

Secure OS 연동 가이드

작성일 : 2016. 8. 30

1. 호환성 문제

1.1. 개요

보메트릭 VTE 암호화 소프트웨어는 커널에서 실행되는 커널 모듈이며, Secure OS 제품 역시 커널에서 실행되는 모듈입니다. 커널 모듈의 경우 먼저 시작된 모듈 위에 나중에 시작된 모듈이 쌓이는 (Stacking) 구조이므로 두 모듈이 시스템에서 상주하는 경우 시스템 종료 시 문제를 유발할 수 있습니다. 한 모듈이 시작된 상태에서 다른 모듈이 실행되면 나중에 실행된 모듈이 종료되지 않는 한 먼저 실행된 모듈이 종료할 수 없는 문제가 발생합니다. 보메트릭 VTE 와 Secure OS 가 이러한 예에 해당합니다.

1.2. 호환성 문제 해결

실제 문제는 시스템 종료 시 발생합니다. VTE 는 물론 대부분의 Secure OS 제품이 자신의 커널 모듈을 정상적으로 unload 하는 기능을 제공하고 있기 때문에 모듈 종료 문제가 발생할 경우 수동으로 나중에 실행된 모듈을 종료하면 먼저 실행된 모듈도 종료할 수 있습니다. 하지만 시스템 종료의 경우 시스템에 정의된 순서에 따라 자동으로 모듈을 종료 시키는데, 이때 시스템에 정의된 종료 순서가 모듈 실행 순서와 맞지 않으면 시스템이 정상 종료할 수 없습니다.

이러한 문제를 해결하기 위해서는 두 제품의 시작 순서 및 종료 순서를 조정하여 먼저 시작된 모듈이 나중에 종료될 수 있도록 해야합니다.

2. 호환성 설정

2.1. Run-Level

보메트릭 VTE 와 Secure OS 제품들은 모두 시스템 시작 시 함께 시작되고 종료 시 종료됩니다. 일반적인 Unix/Linux 시스템의 경우에 다음과 같은 Run-Level 을 가지고 있으며 해당 Run-Level 별 폴더에 시작/종료 시킬 서비스에 대한 링크 파일을 가지고 있습니다. Run-Level 의 정의는 운영체제 별로 다릅니다. 아래는 System V 기준 정의입니다.

- Run Level 0: Shutdown
- Run Level 1: Single-user mode
- Run Level 2: Multi-user mode
- Run Level 3: Multi-user mode with Networking
- Run Level 4: Multi-user mode, user definable
- Run Level 5: System Halt
- Run Level 6: Reboot

운영체제 별 Run-level 정의와 Run-level 폴더는 여기서 설명하지 않습니다. 제품 별로 다양한 Run-level 에 시작 및 종료 스크립트를 링크 시키므로 **모든 Run-level 에 대해 먼저 시작된 모듈이 나중에 종료되도록 순서를 조정**해야 합니다.

2.2. 시작/종료 순서 조정

AIX 시스템의 경우 실제 스크립트의 위치는 /etc/rc.d/init.d 폴더에 위치하며, Run-level 폴더는 /etc/rc.d/rcx.d (x 는 0 ~ 6)입니다. 각 Run-level 폴더에 시작 스크립트와 종료 스크립트를 아래와 같이 생성할 수 있습니다.

시작 스크립트

```
# ln -s /etc/rc.d/init.d/rc.tivoli /etc/rc.d/rc2.d/S20tivoli
```

종료 스크립트

```
# ln -s /etc/rc.d/init.d/rc.tivoli /etc/rc.d/rc0.d/K20tivoli
```

각 Run-level 폴더 내 스크립트는 번호가 낮은 것부터 실행됩니다. 예를 들면, 종료 스크립트의 경우 K01 스크립트가 K02 스크립트보다 먼저 실행 (종료) 되고, 시작 스크립트의 경우 S01 스크립트가 S02 스크립트보다 먼저 실행 (종료) 됩니다.

3. 연동 테스트 결과

주요 Secure OS 제품에 대한 연동 결과는 다음과 같습니다. 모든 운영체제 상에서 테스트 한 결과는 아니므로 사전에 정상 연동 여부 테스트가 권장됩니다.

3.1. CA Control Minder (Access Control)

모듈 실행/종료 순서	자동/수동	결과	비고
VTE > CA / CA > VTE	자동	정상	
CA > VTE / VTE > CA	수동	정상	

3.2. Secuve TOS

모듈 실행/종료 순서	자동/수동	결과	비고
VTE > TOS / TOS > VTE	자동	정상	
TOS > VTE / VTE > TOS	수동	정상	

- 1) Secuve TOS 2.0 과 AIX 6.1 상에서 호환성 테스트 결과

3.3. SGA RedCastle

모듈 실행/종료 순서	자동/수동	결과	비고
VTE > RedCastle / RedCastle > VTE	자동	정상	
RedCastle > VTE / VTE > RedCastle	수동	정상	

- 1) RedCastle TOS 2.0 과 AIX 6.1 상에서 호환성 테스트 결과

Vormetric Korea