VERITAS

NetBackup 보안이 구현된 Flex Appliance

Veritas Flex Appliance는 완벽한 변조 불가 스토리지 솔루션을 제공하여 소프트웨어와 하드웨어에서 백업 데이터를 보호하고 복구합니다.

본 백서는 NetBackup™ 보안이 구현된 Veritas Flex Appliance의 침입 탐지 및 차단, OS 하드닝, 멀티테넌시 보안 기능을 조명합니다.

베리타스 백서 | 2020년 10월

목차

소개

요약

은행, 테크놀로지, 소매업체, 정부를 대상으로 세간의 이목을 끈 사이버 공격의 여파로 기업은 다음 피해자가 되지 않기 위해 노력하고 있습니다. 오늘날 보안 위협은 모든 기업의 주요 관심사입니다. 랜섬웨어 공격, 하드웨어 장애, 실수 또는 의도적인 데이터 파괴 등 그 원인이 무엇이든지 데이터 유출 사고는 고객에게 심각한 피해를 입힐 수 있습니다.

Veritas Flex Appliance는 Veritas NetBackup™ 데이터 보호 기능에 민첩성, 레질리언스, 확장성, 간소화 등의 이점을 제공합니다. Flex Appliance는 SELinux(Security-Enhanced Linux)를 사용하여 침입 탐지 및 차단 기능과 OS 하드닝을 제공합니다. NetBackup 소프트웨어와 Flex Appliance가 제공하는 완벽한 변조 불가 스토리지 솔루션을 통해 소프트웨어 및 하드웨어에서 데이터 백업과 복구를 수행할 수 있습니다.

범위

본 문서의 목적은 Flex Appliance의 SELinux IDS/IPS, OS 하드닝, 멀티테넌시 기능에 대한 상세한 기술 설명을 제공하기 위한 것입니다.

침입 탐지 및 차단 시스템

기업은 악의적인 공격과 파괴 행위로부터 고객의 데이터를 보호해야 합니다. 데이터 유출을 방지하려면 네트워크 및 시스템 모니터링에서 무결성과 보안을 확보해야 하며, 사고 발생 시 실시간으로 위협에 대처할 수 있도록 관리자와 보안 팀에 알림을 전달해야 합니다.

이를 위해 베리타스는 보안을 최우선 목표로 Flex Appliance를 개발했습니다. Linux 운영 체제 및 핵심 NetBackup 애플리케이션을 비롯해 어플라이언스를 구성하는 각각의 요소에 대해 업계 표준 및 고급 보안 제품을 모두 사용하여 취약점 관련 테스트를 완료한 상태입니다. 이러한 조치를 통해 무단 액세스와 그에 따른 데이터 유출이나 도용이 발생하는 사태를 최소화할 수 있습니다. Flex Appliance는 기본 제공된 Red Hat 지원 SELinux를 사용하여 역할, 플랫폼, 서비스, 애플리케이션을 보호합니다.

IDS 및 IPS 개요

침입 탐지 시스템(IDS)은 시스템과 네트워크 활동을 분석하여 인증되지 않은 항목이나 악의적인 활동을 식별하는 방법으로 공격, 오용, 손상 등으로부터 시스템을 보호합니다. IDS는 네트워크 활동과 시스템 구성의 취약점을 모니터링하고 감사를 수행하며 데이터 무결성을 분석할 수 있습니다. IDS에는 관리 콘솔과 센서가 포함됩니다. 콘솔은 관리 및 리포팅을 위한 것이며, 센서는 실시간으로 호스트나 네트워크를 모니터링하는 에이전트에 해당합니다. IDS는 이전에 탐지된 공격의 패턴을 나타내는 공격 시그니처의 데이터베이스를 보유하고 있으며, 일반적으로 IDS는 호스트 기반 IDS와 네트워크 기반 IDS의 두 가지 유형으로 분류됩니다. 호스트 기반 IDS의 경우 각 호스트에 탐지 시스템을 구현해야 하며, 네트워크 기반 IDS는 특정 호스트로 전송하기 전에 단일 디바이스를 통해 패킷을 전달합니다.

침입 차단 시스템(IPS)은 방화벽을 강화하고 분석 레이어를 제공하여 위험한 컨텐트를 선별합니다. IPS는 적극적으로 네트워크를 분석하고 해당 네트워크로 유입되는 모든 트래픽 흐름에 대해 자동으로 조치를 수행합니다. IPS가 침입을 탐지한 경우 트래픽을 차단하고 타깃에 도달하지 못하도록 방지합니다. 여기에는 악의적인 패킷을 중단시키거나 원본 주소에 대한 트래픽을 차단하고 연결을 재설정하는 등의 조치가 포함될 수 있습니다.

Flex Appliance의 IPS/IDS 솔루션은 다음과 같은 기능을 제공합니다.

- Linux OS 구성 요소 하드닝
- 운영 체제 취약점으로 인해 기반 호스트 시스템의 무결성이 손상되지 않도록 악성 코드 차단 및 억제
- 시스템 권한에 관계없이 Appliance 데이터 액세스를 액세스가 필요한 프로그램과 활동으로만 엄격히 제한하는 데이터 보호 기능 제공
- Appliance 스택 하드닝
- Appliance 애플리케이션이나 신뢰할 수 있는 프로그램 및 스크립트로만 변경 사항이 엄격히 제어되도록 애플리케이션 바이너리 및 구성 설정 잠금
- 탐지 및 감사 기능 확장
- 중요한 사용자나 시스템 조치에 대한 가시성을 향상하여 보완 대책으로 PCI 등의 컴플라이언스 규정을 처리하는 유효하고 완전한 감사 추적 확보

Symantec Data Center Security

Veritas NetBackup Appliance는 SDCS(Symantec Data Center Security)를 사용하여 데이터 센터의 서버를 보호합니다. SDCS 소프트웨어는 Appliance에 포함되며 Appliance 소프트웨어 설치 시 자동으로 구성됩니다. SDCS는 정책 기반 보호 기능을 제공하며 호스트 기반 침입 차단 및 탐지 기술을 사용하여 Appliance의 보안을 유지합니다. 최소 권한 차단 기능을 사용하고 보안 관리자가 데이터 센터에서 여러 어플라이언스를 중앙에서 관리할 수 있게 도와줍니다. 시작 시 SDCS 에이전트를 실행하고 맞춤형 NetBackup Appliance IPS 및 IDS 정책을 시행합니다. SDCS는 중앙 SDCS 관리자를 사용하여 SDCS가 관리하는 다른 모든 엔터프라이즈 시스템과 함께 여러 Appliance에 대해 통합 보안 뷰를 제공합니다.

SELinux 지원 Flex Appliance

Flex Appliance 2.0 OS에는 사용자 데이터 보안을 확보하기 위한 여러 기능이 포함되어 있습니다. Appliance의 각 요소는 업계 표준 및 고급 보안 제품을 모두 사용하여 취약점에 대해 테스트를 완료한 상태입니다. 이러한 조치를 통해 무단 액세스와 그로 인한 데이터 유출 또는 도용을 최소화할 수 있습니다(SELinux 지원 Flex Appliance와 SDCS 간 비교는 표 1 참조).

Flex 2.0 OS의 보안 기능은 아래와 같습니다.

- OS 보안 하드닝(SELinux 포함)
- 락다운(Lock down) 모드 및 WORM(Write Once Read Many) 스토리지 지원: 지정한 보관 기간 동안 추가 액세스 제한 및 데이터 삭제 방지 설정 가능
- 암호 정책 강화
  - 최초 구성 중 강제로 암호를 변경하도록 하여 시스템에서 기본 암호가 활성 상태로 남아 있지 않도록 함
  - 자체 암호 정책 설정 가능: 검증을 위해 STIG(Security Technical Implementation Guides)를 사용하는 옵션 포함
  - Flex Appliance Shell의 추가 암호 보호 기능을 통해 잘못된 로그인 시도 3회 발생 시 15분간 hostadmin 계정 잠금
- 세션 타임아웃 기능: 비활성 상태가 10분간 지속되면 Flex Appliance Console 및 Flex Appliance Shell에서 자동으로 로그아웃

SELinux 개요

SELinux는 Linux 커널에 기본 제공되어 부팅 시 로드되는 LSM(Linux Security Module)으로, 관리자 제어 보안 정책을 통해 시스템의 애플리케이션, 프로세스, 파일에 대한 액세스 제어를 정의합니다. 주체(subject)로 알려진 애플리케이션이나 프로세스에서 파일 등의 객체(object)에 대한 액세스를 요청하는 경우 SELinux는 AVC(Access Vector Cache)를 사용하여 검사를 진행하며, 이때 AVC는 주체와 객체에 대한 사용 권한이 캐시되는 위치입니다. 그림 1은 주체가 객체에 대한 액세스 권한을 확보하는 방식을 설명합니다.

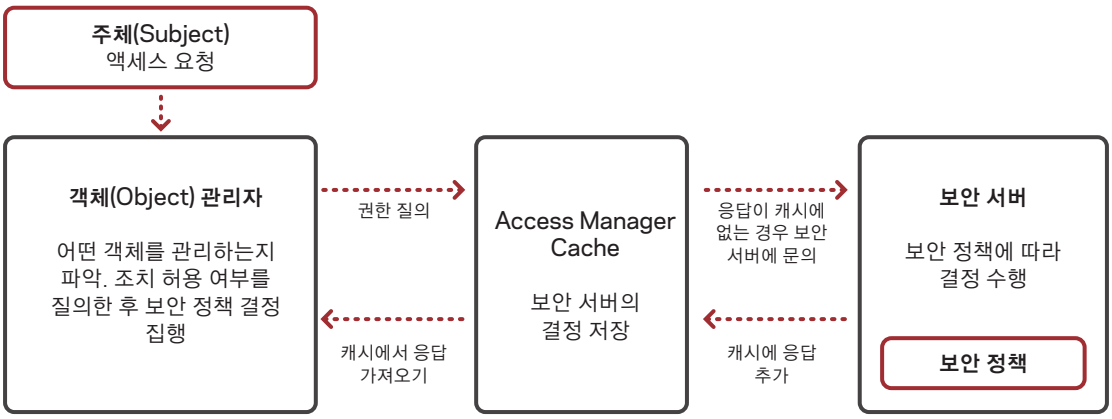

그림 1. SELinux에서 주체가 객체에 대한 액세스 권한을 확보하는 방식

SELinux는 컨테이너 분리를 통해 호스트 파일 시스템에 대한 컨테이너 공격을 방지하는 데 사용됩니다. 표준 Linux 보안 모델의 경우 superuser "root"가 모든 보안 점검을 우회할 수 있으며, 여기에는 사용자가 setuid 비트를 사용하여 실행 파일 소유자의 권한으로 실행 파일을 작동할 가능성이 포함됩니다. 이 경우 시스템에 보안 문제가 발생할 수 있습니다. SELinux는 레이블링 시스템으로, SELinux 레이블이 있는 시스템의 각 객체(모든 파일, 디렉터리, 소켓 파일, 심볼릭 링크(symlink), 공유 메모리, 세마포어(semaphore) 또는 fifo 파일)와 모든 주체(실행 프로세스 또는 Linux 유저 엔티티)를 확인합니다.

RBAC

역할 기반 액세스 제어(RBAC)는 기업 내의 사용자 역할에 따라 권한을 할당하는 것입니다. Flex Appliance는 SELinux RBAC를 사용하여 사용자를 인증하면서 OS 하드닝을 달성합니다. 사용자 권한은 권한을 취득하려는 역할을 통해 부여됩니다. 즉, Flex Appliance 로그인 계정이 SELinux 사용자에게 매핑됩니다. 그림 2는 Flex 계정 hostadmin, root 사용자, 임의의 사용 계정이 staff_r 및 guest_r 역할을 보유한 SELinux 사용자 staff_u와 guest_u에 매핑되는 것을 보여줍니다.

참고

- Flex root 계정과 임의의 맞춤형 계정은 권한 없음 바로 다음 단계인 SELinux 사용자 guest_u로 축소됩니다.
- SELinux 사용자에게는 하나 이상의 역할이 허용되며, 특정 사용자는 가질 수 있는 역할이 제한됩니다.
- 역할은 권한에 매핑되고 하나 이상의 애플리케이션에 대해 특정 도메인 및 런타임 권한이 허용됩니다.

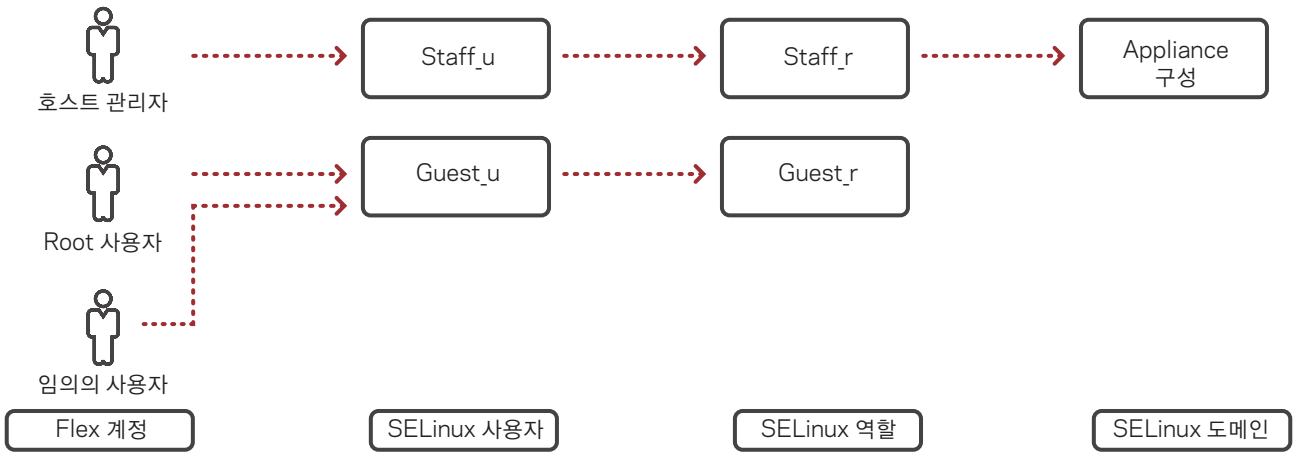

그림 2. Flex Appliance가 RBAC를 사용하여 SELinux 사용자에게 계정을 매핑하는 방법

플랫폼

Flex Appliance 플랫폼 보안을 위해 작업자 서비스는 일반(Non-Root) 사용자에 의해 실행됩니다. Flex Appliance는 구성 중에 인프라스트럭처 인증서를 적용합니다. 애플리케이션 로그는 설치 도중 발생하는 변경 사항을 트래킹합니다. Flex Appliance는 Veritas InfoScale™ 디바이스 모듈과도 통합하여 보다 향상된 셸 베이직 InfoScale 관리를 지원합니다.

서비스 및 애플리케이션

사용자는 SELinux Multi-Category Security(MCS)를 통해 카테고리별로 파일에 레이블을 지정하여 Discretionary Access Control(DAC) 및 Type Enforcement(TE) 로직을 제한할 수 있습니다.

Flex Appliance의 경우 애플리케이션과 서비스를 컨테이너화하여 실행합니다(독점적인 데이터 액세스를 위해 MCS 설정). Docker 엔진은 고유한 카테고리 쌍(C1, C2)을 지정하여 컨테이너 간에 격리할 수 있게 합니다. Flex Appliance는 각 컨테이너에 대한 독점적인 액세스를 위해 보안 컨텍스트가 탑재된 전용 파일 시스템을 제공합니다.

인증서 및 로그 파일 설계 시 고려 사항은 아래와 같습니다.

- 인증서의 경우 파일 공유를 허용하려면 MCS를 비활성화합니다.
- 로그는 /log/containers/service-name으로 이동합니다.
- MCS 정책에서 로그 순환을 허용합니다.
- 컨테이너 서비스가 로그 파일에 액세스할 수 있습니다.

	NetBackup Appliance SDCS	Flex Appliance SELinux
하드닝된 Linux OS구현	이 정책에는 규칙 세트가 있고 각 규칙 세트에는 주체, 리소스 경로, 액세스 규칙이 포함됩니다.	모든 프로세스 및 파일에 레이블이 지정되며, SELinux 정책 규칙은 프로세스가 파일과 상호 작용하는 방식을 비롯해 프로세스 간에 상호 작용하는 방식을 정의합니다. 액세스는 SELinux 정책 규칙에서 특별히 허용한 경우에만 가능합니다.
컨테이너 보호	선호되지 않음	지원 개선, Red Hat에서의 통합, 유연성 증대
중앙 집중식 관리 모드 작업	사용 가능	향후 Syslog 전달에 사용 가능
통합 및 지원 가능성	세분화 감소 및 불충분한 통합	개별 단위 런타임 옵션 증가, 개발자 및 관리자 친화적
OS 보호	OS 및 정책에 대한 사용자 이해 필요	Red Hat에서 기본적으로 OS 정책 제공
공공 부문 요건 STIG	선호되지 않음	SELinux는 STIG DISA 프로파일에서 선호하는 접근 방식
벤더	타사	Red Hat 지원, 커널 내 기본 제공
승격	IPS가 비활성화됨	IPS가 비활성화되지 않음

표 1. SDCS vs. Flex Appliance SELinux

FLEX APPLIANCE 변조 불가 스토리지

NetBackup 소프트웨어와 Flex Appliance가 제공하는 완전한 변조 불가 스토리지 솔루션을 통해 소프트웨어와 하드웨어에서 데이터 백업 및 복구를 수행할 수 있습니다. 변조 불가 및 삭제 불가 데이터는 지정한 시간 동안 변경할 수 없으므로 이중화 부족 시 사이버 범죄 침투, 내부 위협 요소, 임의의 디스크 오류로부터 데이터가 보호됩니다. 이러한 인스턴스에 저장된 모든 데이터는 다음과 같은 보안 조치를 통해 보호됩니다.

- **변조 불가** — 백업 이미지가 읽기 전용이며 백업 후 수정, 손상, 암호화가 불가능합니다.
- **삭제 불가** — 백업 이미지가 기간 만료 전에 삭제되지 않도록 보호되어, 악의적인 삭제 행위로부터 데이터가 보호됩니다.

락다운(Lock down) 모드

NetBackup 8 3 마스터 서버는 스토리지 장치와 통신하면서 변조 불가 및 삭제 불가 기능, WORM 최소 및 최대 보관 기간 설정을 수집합니다. 그런 다음 마스터 서버가 스토리지 장치에 변조 불가 컨트롤을 설정하고 WORM 보관 기간 정책을 적용합니다. NetBackup 소프트웨어는 변조 불가 잠금을 시각적으로 표현하고 WORM 보관 기간 종료 후 (명령줄 인터페이스 및 CLI를 통해) 이미지를 삭제하며 카탈로그에 자료 보존을 적용하는 등 백업 이미지를 관리합니다.

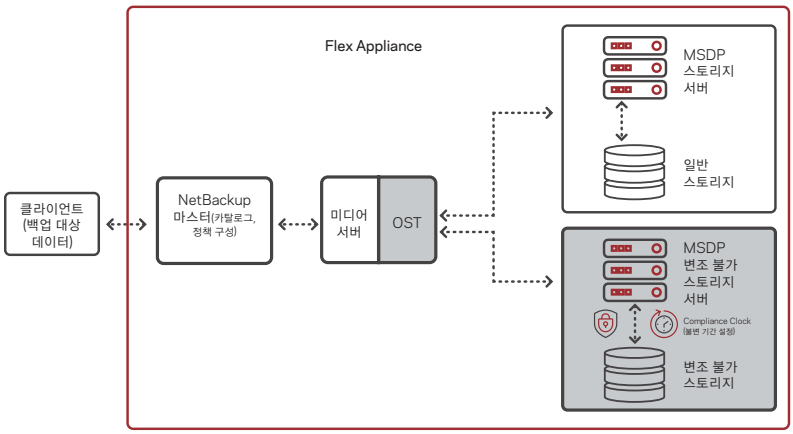

그림 3. Flex Appliance가 변조 불가 스토리지를 사용하여 데이터를 보호하는 방법

Flex Appliance는 변조 불가 스토리지 서버를 실행하여 랜섬웨어 및 악성 코드 위협에 대해 WORM 기능, Retention Lock(삭제 불가능), 플랫폼 하드닝을 제공합니다. Compliance Clock(불변 기간 설정)은 보관 기간에 사용되며 OS 시간과 무관합니다. Flex Appliance는 엔터프라이즈와 컴플라이언스의 두 가지 락다운(Lock down) 변조 불가 모드를 제공합니다. Appliance 락다운(Lock down) 상태는 언제든지 활성화할 수 있습니다. MSDP 스토리지 컨테이너 컴플라이언스 모드와 엔터프라이즈 모드 중에 선택할 수 있으며, 혼합해서 사용할 수는 없습니다(그림 3 참조). 표 2에서 엔터프라이즈 모드와 컴플라이언스 모드의 차이점을 확인할 수 있습니다.

	엔터프라이즈 모드	컴플라이언스 모드
WORM 스토리지 인스턴스 생성	WORM 스토리지 인스턴스 생성 가능	WORM 스토리지 인스턴스 생성 가능
WORM 스토리지 인스턴스 삭제	변조 불가 데이터가 없으면 모든 관리자가 WORM 스토리지 인스턴스를 삭제할 수 있습니다. 단, 변조 불가 데이터가 있는 경우에는 오직 기본 관리자만 데이터를 삭제할 수 있습니다.	변조 불가 데이터가 없으면 모든 관리자가 WORM 스토리지 인스턴스를 삭제할 수 있습니다. 변조 불가 데이터가 있는 경우에는 WORM 스토리지 인스턴스를 삭제할 수 없습니다.
잠금 삭제	Flex Appliance MSDP 솔루션의 경우 아래 2단계를 수행하여 엔터프라이즈 잠금을 삭제할 수 있습니다. 1 스토리지 "보안 관리자"가 보관 기간 제거(기존 스토리지 관리자에게는 권한이 부여되지 않음) 2 NetBackup 관리자가 카탈로그를 통해 이미지 삭제 요청	해당 없음
보안 레벨 변경	엔터프라이즈 모드에서 정상 모드로 변경하려면 먼저 모든 WORM 스토리지 인스턴스를 삭제해야 합니다.	엔터프라이즈 모드 또는 정상 모드로 이동하려면 먼저 WORM 스토리지 인스턴스의 모든 데이터를 만료 처리한 후 해당 인스턴스를 삭제해야 합니다.

표 2: 엔터프라이즈 모드 vs. 컴플라이언스 모드

MSDP 변조 불가 스토리지 서버 생성 시 최소 및 최대 보관 기간을 묻는 메시지가 표시됩니다. 최소 보관 기간은 스토리지 장치에 WORM 파일을 보관할 수 있는 가장 짧은 기간을 의미합니다. 최대 보관 기간은 파일을 WORM에 커밋할 수 있도록 가장 길게 확보한 보관 기간을 말합니다(그림 4 참조). 보관 기간 구성은 CLI를 통해 변경할 수 있습니다.

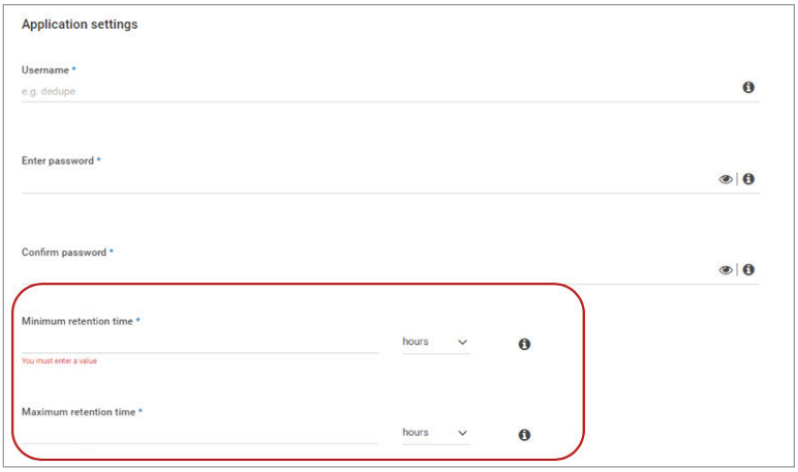

그림 4. MSDP 변조 불가 스토리지 서버 생성 시 최소 및 최대 보관 기간 설정

NetBackup과 Flex Appliance의 변조 불가 솔루션은 다음과 같이 Cohasset 변조 불가 평가를 제공합니다(컴플라이언스 모드).

- SEC(Securities and Exchange Commission) 17 CFR § 240 17a-4(f)
- FINRA(Financial Industry Regulatory Authority) Rule 4511(c)
- CFTC(Commodity Futures Trading Commission) 규정 17 CFR § 1 31(c)-(d)

변조 불가 스토리지 서버 보호

Flex Appliance는 어플라이언스 OS 및 MSDP 컨테이너에 대한 root 계정 액세스 권한을 제거하며, 오직 host admin 계정만 컴퓨팅 노드에 로그인할 수 있습니다. 계정 정책을 사용하여 승격된 사용자에게 셸 및 웹 UI 작업에 대한 특정 관리 명령 및 액세스를 허용할 수 있습니다.

아래 목록은 펌웨어 보안 하드닝에 대해 설명합니다.

- 부트
  - "single user" 모드/"rescue" 모드 부팅 옵션 제거
  - GRUB(GNU GRand Unified Bootloader) 메뉴 편집 비활성화
- 스토리지
  - 스토리지를 재설정하지 않음(공장 초기화/재이미징 허용)
  - 락다운(Lock down) 스토리지 어레이

OS 하드닝

Flex Appliance는 SELinux를 사용하여 플랫폼 및 호스팅 어플라이언스를 강화하고 변조 불가 스토리지에 대한 무단 액세스를 차단합니다. SELinux는 강제(enforcing) 및 허용(permissive)의 두 가지 모드를 제공합니다. Flex Appliance는 아래와 같이 SELinux를 강제(enforcing) 모드로 설정하여 정책 규칙을 설정합니다.

- root 사용자 계정 권한은 최소 권한에 가깝게 축소되며, 오직 hostadmin 계정만 컴퓨팅 노드에 로그인할 수 있습니다.
- Flex Appliance는 권한 상향 조정 시에도 IPS 활성화 상태를 유지하며, 승격된 사용자는 최대의 권한을 갖게 됩니다.
- 모든 Flex 셸 및 웹 UI 작업을 허용하는 정책
- 승격된 사용자에게 특정 추가 관리 명령을 허용하는 정책
- 플랫폼 인증서, 토큰, 로그, Compliance Clock(불변 기간 설정) 디바이스를 위한 파일 레이블 지정
- 스토리지에 대해 독점적인 액세스 권한을 사용하여 각 인스턴스 및 인프라스트럭처 서비스 제한
- 인스턴스에서 systemd 및 NFS 서비스를 실행하고 FUSE 디바이스에 액세스하며 NFS/CIFS 공유를 마운트할 수 있도록 허용하는 정책

STIG(SECURITY TECHNICAL IMPLEMENTATION GUIDE)

STIG(Security Technical Implementation Guide)는 전반적인 보안 향상을 위해 네트워크, 서버, 시스템, 논리적 설계 내에서 보안 프로토콜을 표준화하기 위한 사이버 보안 방법론입니다. Flex Appliance는 STIG 템플릿을 사용하여 DISA(Defense Information Systems Administration) 프로파일에 대한 보안 요건을 충족합니다.

Flex Appliance는 다음을 수행하여 STIG를 통한 OS 하드닝을 구현합니다.

- OS 명령 및 시스템 호출 등 하위 레벨 작업에 대해 감사 활성화
- Ctrl-Alt-Delete 재부팅 비활성화
- SSH root 로그인 비활성화
- hostadmin 계정에 대해 최대 10개의 동시 로그인 세션 허용
- 대화형/로그인 세션의 유휴 상태 타임아웃 10분
- 15분 내에 Flex Appliance 셸에서 연속 3회 잘못된 로그인 시도 시 15분간 계정 잠금
- 웹 UI 옵션으로 암호 정책 요건 적용(Appliance 노드별로 자동 적용)

FLEX APPLIANCE 멀티테넌트 아키텍처

Flex Appliance는 베리타스 애플리케이션에 대한 공통 플랫폼을 제공하여 NetBackup과 긴밀하게 통합하고 사용자 환경을 간소화합니다. 단일 Flex Appliance에서 여러 NetBackup과 CloudCatalyst 구축(도메인)을 통합할 수 있으므로 데이터 센터의 비용과 복잡성이 대폭 감소합니다(그림 5 참조).

Docker 컨테이너 소프트웨어는 Linux 기반 운영 체제인 VxOS(Veritas Optimized Operating System)에서 직접 실행됩니다. VxOS는 Flex Appliance 커널, 런타임 라이브러리, 컨테이너 엔진을 제공합니다. Flex Appliance는 컨테이너 격리 및 보안 기술을 사용하여 사용자가 단일 Appliance에서 서로 다른 NetBackup 인스턴스를 사용하는 경우에도 별도로 운영할 수 있게 지원합니다. NetBackup 서비스 사용자는 VxOS에 기본 제공된 커널 기능과 네트워크 및 데이터 분리를 활용하여 방화벽을 통해 서로 효과적으로 차단됩니다.이러한 멀티테넌트 아키텍처는 공통 플랫폼에서 여러 NetBackup 도메인을 실행하는 방식으로 NetBackup 환경을 간소화합니다.

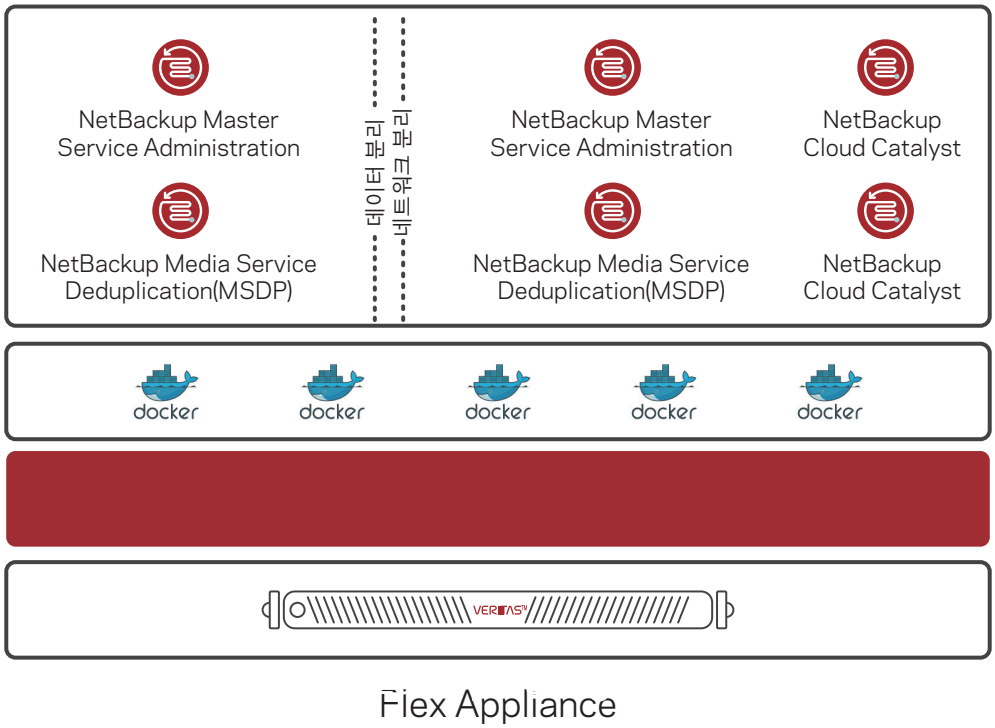

그림 5. 단일 Flex Appliance에서 여러 NetBackup 및 CloudCatalyst 구축(도메인) 통합

참조

- Flex Appliance 제품:
  https://sort veritas com/DocPortal/pdf/130821112-136840843-1
- NetBackup 제품 설명서:
  https://sort veritas com/documents/doc_details/nbu/8 2/Windows%20and%20UNIX/Documentation
- SELinux:
  https://www redhat com/en/topics/linux/what-is-selinux
- 관리자 가이드:
  https://access redhat com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index
- 컨테이너용 MCS:
  https://www redhat com/en/blog/why-you-should-be-using-multi-category-security-your-linux-containers
- 집중 코스:
  https://www slideshare net/ffri/mr201406-a-re-introduction-to-se-linux

VERITAS TECHNOLOGIES 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 500대 기업 중 87%를 포함한 5만개 이상의 전세계 기업이 베리타스 기술을 기반으로 IT 복잡성을 해결하고 데이터 관리를 간소화합니다. 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 데이터의 위치와 관계없이 데이터 보호를 자동화하고 복구를 조정함은 물론, 비즈니스 크리티컬 애플리케이션의 가용성을 항시 보장하고 기업이 데이터 규제 변화를 준수하는 데 필요한 인사이트를 제공합니다. 더불어 높은 신뢰성과 모든 요구사항을 충족하는 배포 모델을 제공하는 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 800개 이상의 데이터 소스와 100개 이상의 운영체제(OS), 1400개 이상의 스토리지 타깃, 60개 이상의 클라우드 플랫폼을 지원합니다. 보다 자세한 정보는 베리타스 홈페이지(www.veritas.com/kr) 또는 베리타스 트위터(@veritastechllc)에서 확인하실 수 있습니다.

Veritas Korea Ltd.
서울시 송파구 올림픽로 300 롯데월드타워 35층
Tel: 02 3468 2100 | www.veritas.com/kr

V1108 10/20