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) SSH service ended.). The eighth log is from 2023.10.27 at 5:27:23, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] FTP 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) FTP service ended.). The ninth log is from 2023.10.27 at 5:26:05, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] 윈도우 파일공유 서비스가 시작되었습니다.' (User:sudouser(218.153.104.54) Windows file sharing service started.). The tenth log is from 2023.10.27 at 5:26:05, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] SSH 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) SSH service ended.). The eleventh log is from 2023.10.27 at 5:26:05, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] FTP 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) FTP service ended.). The twelfth log is from 2023.10.27 at 5:26:05, categorized as '사용자 관리' (User Management), with the description '[사용자:sudouser(218.153.104.54)] 사용자 'sudouser'의 설정을 변경하였습니다.' (User:sudouser(218.153.104.54) changed the settings of user 'sudouser'). The thirteenth log is from 2023.10.27 at 5:25:50, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] 윈도우 파일공유 서비스가 시작되었습니다.' (User:sudouser(218.153.104.54) Windows file sharing service started.). The fourteenth log is from 2023.10.27 at 5:25:50, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] SSH 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) SSH service ended.). The fifteenth log is from 2023.10.27 at 5:25:50, categorized as '서비스 관리' (Service Management), with the description '[사용자:sudouser(218.153.104.54)] FTP 서비스가 종료되었습니다.' (User:sudouser(218.153.104.54) FTP service ended.). The sixteenth log is from 2023.10.27 at 5:25:49, categorized as '사용자 관리' (User Management), with the description '[사용자:sudouser(218.153.104.54)] 사용자 'etouser'를(을) 추가하였습니다.' (User:sudouser(218.153.104.54) added user 'etouser'). The seventeenth log is from 2023.10.27 at 5:06:28, categorized as '시스템 관리' (System Management), with the description '[사용자:sudouser(218.153.104.54)] 시스템 설정 마법사를 시작하였습니다.' (User:sudouser(218.153.104.54) started the system settings wizard.).

○ 최대 로그 사이즈 설정

- ▶ [시스템 설정] > [기타 설정] > [시스템 로그 설정] 탭에서 '최대 로그 사이즈' 설정
- ▶ 로그 사이즈는 로그 분석 시 가시성 확보를 위해 가능한 크게 설정하는 것을 권장하며, '디스크 경고 메일 수신' 설정 등 시스템 용량에 대한 모니터링을 필요로 함



iptime-12 백업 관리

취약점 개요

점검 내용	NAS 장치에 저장된 데이터 백업 여부 점검						
점검 목적	장애 및 보안사고 발생 시 피해로부터 신속한 복구를 하기 위해 중요자료에 대한 2차 백업 (클라우드, 외부 저장매체, 스냅샷 등)을 설정하고 있는지 점검하여 자료 손실에 대비한 대응체계 점검						
보안 위협	NAS 장치에 저장된 데이터를 노리는 랜섬웨어 및 해킹 공격으로 인한 데이터 변조, 유출, 암호화의 위험이 존재함						
점검 기준	<table border="1"> <tr> <td>양호</td><td>주기적인 백업 관리를 이행하고 있는 경우</td></tr> <tr> <td>취약</td><td>주기적인 백업 관리를 이행하지 않는 경우</td></tr> </table>	양호	주기적인 백업 관리를 이행하고 있는 경우	취약	주기적인 백업 관리를 이행하지 않는 경우		
양호	주기적인 백업 관리를 이행하고 있는 경우						
취약	주기적인 백업 관리를 이행하지 않는 경우						
참고	※ NAS 장치에서 데이터 백업 종류 <table border="1"> <tr> <td>외부 저장매체 활용</td><td>네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식</td></tr> <tr> <td>외부 저장소 동기화</td><td>클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음</td></tr> <tr> <td>스냅샷(Snapshot) 기능 활용</td><td>제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함</td></tr> </table> ※ 백업 방식별 장·단점을 고려하여 데이터 백업을 진행하고, 중요한 데이터일수록 다중 백업을 적용하여 복구 신뢰성을 확보하여야 함	외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식	외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음	스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함
외부 저장매체 활용	네트워크가 연결되지 않은 외장하드, USB 등을 이용하여 자료를 백업하는 방식으로 상대적으로 시간이 많이 소요될 수 있으나, 네트워크를 통한 악성코드 전파 등 2차 피해에 대해 효율적인 방식						
외부 저장소 동기화	클라우드, 외부 NAS 등과 rsync 서비스, 별도 백업 솔루션 등을 이용하여 동기화하는 방식으로 편리하게 백업을 진행할 수 있으며, 최초 백업이후에는 변경된 데이터만 백업할 수 있다. 다만, 랜섬웨어 감염 시 네트워크가 상시로 연결되어 실시간 동기화를 사용하는 경우 백업 자료에도 영향을 끼칠 수 있음						
스냅샷(Snapshot) 기능 활용	제조사에서 제공하는 스냅샷 기능을 활용하여 복원 지점을 생성할 수 있으며 데이터가 변조되거나 유실되었을 때 복원 지점으로 롤백하여 손실된 데이터를 복구 할 수 있음. 다만, 복구 지점부터 현 시점까지의 데이터 변경은 반영되지 않으며, 스냅샷 파일 자체가 훼손된 경우 복구가 불가능함						

점검 및 조치방법

- ipTIME NAS 장치에서는 데이터 백업을 위해 다양한 서비스를 제공하고 있으며, 사용자 환경에 맞는 백업 방식 및 매체를 선정하여 백업을 진행하여야 함

방식	설명
USB, 외장하드 등 외부 장치 활용	• NAS 장치에 USB, 외장하드와 같은 외부 저장매체를 연결하여 수동으로 데이터 백업을 수행할 수 있음
NAS 백업 서버 활용 (ipTIME)	• ipTIME NAS 장치를 추가 보유하고 있다면, 서버-클라이언트 연결을 통해 진행하는 방식 • ipTIME에서 제공하는 백업 관리 기능을 이용하여 백업 주기, 백업 대상, 접속 계정 등을 설정하여 데이터 백업을 수행할 수 있음 ※ [NAS 백업 관리] > [NAS 백업 서버], [NAS 백업 클라이언트] 탭
파일 서비스 활용	• ipTIME NAS 장치에서 제공하는 다양한 파일 서비스(SMB, FTP, WebDAV 등)를 이용하여 외부 저장소와 원격으로 연결을 통해 수동으로 데이터 백업을 수행 ※ [서비스 관리] > 각 파일 서비스 탭
클라우드 서비스 활용	• ipTIME Cloud 서비스를 통해 NAS 장치의 홈 폴더와 내PC 폴더 간 '동기화 기능' 진행. 단, 어느 한쪽의 데이터 변경 시 양쪽 모두에 변경사항이 적용됨. 복수의 PC에 동기화를 진행할 수 있음 ※ [서비스 관리] > [ipTIME Cloud 서비스] 탭 • CloudBackup 서비스를 이용하여 파일 및 폴더를 외부 저장소에 백업할 수 있으며 양방향 백업 가능 ※ [서비스 관리] > [CloudBackup 서비스] 탭

○ ipTIME NAS 백업 관리를 통한 정기백업 실시

- ▶ 별도의 ipTIME NAS 백업 장비를 보유하고 있는 경우, 서버-클라이언트 설정을 통해 정기적인 백업을 실시할 수 있음
- ▶ [NAS 백업 관리] > [NAS 백업 클라이언트] 탭에서 백업을 진행할 NAS 서버 정보 입력 및 백업 주기, 백업 폴더 설정

- ▶ 백업 서버로 지정할 NAS 장치의 [NAS 백업 관리] > [NAS 백업 서버] 탭에서도 클라이언트에서 설정한 접속계정 및 포트를 동일하게 설정하여야 함

iptime-13 NTP 서버 연동

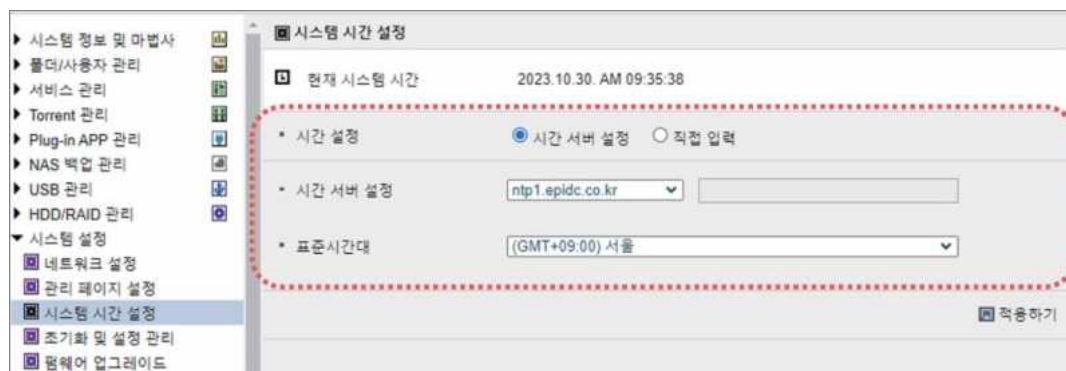
🔒 취약점 개요

점검 내용	• NTP 서버 연동 설정 적용 여부 점검				
점검 목적	• 시스템 운영 또는 보안사고 발생으로 인한 로그 분석 과정에서 이벤트 간의 인과 관계 파악에 도움을 주고 로그 자체의 신뢰성을 확보하기 위함				
보안 위협	• 시스템 간 시간 동기화 미흡으로 보안사고 및 장애 발생 시 로그에 대한 신뢰도 확보 미흡				
점검 기준	<table border="1"> <tr> <td>양호</td><td>NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우</td></tr> <tr> <td>취약</td><td>NTP 서버와 연동되어 있지 않은 경우</td></tr> </table>	양호	NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우	취약	NTP 서버와 연동되어 있지 않은 경우
양호	NTP 서버를 통한 시스템 간 실시간 시간 동기화가 설정된 경우				
취약	NTP 서버와 연동되어 있지 않은 경우				
참고	※ NTP(Network Time Protocol) : 네트워크를 통해 컴퓨터 시스템 간의 시간을 정확하게 유지 시켜주기 위한 네트워크 프로토콜. ※ Public NTP 서버 : 글로벌 IT 기업(Google, Microsoft), 비영리 단체(ntppool.org) 등에서 제공하고 있는 공개된 NTP 서버로 국내에서는 주요 통신사(LG유플러스, KT 등)에서 제공하고 있음				

🔒 점검 및 조치방법

○ NTP 서버 연동 여부 점검

- ▶ [시스템 설정] > [시스템 시간 설정] 탭에서 '시간 서버 설정'에 NTP 서버 주소 입력
- ▶ NAS 장치가 폐쇄망 환경에서 운영되는 경우 별도 NTP 서버를 구축하여 내부 시스템 간 시간 동기화 권장



7.6 서비스 관리

iptime-14 불필요한 서비스 사용 금지

❖ 취약점 개요

점검 내용	• 사용하지 않는 서비스 활성화 여부 점검				
점검 목적	• 불필요한 서비스 활성화로 인한 시스템 성능 저하 및 잠재적인 보안 취약점 노출 위험을 예방하기 위해 불필요한 서비스 활성화 여부 점검				
보안 위험	• NAS 장치에서 제공되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침입의 가능성이 존재함				
점검 기준	<table border="1"> <tr> <td>양호</td><td>불필요한 서비스 사용이 비활성화된 경우</td></tr> <tr> <td>취약</td><td>불필요한 서비스 사용이 활성화된 경우</td></tr> </table>	양호	불필요한 서비스 사용이 비활성화된 경우	취약	불필요한 서비스 사용이 활성화된 경우
양호	불필요한 서비스 사용이 비활성화된 경우				
취약	불필요한 서비스 사용이 활성화된 경우				
참고	※ 서비스 사용이 필요한 경우에도 서비스 오남용 방지를 위해 계정(또는 그룹)별 사용 권한을 부여하여 필수 계정만 사용할 수 있도록 통제하는 것을 권장				

❖ 점검 및 조치방법

○ 불필요한 서비스 활성화 여부 점검

- ▶ [서비스 정보 및 마법사] > [시스템 정보] 탭에서 실행 중인 서비스 목록 확인 및 불필요한 서비스의 실행 여부 점검

The screenshot shows the 'System Information' tab in the NAS management interface. The left sidebar lists various system settings, and the main area displays system details. A red dashed box highlights the 'System Running Time' (up 1 week, 4 days, 15 hours, 55 minutes) and the 'Services' section, which lists various services and their status (e.g., FTP, ipDISK, MySQL, Apache, IP CAM, WebDAV, URL, RADIUS, CloudBackup, ipTIME Cloud, Docker, SSH, Portmap, NAS Backup, Network Printer, Hard Disk & CPU Status).

▶ 서비스별 설정 위치

서비스명	설정 위치
윈도우 파일공유(SMB)	[서비스 관리] > [윈도우 파일공유]
FTP	[서비스 관리] > [FTP 서버]
ipDISK(DDNS) 서비스	[서비스 관리] > [ipDISK(DDNS) 서비스]
미디어 서버	[서비스 관리] > [미디어 서버]
MYSQL	[서비스 관리] > [MYSQL 서버]
Apache	[서비스 관리] > [Apache 서버]
IP CAM 서비스	[서비스 관리] > [IP CAM 서비스]
WebDAV	[서비스 관리] > [WebDAV 서비스]
URL 서비스	[서비스 관리] > [URL 서비스]
RADIUS	[서비스 관리] > [RADIUS 서버]
CloudBackup	[서비스 관리] > [CloudBackup 서비스]
ipTIME cloud	[서비스 관리] > [ipTIME Cloud 서비스]
Docker	[서비스 관리] > [Docker 서비스]
Torrent	[Torrent 관리] > [Torrent 서비스]
NAS 백업 서버	[NAS 백업관리] > [NAS 백업 서버]
NAS 백업 클라이언트	[NAS 백업관리] > [NAS 백업 클라이언트]
SMTP 서버	[시스템 설정] > [기타 설정] > [외부 SMTP 서버]
네트워크 프린터 서버	[시스템 설정] > [기타 설정] > [네트워크 프린터 서버]
SSH 서버	[시스템 설정] > [기타 설정] > [SSH 서버]

▶ 위 서비스 목록 중 사용하지 않는 서비스가 동작중인경우 각 서비스 설정 위치에서 서비스 중단 (예시) Apache 서버
※ [서비스 관리] > [Apache 서버]



iptime-15 안전한 FTP 서비스 사용

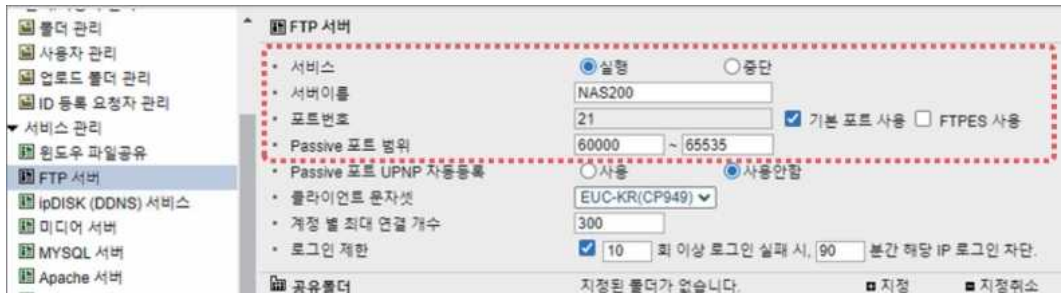
취약점 개요

점검 내용	FTP 서버 서비스 활성화 시 FTPES 사용 여부 점검										
점검 목적	보안에 취약한 FTP 서비스 사용은 지양하고, FTP 서비스 사용이 필요한 경우 암호화된 파일 전송 프로토콜(FTPES)을 사용하여 안전한 데이터 전송을 하기 위함										
보안 위협	FTP는 파일을 전송하기 위한 프로토콜로 계정과 패스워드를 암호화하지 않고 평문 전송하여 네트워크 스니핑 등의 위협으로부터 계정 정보 및 모든 전송 데이터에 대한 침해사고 가능성이 존재함										
점검 기준	<table border="1"> <tr> <td>양호</td><td>FTP 서버 서비스를 사용하지 않거나, FTPES 프로토콜을 사용하고 있는 경우</td></tr> <tr> <td>취약</td><td>FTP 서버 서비스를 사용하고 있고, FTPES 프로토콜을 사용하지 않는 경우</td></tr> </table>	양호	FTP 서버 서비스를 사용하지 않거나, FTPES 프로토콜을 사용하고 있는 경우	취약	FTP 서버 서비스를 사용하고 있고, FTPES 프로토콜을 사용하지 않는 경우						
양호	FTP 서버 서비스를 사용하지 않거나, FTPES 프로토콜을 사용하고 있는 경우										
취약	FTP 서버 서비스를 사용하고 있고, FTPES 프로토콜을 사용하지 않는 경우										
참고	※ 파일 전송 프로토콜(FTP) 버전 <table border="1"> <thead> <tr> <th>버 전</th><th>설 명</th></tr> </thead> <tbody> <tr> <td>FTP (File Transfer Protocol)</td><td>기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)</td></tr> <tr> <td>SFTP (SSH File Transfer Protocol)</td><td>SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)</td></tr> <tr> <td>FTPS (FTP Secure)</td><td>FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)</td></tr> <tr> <td>FTPES (FTP over Explicit TLS/SSL)</td><td>FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)</td></tr> </tbody> </table> * SSL(Secure Sockets Layer) : 웹에서 데이터를 안전하게 전송하기 위해 사용되는 프로토콜 * TLS(Transport Layer Security) : SSL의 후속 프로토콜로, SSL 3.0의 보안 취약성을 보완하고 개선된 버전	버 전	설 명	FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)	SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)	FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)	FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)
버 전	설 명										
FTP (File Transfer Protocol)	기본적인 파일 전송 프로토콜로 데이터와 제어 연결이 분리되어 있으며, 데이터 및 제어 연결이 암호화되어 있지 않음 (Port : 21)										
SFTP (SSH File Transfer Protocol)	SSH 프로토콜을 기반으로 하는 안전한 파일 전송 프로토콜로 사용자 인증, 데이터 암호화, 무결성 보호 등 다양한 보안 기능 제공 (Port : 22)										
FTPS (FTP Secure)	FTP에 SSL 또는 TLS와 같은 보안 계층을 추가하여 암호화된 제어 연결 및 데이터 연결로 데이터의 기밀성과 무결성을 강화한 프로토콜 (Port : 990)										
FTPES (FTP over Explicit TLS/SSL)	FTP에 명시적인 TLS/SSL을 추가한 것으로 FTPS와 유사한 수준의 보안 수준 제공 (Port : 21)										

점검 및 조치방법

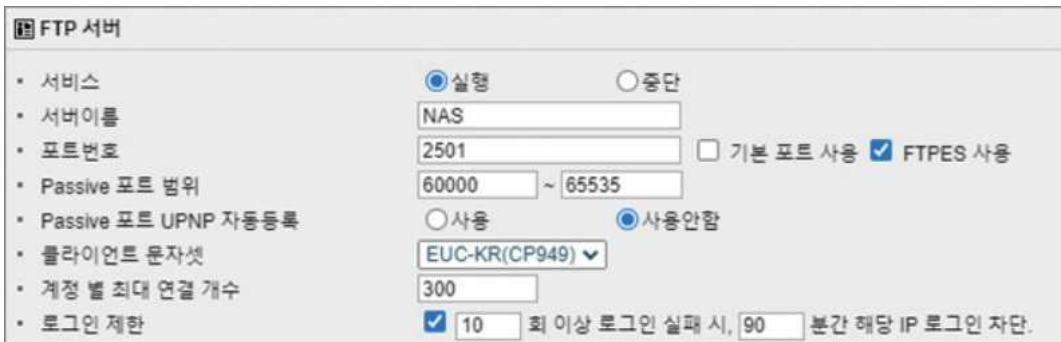
FTP 서비스 설정 확인

▶ [서비스 관리] > [FTP 서버] 탭에서 서비스 실행 여부, 기본 포트 변경 여부, FTPES 사용 여부 등을 점검



안전한 FTP 서비스 사용 설정

- ▶ FTP 서비스를 사용하지 않는 경우 서비스 사용 중단
- ▶ FTP 서비스 사용이 필요한 경우 데이터 암호화를 제공하는 FTPES 프로토콜을 사용하고, 기본 포트는 알려지지 않은 포트로 변경하여 사용할 것을 권장



※ 포트 번호 변경 시 내부에 방화벽, 공유기 등을 사용하는 경우 '포트 포워딩' 기능을 사용하여 외부에서 변경된 포트로 접속할 수 있도록 설정하여야 함



맺음말

08

08

맺음말



보안은 현대 디지털 환경에서 가장 중요한 과제 중 하나로 부각되고 있습니다. 데이터의 증가와 함께 NAS 서버의 활용이 증가되었으며, 지능화된 사이버 공격 및 랜섬웨어의 발달로 안전한 데이터 관리는 기업과 개인에게 절대적인 필요성이 되었습니다.

또한 NAS 서버가 데이터 저장과 공유의 핵심 장치로 부상하고 다양한 부가 서비스를 제공하는 만큼 보안에 대한 요구도 커지고 있습니다. 중요한 데이터를 안전하게 보호하고, 랜섬웨어 공격을 사전에 예방해야 하며, 기업에서는 규정 준수를 통해 비즈니스 연속성을 확보하는 것은 이제 불가피한 필수과제입니다.

본 가이드는 이에 대한 사용자들의 인식을 높이고 효과적인 보안 대책을 마련할 수 있도록 도와주는 데 초점을 맞추고 있습니다.

한국인터넷진흥원이 제공하는 '내서버 돌보미 서비스'는 이러한 상황에서 중소기업의 정보시스템 보안을 강화하고자 노력하고 있으며 앞으로도 보다 강력하고 체계적인 보안 정책을 제시하여 사용자들이 안전하게 디지털 기술을 활용할 수 있도록 노력할 것입니다.

모든 기업과 개인에게 더 나은 보안 환경과 혁신적인 디지털 환경을 제공하기 위해 계속해서 노력하겠습니다. 감사합니다.

안전한 데이터 보호를 위한
NAS 보안 가이드

인 쇄 2024. 2월

발 행 2024. 2월

발행처 한국인터넷진흥원
(58324) 전라남도 나주시 진흥길 9
(한국인터넷진흥원)
TEL 1544-5118 FAX 405-5119
www.kisa.or.kr | www.krcert.or.kr
