



Solaris Zone 암호화 가이드

Version 0.5 – 2015 년 1 월 22 일

Vormetric Korea

Copyright Vormetric, Inc. 2014. All rights reserved. For Vormetric Partners and Licensees.

Revision History

변경	작성자	날짜
Document released as version 0.5	Hyeonjun Kim	7/16/2014
5.2.1 Update – version 0.7	Hyeonjun Kim	1/22/2015

목차

1.	Solaris Zone 암호화 개요.....	4
2.	에이전트 설치 및 Guard Point 설정	5
2.1.	에이전트 설치.....	5
2.2.	Guard Point 설정	5
3.	Startup 및 Shutdown.....	6
3.1.	Startup.....	6
3.2.	Shutdown	6
4.	상태 확인.....	7

1. Solaris Zone 암호화 개요

본 문서는 Solaris 운영체제에서 구동되는 가상 서버 환경인 Zone 환경에서 암호화를 구축할 때 권장되는 약식 절차를 설명합니다.

Solaris Zone 시스템이 OS 자원을 공유하는 시스템이기 때문에, 암호화 이전에 다음과 같은 사항을 먼저 파악하여야 합니다.

- Zone 레이아웃 및 베이스 디렉토리
- Zone 유형: **Sparse Zone** 및 **Whole Root Zone** 만 지원됩니다. (Branded Zone 은 지원되지 않습니다.)
- 5.2.1 의 경우, Solaris 10 에서는 Sparse Zone 만 지원됩니다.

DSM 에는 원칙적으로 "Local Zone"이라는 개념이 구현되지 않았습니다. 따라서 다음과 같은 구조를 갖게됩니다.

- DSM 과 통신을 하는 프로세스인 vmd 는 Global Zone 에서만 실행됩니다.
- 관리 콘솔에는 Global Zone 호스트 만이 표시됩니다.
- Global Zone 과 Local Zone 사이에 종속성이 있습니다. 즉, Global Zone 없이는 Local Zone 이 존재할 수 없고, Global Zone 상에 에이전트가 실행되지 않고 Local Zone 상에 에이전트가 실행될 수 없습니다.

지원되는 Solaris 버전은 <https://support.vormetric.com> 사이트의 Compatibility 목록을 통해 확인하십시오.

2. 에이전트 설치 및 Guard Point 설정

2.1. 에이전트 설치

에이전트 설치 과정에서는 Global Zone 과 Local Zone.

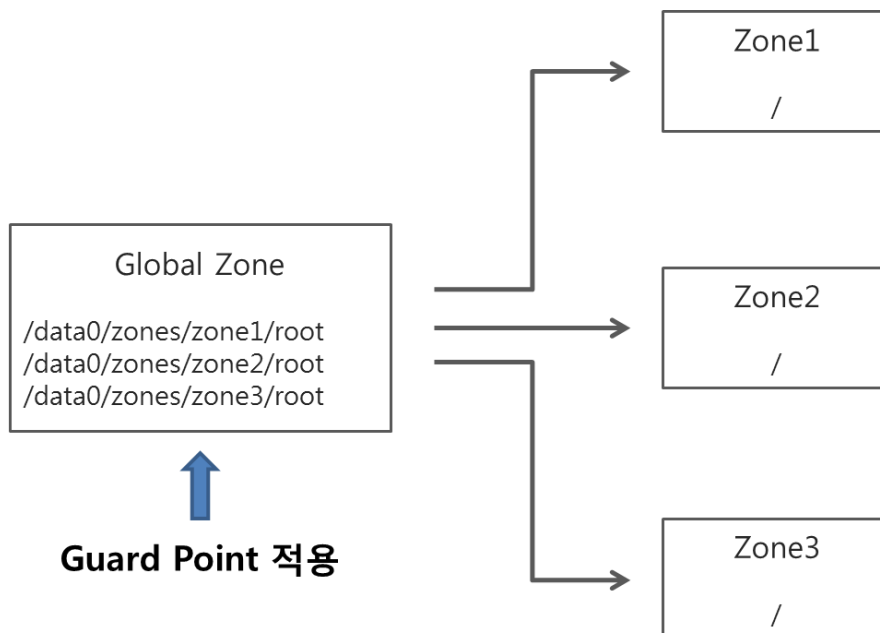
주요 과정은 다음과 같습니다.

- Global Zone 에 에이전트 설치 후 (Primary) DSM 에 레지스터
- 시스템 재부팅
- Local Zone 에 에이전트 설치 (시스템 재부팅 필요 없음)

2.2. Guard Point 설정

DSM 에는 원칙적으로 "Local Zone"이라는 개념이 구현되지 않았습니다. 모든 Guard Point 는 Global Zone 에서 설정합니다. Local Zone 은 Global Zone 에서 적용한 Guard Point 정보를 상속받습니다.

다음은 Global Zone 의 Guard Point 설정 경로 예를 보여줍니다. 그림의 Global Zone 경로에서 볼 수 있듯이 파일 시스템 경로를 통해 Local Zone 을 구분할 수 있습니다.



3. Startup 및 Shutdown

다음은 /etc/init.d 스크립트를 통한 에이전트 시작 및 종료 절차를 설명합니다. 에이전트의 Startup 및 Shutdown 은 Global Zone 및 Local Zone 모두에서 실행됩니다. 정상적으로 설치되었다면 시스템 시작 시 Global Zone 및 Local Zone 모두에서 에이전트가 자동적으로 시작됩니다.

3.1. Startup

다음은 Global Zone 및 Local Zone 에서 에이전트가 실행 중이 아닐 경우 Startup 의 상관 관계 및 종속성입니다.

- Global Zone 의 에이전트를 먼저 시작한 후 Local Zone 에이전트를 실행합니다.
- Global Zone 의 에이전트를 시작해도 Local Zone 에이전트가 자동으로 시작되지 않습니다.
- Global Zone 의 에이전트가 시작되지 않은 상태에서 Local Zone 에이전트를 시작하면 에이전트가 시작되지 않습니다. (시작 실패)
- Local Zone 에서는 secfsd 만 실행됩니다.

3.2. Shutdown

- Global Zone 의 에이전트를 종료하면 Local Zone 에이전트를 종료시킨 후 이어 Global Zone 의 에이전트를 종료시킵니다.
- Local Zone 에이전트를 종료시키면 해당 Zone 의 에이전트만이 종료됩니다.
- Local Zone 의 시스템 재시작은 해당 Zone 의 에이전트 만을 종료 후 재시작 시킵니다.

4. 상태 확인

Zone 환경에서 Vormetric 프로세스는 다음과 같이 실행됩니다.

- vmd 는 Global Zone 에서만 실행됩니다. Local Zone 에 vmd 프로세스가 실행되지 않는 것은 정상입니다.
- Global Zone 에서 secfsd 프로세스를 확인하면 모든 Local Zone 의 프로세스도 함께 표시되고, Local Zone 에서는 해당 Zone 과 Global Zone 의 secfsd 두 개가 표시됩니다. Global Zone 에서 실행되는 secfsd 를 구분하는 방법은 프로세스 ID 뿐입니다.

예) 아래의 경우 Zone1 과 Global Zone 모두에 표시되는 29487 이 Global Zone 의 secfsd 입니다:

Zone1

```
root 29487 3937 0 Sep 04 ? 0:01 /opt/vormetric/DataSecurityExpert/agent/ secfs/.sec/current/bin/secfsd
root 29488 3937 0 Sep 04 ? 0:36 /opt/vormetric/DataSecurityExpert/agent/ secfs/.sec/current/bin/secfsd
```

Global Zone

```
root 29487 1 0 Sep 04 ? 0:01 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 26698 1 0 Sep 04 ? 0:15 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 26696 1 0 Sep 04 ? 0:00 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 29422 1 0 Sep 04 ? 0:15 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 29421 1 0 Sep 04 ? 0:01 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 29296 1 0 Sep 04 ? 0:01 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
root 29488 1 0 Sep 04 ? 0:36 /opt/vormetric/ DataSecurityExpert/agent/secfs/.sec/current/bin/secfsd
```