Vormetric | Enterprise Encryption and Key Management Simplified

DSM 5.x Host Settings Guide v0.1

2013 년 8 월 27 일

Vormetric Korea

1. 개요

1.1 인증과 권한

Unix 계열 시스템에서는 로컬 시스템 (/etc/passwd 및 /etc/group)과 LDAP 등의 인증 시스템을 사용하여 로그인하는 사용자에게 사용자 ID 를 부여하고, 실행되는 모든 프로세스는 자신을 실행한 사용자의 ID 권한에 허용된 파일만을 처리할 수 있습니다.

Vormetric Encryption 은 사용자의 권한을 기준으로 파일에 대한 액세스를 제어할 수 있고 관리자 계정도 통제할 수 있지만, 아래와 같은 두 가지 상황이 이러한 처리를 어렵게 만들 수 있습니다.

- 일반 사용자 ABC 가 su, sudo 명령을 통해 root 권한을 취득
- 특정 파일에 대해 ABC 에게 권한을 부여하고 root 도 액세스하지 못하도록 하고 싶지만 root 가 su 명령을 통해 ABC 로 ID 를 변경

본 문서에서는 사용자 ID 와 관련된 내부 구조를 이해하고 위와 같은 문제를 해결할 수 있는 방법을 설명합니다.

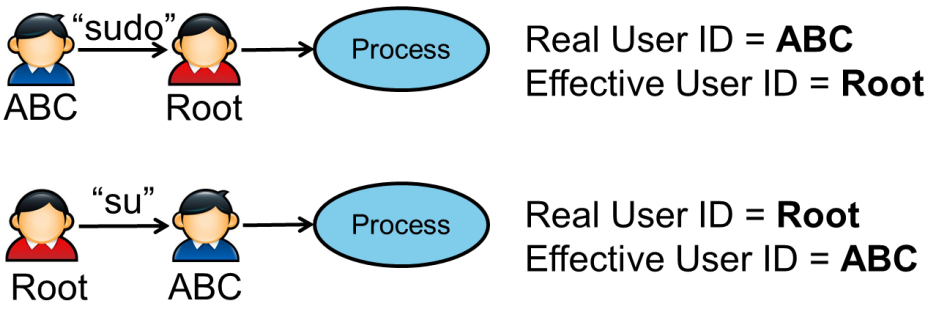
1.2 Real User ID 와 Effective User ID

Unix 계열 시스템에서 사용자 ABC 가 passwd 명령을 사용하면 root 만 변경할 수 있는 /etc/passwd 파일에서 사용자 ABC 의 암호만을 변경합니다. 이러한 작업이 가능한 이유는 Unix 시스템이 내부적으로 Real User ID 와 Effective User ID 라는 서로 다른 두 가지 사용자 ID 를 관리하고 있기 때문입니다.

- Real User ID: 로그인 시 사용한 계정의 ID
- Effective User ID: 액세스 권한을 결정하는 ID

위 passwd 명령의 경우 passwd 프로그램 내에서 Effective User ID 를 root 로 하기 때문에 /etc/passwd 파일을 수정할 수 있고, 프로그램에서 Real User ID 를 확인하기 때문에 명령을 실행한 사용자의 암호만을 변경할 수 있습니다.

1.1 에서 제시한 두 문제 상황의 경우 각각의 Real User ID 와 Effective User ID 는 아래 그림과 같습니다.



2. Host Settings 적용

2.1 적용 시나리오

사용자를 기준으로 파일에 대한 액세스를 통제하기 위해서는 정책에서 User Set 를 사용합니다. Vormetric Encryption 에서 사용자를 기준으로 통제가 필요한 주요 시나리오를 살펴보면 다음과 같습니다.

- authenticator: 로그인 절차를 통해 Real User ID 를 생성하는 프로세스에 적용하면 su, sudo 명령 등을 통해 ID 를 변경한 사용자가 원래 사용자 권한으로 액세스하는 것을 방지할 수 있습니다
  - 형식: |authenticator|/full/path/to/binary
  - 대상: login, sshd 에 적용
  - 주의: telnetd 는 다시 login 프로세스를 호출하므로 적용하지 않음
- authenticator_euid: 등록된 프로세스의 Effective User ID 및 그 자식 프로세스의 Effective User ID 를 신뢰
  - 형식: |authenticator_euid|/full/path/to/binary
  - 대상: ftpd, samba 에 적용
  - 주의: oracle 프로세스의 경우 setuid oracle 프로세스이므로 실행 사용자 UID 를 기준으로 통제하려면 authenticator 를 사용하고 사용자 UID 와 관계 없이 oracle 을 신뢰하기 위해서는 authenticator_euid 적용.

주) trust 및 trustfrom Tag 는 지원되지 않습니다.

2.2 Host Settings 설정

Host Settings 에 등록된 프로세스는 자동 서명되므로 다음과 같은 작업 후에는 Host Settings 을 반영시켜야 합니다.

- 에이전트 설치
- 에이전트 업그레이드
- Host Settings 탭 목록 변경

Host Settings 수정 후 수정 사항을 반영하기 위해서는 다음 작업이 필요합니다.

- 가능한 경우 설정이 반영될 호스트의 재시작 또는 Vormetric Service 재시작
- Vormetric Service 를 재시작 한 경우 Host Settings 탭에 설정된 프로세스를 재시작

2.3 User Not Authenticated 로그

사용자가 위에 예시한 인증 시스템을 통해 적절한 인증을 거치지 않을 경우 로그에 “User Not Authenticated”가 표시됩니다.

이 로그는 사용자 기반 인증을 사용하지 않고 있다는 표시이며 오류가 아닙니다.

끝.