VSD 기능 사양서

작성 :2004-08-03

수정 : 2004-10-11

목차

1. VSD와 문서보안과의 연동

1) VSD 로그 인은 문서보안 로그인과 연동: 문서보안 서버에 로그인 되면 자동으로 VSD 로그 인이 이루어지고, Disk Mount, VSD Agent 동작 등이 이루어 진다.

2) VSD Agent는 SDSMan으로부터 사용자 ID, VSD 사용 권한, VSD 설정 정보 등을 받아온다.

3) 문서보안 콘솔과 서버, DB 등에는 VSD 관련된 관리를 위한 기능 및 정의가 추가 된다.

※ 문서보안 제품과 연동 버전과 비 연동 버전의 구분을 어떻게 할것인지?

2. 사내 사용자 VSD Mount/Unmount

1) VSD는 사용자의 선택에 따라 Unmount 가 가능하다. 단, Unmount는 기존 지정 APP와 보안 탐색기를 모두 종료(또는 file close?) 한 후에만 가능하다.

2) Unmount 시에는 모든 APP의 VSD에 대한 접근을 막고, 지정 APP도 VSD 밖에 저장이 가능하다.

3. 사내 사용자 VSD내의 문서 작업 시 처리

1) VSD 내에 저장되는 문서(문서보안 대상 file)는 모두 문서보안 대상 file이라 가정한다. (PDM down 시 한꺼번에 down 받는 경우로 가정)

2) VSD 안에 문서 저장 시는 VSD Driver에 의한 암호화만 수행 하며, 문서보안 암호화는 수행하지 않는다.

3) VSD내의 문서는 VSD 밖으로 꺼내서(꺼낼 때 범주로 자동 암호화함) open하는 것을 원칙으로 한다.

4) 불가피한 경우 VSD내에서 open을 허용하고, 문서 open 시 VSD 밖에 임시 보안 file을 (사전에 정의된 범주로 암호화함) 생성하여 open하고, close 시 다시 VSD 안에 저장한다. 단, 이 때 open된 file의 정보를 관리하고, 보안탐색기가 이를 참조하여 중복 open 등의 문제를 해결한다.

4. 사내 사용자 CAD 작업 제어

1) VSD가 Mount된 이후에는 CAD 작업 시에는 VSD에만 저장가능하고, Unmount 시에는 다른 곳에의 저장도 가능하다. 단, Unmount 시에는 PDM 등에의 접근을 불허하고, 이것이 불가능할 경우에는 Unmount 기능을 사용할 수 없도록 한다.

2) VSD 내에서는 User 단위로 권한 제어를 수행한다. 즉, Read 여부, Write 여부, Print 가능 여부, Print Marking 여부, 유효기간(유효기간 경과 후 VSD 삭제 등의 조치 필요), 반출입 권한 등을 User 단위로 제어한다.

3) VSD 접근 가능 APP 의 통신은 특정 IP와 포트만을(PDM 서버 등) 콘솔에서 지정하여 허용한다.(추후 지원)

4) VSD 접근 가능 APP에서의 Copy & Paste 는 VSD 접근 가능 APP로만 한정된다.

5. VSD내 file 사내 전달 프로세스

1) 문서의 경우 범주로 자동암호화 후 전달한다(단, 다수파일 동시 선택시에는 CAD전달 방식을 따름).

2) CAD file의 경우 여러 개의 file을 암호화하여 Packing 한 후 전달한다. 이 때 사용되는 키는 문서보안의 그룹 키나 범주 키의 개념을 이용하여 해당 사용자들만이 풀어서 자신의 VSD에 저장하여 볼 수 있도록 한다.

6. VSD내 file 사외 반출 프로세스

1) 문서의 경우 SOM으로 만들어 전달한다.(단, 다수파일 동시 선택시에는 CAD전달 방식을 따름)

2) CAD file의 경우에는 VSD내의 사내 전달 프로세스와 기본 방법은 동일하다. 단, 범주나 그룹이 의미가 없으므로, 사외에서 해당 file을 받을 사람의 VSD 정보를 가져다 이를 이용하여 그 사람의 VSD에만 저장되도록 암호화하여 Packing 한 후 전달한다.

3) 2)가 가능하기 위해서는 외부 사용자는 VSD 설치 시 설치 프로그램이 자동으로 해당

VSD의 고유 정보를 사내로 전달 가능한 형태로 만드는 기능이 필요하고, 사내 사용자는 외부 전달 전에 이 정보 file이 있어야만 외부 전달이 가능하다.

4) 외부 전달용 packing 시에는 Read 여부, Write 여부, Print 가능 여부, Print Marking 여부, 유효기간(유효기간 경과 후 VSD 삭제 등의 조치 필요), 사내 회수 방법(회수자 정보 등?) 등이 포함되어 Packing 되어야 한다.

5) 이렇게 전달된 file은 보안탐색기를 통하여 사외 사용자의 VSD 내에 자동으로 Directory를 생성하고 그 안에 file이 저장되고, 이 안에서만 모든 작업이 이루어져야 한다. 따라서, 이 Directory의 file을 Open한 경우에는 다른 곳(VSD 밖 또는 VSD내의 다른 Directory) 에는 저장이 불가능하여야 한다. 즉, 이 Directory 밖으로 유출되는 것을 차단하여야 한다. 작업이 끝난 후에는 VSD를 Unmount 하면 제약없이 다른 CAD 작업이 가능하다.

6) 보안탐색기는 실행될 때마다 유효기간이 경과된 Directory가 있는지 확인하여 삭제하는 기능이 포함된다. (사내로 다시 회수 되어야 하는 경우에는 미리 경고하는 기능이 필요할 수도?)

7. 반출된 file의 사내 회수 프로세스

1) 반출된 file 또는 작업 완료된 file은 사외 사용자 VSD 내에 특정 Directory 내에서 관리된다. 따라서 사외 사용자는 이 해당 Directory 내의 모든 file을 보안 탐색기의 반납 기능을 이용하여 사내 회수용 file로 Packing한다. (이미 사내 회수 위치 등의 방법은 반출 시 그 정보가 포함되어 전달되므로 사용자의 선택이 필요없다.)

2) 사내 회수용 file이 만들어진 후에는 정책에 따라 Directory를 삭제한다. (삭제 여부는 반출 시에 결정)

3) 사내 회수용 file은 반출 시와 마찬가지로 자동 또는 수동으로 사내로 전달되고, 지정된 곳에서만 풀어 볼 수 있다.

8. 보안 탐색기의 프로세스 ID 등록

1) 다른 APP를 보안 탐색기로 가장하는 것을 막기 위하여 보안 탐색기는 기동 시 VSD Agent 에 process ID를 등록 한다.

2) 다른 APP는 프로세스 이름으로 제어한다. (단, 이는 다른 APP의 VSD 외부로의 저장 가능성이 없다는 가정하에 가능한 것임)

9. VSD 사용 환경

1) 운영체제

- Microsoft Windows 2000 Pro
- Microsoft Windows XP HOME, Pro
- Windows 9x계열(95, 98, ME)은 지원하지 않음.

2) 파일 시스템

- NTFS : 보안영역의 크기를 디스크의 최대 용량까지 생성 가능함
  Sparse File지원
- FAT32: 보안영역의 최대 크기를 4Gbyte이하로 제한함(파일시스템의 한계)
  Sparse File 지원하지 않음

※ Sparse File이란?

NTFS에서 지원하는 파일 형식으로 대용량의 파일을 생성하면 파일 시스템에서 인식하는 파일의 크기는 대용량으로 나타 나지만 실제 파일이 디스크 상에서 차지 하는 공간은 실제 데이터가 기록된 만큼만 소모되는 신개념의 파일 형식

2) 하드웨어

- HDD : 500MByte이상의 여유 공간
- RAM : 해당 운영체제의 권장 사양 이상
- CPU : 해당 운영체제의 권장 사양 이상

10. VSD 지원 프로그램

1) 캐드 프로그램(지원 예정 : 목록에 없더라도 필요 시 테스트 후 추가 가능)

- AutoCAD
- Pro-E
- OrCAD
- SolidWorks
- I-DEAS

2) 개발도구(향후 지원 : 일정 미정)

- Visual Studio
- C++ Builder
- Delpahi

11. VSD의 동작 원리

1) VSD란?

일반적으로 많이 쓰이는 'CDSpace'나 'Alcohol 120%'와 같은 가상 CD프로그램과 비슷한방식으로 물리적인 디스크내부에 대용량의 Image파일을 생성하여 이를 운영체제에 드라이브로 등록하여 사용하는 방식으로 Image파일에 대한 제어를 우리 프로그램이 담당하므로 인증을 통과하지 못하면 Image파일을 드라이브로 등록하지 못하며, Image파일이 암호화 되어 있으므로 우리 프로그램을 사용하지 않으면 강제로 드라이브로 마운트 시킨다 하더라도 포맷되지 않은 디스크로 마운트 되어 전혀 Image파일 내부의 파일이 유출될 염려가 없다.

2) 동작 원리

VSD프로그램이 실행되어 인증을 통과 하면 Image을 드라이브로 마운트 시키며, 해당 Image에 대한 암호화 키를 전달하여 Image파일내의 데이터를 정상적으로 복호화 할 수 있게 한다. Image파일에 대한 암호화는 Filesystem layer수행하는 File단위 암호화가 아닌 Physical layer에서 Sector단위로 암호화 하는 방식으로 기존의 암호화 방식이 가지는 암호화 파일의 손상 등에서 자유롭다(단, image파일의 손상은 제외).

VSD프로그램이 허용하는 프로그램만 VSD드라이브에 접근이 가능하며, 특히 '윈도우 탐색기'는 보안드라이브에 접근 허용 시 보안의 홀이 너무 많아 접근을 완전히 차단하고 보안드라이브에 접근할 수 있는 '보안탐색기'를 별도로 제공하여 파일에 대한 처리를 하도록 했으며, CAD 프로그램들을 등록하여 이 프로그램들은 보안드라이브에 접근이 가능한 반면, 일반 드라이브에는 파일을 생성할 수 없도록 하여 보안드라이브의 정보가 새어 나가지 않도록 하였다(VSD 마운트 해제 시 일반드라이브에도 파일 저장 가능).