CA Access Control Premium Edition

문제 해결 안내서

12.6.02

타사 고지 사항

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

샘플 스크립트와 샘플 SDK 코드

CA Access Control 제품에 포함된 샘플 스크립트와 샘플 SDK 코드는 정보 제공 목적으로만 "있는 그대로" 제공됩니다. 이 항목은 특정 환경에 맞게 수정이 필요할 수 있으며, 프로덕션 환경에 사용하려면 프로덕션 시스템에 배포하기 전에 반드시 테스트 및 검사를 수행해야 합니다.

CA Technologies 는 이러한 샘플에 대한 지원을 제공하지 않으며 이 스크립트로 인한 어떠한 오류에도 책임을 지지 않습니다.

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On(CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA NSM(CA Network and Systems Management, 이전의 Unicenter NSM 및 Unicenter TNG)
- CA Software Delivery(이전의 Unicenter Software Delivery)
- CA Service Desk(이전 이름: Unicenter Service Desk)
- CA User Activity Reporting Module (이전 명칭: CA Enterprise Log Manager)
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

형식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	강조 또는 새 용어
굵게	표시된 대로 동일하게 입력해야 하는 텍스트
슬래시(/)	UNIX 및 Windows 경로를 기술하는 데 사용되는 플랫폼 독립적인 디렉터리 구분 기호

이 설명서는 또한 명령 구문과 사용자 입력(고정 폭 글꼴로 표시됨)을 설명할 때 다음과 같은 특별한 규칙을 사용합니다.

형식	의미
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 *또는* 그룹 이름 중 *하나*라는 의미입니다. {*username*|*groupname*}
…	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.

- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 *all* 을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

- *ACInstallDir* - 기본 CA Access Control 설치 디렉터리입니다.
  - Windows - C:\Program Files\CA\AccessControl\
  - UNIX - /opt/CA/AccessControl/
- *ACSharedDir* - UNIX 에서 CA Access Control 에 의해 사용되는 기본 디렉터리입니다.
  - UNIX - /opt/CA/AccessControlShared
- *ACServerInstallDir* - 기본 CA Access Control 엔터프라이즈 관리 설치 디렉터리입니다.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* - 기본 배포 서버 설치 디렉터리입니다.
  - /opt/CA/DistributionServer
- *JBoss_HOME* - 기본 JBoss 설치 디렉터리입니다.
  - /opt/jboss-4.2.3.GA

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- CA Access Control 끝점 및 서버 구성 요소 설치 - 다음 변경 내용으로 업데이트되었습니다.
  - CA Access Control 로 업그레이드할 때 라이선스 오류가 발생

목차

제 1 장: 소개

이 섹션은 다음 항목을 포함하고 있습니다.

안내서 정보

이 안내서는 CA Access Control Premium Edition 에서 발생할 수 있는 일부 공통적인 문제점에 대한 해결 방법을 설명합니다.

용어를 간단히 나타내기 위해 이 안내서에서는 제품을 CA Access Control 이라고 합니다.

본 안내서의 사용자

이 안내서는 CA Access Control-보호 환경을 구현, 구성, 유지 관리할 때 문제를 겪을 수 있는 보안 관리자와 시스템 관리자를 대상으로 합니다.

제 2 장: CA Access Control 끝점 및 서버 구성 요소 설치

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control 엔터프라이즈 관리 설치 중 "잘못된 인터프리터" 메시지가 표시됨

UNIX 및 Linux 에 적용됨

증상

CA Access Control 엔터프라이즈 관리를 설치하려고 하면 다음 오류 메시지가 표시됩니다:

```
/bin/sh: 잘못된 인터프리터: 사용 권한이 거부되었습니다.
```

해결 방법

일부 UNIX 또는 Linux 릴리스에서 운영 체제는 noexec 옵션을 사용하여 광학 디스크 드라이브를 자동으로 마운트합니다. CA Access Control 엔터프라이즈 관리를 설치하려면 noexec 옵션을 사용하여 광학 디스크 드라이브가 마운트되지 않도록 하십시오.

CA Access Control 엔터프라이즈 관리 데이터베이스 암호에 '$' 문자를 사용할 수 없음

증상

CA Access Control 엔터프라이즈 관리를 설치할 때 데이터베이스 암호를 입력하면 "데이터베이스 버전을 확인할 수 없습니다"란 오류 메시지가 표시됩니다.

해결 방법

암호 끝에 '$' 문자를 입력하면 CA Access Control 엔터프라이즈 관리 설치 중 이 오류 메시지가 표시됩니다. 암호 뒤에 '$' 문자를 반드시 넣어야 하는 경우에는 설치 후 데이터베이스 암호를 변경해야 합니다.

CA Access Control 서버 구성 요소를 열 수 없음

증상:

모든 필수 CA Access Control 서비스를 시작한 이후에 웹 브라우저에서 CA Access Control 엔터프라이즈 관리, CA Access Control 끝점 관리, CA Access Control 암호 관리자를 열 수 없습니다. JBoss 와 Oracle 은 동일한 서버에 설치되어 있습니다.

해결책:

Oracle 과 JBoss 가 모두 기본 포트 8080 을 사용합니다. 이 문제를 해결하려면 Oracle 과 JBoss 사이의 포트 충돌을 해결해야 합니다. Oracle 또는 JBoss 포트를 변경하기 전에 회사에서 어떤 포트를 변경하는 것이 더 쉬운지 고려해야 합니다.

다음 절차에 따라 기본 JBoss 및 Oracle 포트를 변경하십시오.

기본 JBoss 포트를 변경하려면

1. 명령 창을 연 다음 디렉터리로 이동합니다. *JBossInstallDir* 는 JBoss 가 설치된 디렉터리입니다.

   *JBossInstallDir/*bin

2. JBoss 를 중지합니다.

   - (Windows) shutdown.bat -S
   - (UNIX) shutdown.sh -S

3. 텍스트 편집기에서 다음 파일을 엽니다.

   *JBossInstallDir/*server/default/deploy/jbossweb-tomcat55.sar/server.xml

4. 다음 섹션에서 포트 번호를 변경합니다.

   ```
   <!-- A HTTP/1.1 Connector on port 8080 -->
       <Connector port="8080" address="${jboss.bind.address}"
   ```

5. 파일을 저장한 후 닫습니다.

6. 텍스트 편집기에서 다음 파일을 엽니다.

   *JBossInstallDir/*server/default/deploy/httpha-invoker.sar/META-INF/jboss-service.xml

7. 다음 줄 각각에서 포트 번호를 변경합니다.

```
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerHAServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/readonly/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerHAServlet</attribute>
```

8. 파일을 저장한 후 닫습니다.
9. JBoss 를 시작합니다.
10. (Windows) 다음과 같이 CA Access Control 엔터프라이즈 관리, CA Access Control 끝점 관리, CA Access Control 암호 관리자 바로 가기를 변경합니다.
    a. "시작", "프로그램", "CA", "Access Control"을 클릭한 다음 적절한 바로 가기를 마우스 오른쪽 단추로 클릭합니다.

       예를 들어, CA Access Control 엔터프라이즈 관리 바로 가기를 변경하려면 "시작", "프로그램", "CA", "Access Control"을 클릭한 다음 "엔터프라이즈 관리"를 마우스 오른쪽 단추로 클릭합니다.
    b. "속성"을 클릭합니다.
    c. URL 필드에서 포트 번호를 새 JBoss 포트 번호로 변경합니다.

기본 Oracle 포트를 변경하려면

1. SQL 명령줄을 시작합니다.
2. sysdba 로 Oracle 에 연결합니다.

```
connect / as sysdba
```

3. HTTP 통신에 현재 사용되는 포트를 확인합니다.

```
select dbms_xdb.gethttpport from dual;
```

4. 원하는 포트 번호를 설정합니다.

```
exec dbms_xdb.sethttpport('portNumber');
```

5. 데이터베이스를 중지한 후 다시 시작합니다.

```
shutdown immediate
```

시작

CA Access Control 엔터프라이즈 관리에서 탭이 표시되지 않음

Active Directory 사용자 저장소에 해당

증상

CA Access Control 엔터프라이즈 관리를 성공적으로 설치했습니다. 설치 중 지정한 시스템 사용자로 로그인하면 인터페이스에 탭이 표시되지 않습니다.

해결 방법

CA Access Control 엔터프라이즈 관리를 설치할 때 다음과 같은 Active Directory 매개 변수를 제공합니다.

- 호스트
- 포트
- 검색 루트
- 사용자 DN(및 이 사용자의 암호)
- 시스템 사용자

이 문제는 Active Directory 검색 루트가 디렉터리 트리에서 사용자 DN 및 시스템 사용자에 대한 DN(고유 이름)과 동일한 노드에 있을 때 발생합니다. 이 문제를 해결하려면 디렉터리 트리에서 지정된 사용자 DN 및 시스템 사용자에 대한 DN 보다 노드가 하나 이상 더 높게 검색 루트를 지정하십시오.

예: Active Directory 검색 루트

이 예는 사용자 DN 및 시스템 사용자에 대해 다음 DN 을 사용합니다.

- 사용자 DN: CN=MyQueryUser,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
- 시스템 사용자: CN=MySystemManager,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB

다음 검색 루트는 디렉터리 트리에서 사용자 DN 및 시스템 사용자에 대한 DN 보다 한 노드 위에 있습니다. 다음 검색 루트를 지정하면 CA Access Control 엔터프라이즈 관리가 성공적으로 설치되고 인터페이스에 탭이 표시됩니다.

```
OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

다음 검색 루트는 디렉터리 트리에서 사용자 DN 및 시스템 사용자에 대한 DN 과 동일한 노드에 있습니다. 다음 검색 루트를 지정하면 CA Access Control 엔터프라이즈 관리가 성공적으로 설치되지만 인터페이스에 탭이 표시되지 않습니다.

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

예: Active Directory 검색 루트를 디렉터리 트리에서 한 노드 위에 설정

이 예는 이전 예와 동일한 사용자 DN 및 시스템 사용자에 대한 DN 을 사용합니다.

이 예에서 CA Access Control 엔터프라이즈 관리를 설치할 때 다음 검색 루트를 지정했습니다.

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

이 검색 루트가 디렉터리 트리에서 사용자 DN 및 시스템 사용자에 대한 DN 과 동일한 노드에 있으므로 검색 루트를 디렉터리 트리에서 한 노드 위에 지정해야 합니다.

Active Directory 검색 루트를 디렉터리 트리에서 한 노드 위에 설정하려면

1. CA Identity Manager 관리 콘솔을 활성화합니다.
2. CA Identity Manager 관리 콘솔을 엽니다.
3. "디렉터리"를 클릭하고 ac-dir 디렉터리를 클릭합니다.

   "디렉터리 속성" 대화 상자가 나타납니다.
4. "디렉터리 속성" 대화 상자의 맨 아래에서 "내보내기"를 클릭합니다.
5. 요청되는 경우 XML 파일을 저장하고 편집을 위해 엽니다.

   참고: 파일 이름은 ac-dir.xml 입니다.
6. 설치 중 지정한 검색 루트를 포함하는 태그를 찾습니다. 예:

   ```
   <LDAP searchroot="OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB"
   secure="false"/>
   ```
7. 기존 검색 루트를 새 검색 루트로 대체합니다. 예:

   ```
   <LDAP searchroot="OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
   ```

   참고: 엔터프라이즈 OU(조직 단위)를 제거했으므로 이 검색 루트는 디렉터리 트리에서 이전 검색 루트보다 한 노드 위에 있습니다.
8. 파일을 저장한 후 닫습니다.

9. CA Identity Manager 관리 콘솔의 "디렉터리 속성" 대화 상자에서 "업데이트"를 클릭합니다.

   "디렉터리 업데이트" 페이지가 나타납니다.

10. "파일 선택"을 클릭하고 편집한 XML 파일로 이동하여 "열기"를 클릭한 다음 "마침"을 클릭합니다.

    CA Identity Manager 관리 콘솔이 XML 파일의 유효성을 검사하고 "디렉터리 구성 출력" 필드에 상태 정보를 표시합니다.

    참고: "가져오지 못했습니다" 오류가 표시되는 경우 "ac-dir.xml 디렉터리 구성 파일을 가져올 수 없음" 절을 참조하십시오.

11. [계속]을 누릅니다.

    "디렉터리" 페이지가 나타납니다.

12. "ac-dir"을 클릭하고 "환경" 섹션에서 "ac-env"를 클릭합니다.

    "환경 속성" 페이지가 나타납니다.

13. "다시 시작"을 클릭합니다.

    CA Identity Manager 관리 콘솔이 환경을 다시 시작하고 변경 내용을 적용합니다.

참고: CA Identity Manager 관리 콘솔을 활성화하고 시작하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

추가 정보:

ac-dir.xml 디렉터리 구성 파일을 가져올 수 없음 (페이지 22)

ac-dir.xml 디렉터리 구성 파일을 가져올 수 없음

증상

CA Identity Manager 관리 콘솔에서 ac-dir.xml 디렉터리 구성 파일을 가져왔습니다. 이 파일을 가져오려고 시도하면 "디렉터리 구성 출력" 필드에 다음과 같은 오류 메시지가 표시됩니다.

```
디렉터리 구성을 배포하는 중...

입력 스트림을 구문 분석하는 중...
오류: (140:67): cvc-complex-type.4: 특성 "value"가 요소 "Container"에 있어야 합니다.
오류: 가져오지 못했습니다.

*********
1 개 오류, 0 개 경고
```

해결 방법

ac-dir.xml 디렉터리 구성 파일은 사용자 저장소의 구조 및 콘텐츠를 기술합니다. 이 파일을 사용하면 CA Access Control 엔터프라이즈 관리가 사용자 저장소와 상호 작용하는 방식을 변경할 수 있습니다. 예를 들어, 사용자 디렉터리 암호 또는 Active Directory 검색 루트를 변경하는 데 사용할 수 있습니다. 또한 SSL 통신을 위해 CA Access Control 엔터프라이즈 관리를 구성하고 장애 조치를 위해 Active Directory 를 구성할 때 ac-dir.xml 파일을 편집합니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. 편집을 위해 ac-dir.xml 파일을 엽니다.
2. 다음 태그를 찾습니다.

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou"/>
   ```

3. 이전 태그를 다음 태그로 대체합니다.

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

4. 파일을 저장한 후 닫습니다.

이제 CA Identity Manager 관리 콘솔로 디렉터리 구성 파일을 가져올 수 있습니다. 디렉터리 구성 파일에 대한 변경 내용을 적용하려면 파일을 가져온 이후에 환경을 다시 시작해야 합니다.

CA Access Control 엔터프라이즈 관리 DMS 에 연결할 수 없음

증상

CA Access Control 엔터프라이즈 관리에 로그인할 때 다음과 유사한 메시지가 표시됩니다.

```
오류: 로그인 절차에 실패했습니다.
오류: 대상의 암호가 클라이언트의 암호와 일치하지 않습니다.
```

해결 방법

사용자 ac_entm_pers 가 DMS 에 로그인할 수 없습니다. 이 사용자는 엔터프라이즈 관리 서버와 DMS 사이에서 통신 및 데이터 흐름을 인증합니다.

참고: ac_entm_pers 사용자는 다음과 같은 인증 특성을 갖습니다: ADMIN, AUDITOR, IGN_HOL, LOGICAL

이 문제를 해결하려면 다음을 수행하십시오.

1. selang 을 엽니다.
2. DMS 에 연결합니다:

   ```
   host DMS__@entM_host_name
   ```

3. ac_entm_pers 에 대한 암호를 변경합니다:

   ```
   eu ac_entm_pers password(password) nonative grace-
   ```

4. 엔터프라이즈 서버가 설치된 호스트에 ac_entm_pers 가 로그인하도록 허용합니다:

   ```
   authorize TERMINAL entM_host_name uid(ac_entm_pers) access(a)
   ```

5. ac_entm_pers 가 엔터프라이즈 관리 서버에 로그인할 수 있도록 허용합니다:

   ```
   host DMS_@entM_host_name uid(ac_entm_pers) password(password) logical
   ```

6. 엔터프라이즈 관리 서버 DMS 연결 설정을 ac_entm_pers 에 대한 새 암호로 업데이트합니다.

   DMS 는 ac_entm_pers 를 인증하고 CA Access Control 엔터프라이즈 관리가 DMS 에 연결됩니다.

   참고: DMS 에 대한 연결을 구성하는 방법에 대한 자세한 내용은 *CA Access Control 엔터프라이즈 관리 온라인 도움말*을 참조하십시오.

연결 설정을 업데이트할 때 오류가 발생하면 DMS 는 ac_entm_pers 를 인증할 수 없습니다. 이 문제를 해결하려면 다음을 수행하십시오.

1. 이전 절차의 각 단계에서 동일한 암호를 입력했는지 확인합니다.
2. 이전 절차의 4 단계에서 엔터프라이즈 관리 서버의 호스트 이름(*entM_host_name*)이 올바른지 확인합니다.

   예를 들어, 4 단계에서 엔터프라이즈 관리 서버의 정규화된 호스트 이름을 지정했지만 엔터프라이즈 관리 서버의 TERMINAL 레코드가 간략한 호스트 이름을 사용하는 경우, 호스트 이름이 확인되지 않고 ac_entm_pers 가 엔터프라이즈 관리 서버에 로그인할 수 없습니다.
3. CA Access Control 감사 파일을 검토합니다:

   ```
   seaudit -a
   ```
4. DMS 감사 파일을 검토합니다:

   ```
   seaudit -a -fn DMS_log_file
   ```

   참고: 감사 레코드에 엔터프라이즈 관리 서버에 대한 TERMINAL 레코드의 올바른 호스트 이름에 대한 정보가 수록되어 있을 수 있습니다.

예: DMS 감사 파일 표시

다음 예는 DMS__란 이름의 DMS 에 대한 감사 파일을 표시합니다:

```
seaudit -a -fn "C:\Program
Files\CA\AccessControlServer\APMS\AccessControl\Data\DMS__\pmd.audit"
```

CA Access Control 엔터프라이즈 관리 탭에 물음표가 표시됨

증상

CA Access Control 엔터프라이즈 관리를 열면 탭에 물음표가 표시됩니다.

해결 방법

이 문제를 해결하려면 브라우저의 기본 언어를 미국 영어로 변경하십시오.

InfoView 에서 "Null page" 오류 수신

증상

CA Access Control 보고서에 액세스하려고 시도하면 InfoView 에서 다음 오류가 발생합니다.

```
Null page: Unable to create page from report source(널 페이지: 보고서 소스에서 페이지를 작성할 수 없음)
```

해결 방법

Windows 의 경우 CA Access Control Universe 가 정의되지 않았거나 제대로 설치되지 않았을 수 있습니다. CA Access Control Universe 에 대한 연결을 테스트하십시오. 연결되지 않으면 연결을 편집하고, 연결이 되면 연결을 대체하십시오.

Solaris 에서 bouser 로 로그인하여 다음과 같이 $CASHCOMP/CommonReporting/bobje/setup/env.sh 스크립트를 편집하십시오.

1. 다음 LIBRARYPATH 를 추가합니다.

   ```
   $MWHOME/lib-sunos5_optimized
   ```

2. BusinessObjects 서비스를 다시 시작합니다.

   ```
   cd $CASHCOMP/CommonReporting/bobje
   ./stopservers
   ./startservers
   ```

CA Access Control 이 UNIX 설치 후 자동으로 시작되지 않음

UNIX 에 해당

증상:

UNIX 끝점에 설치 후 CA Access Control 이 자동으로 시작되지 않습니다.

해결책:

기본적으로 CA Access Control 은 UNIX 끝점에서 자동으로 시작되지 않습니다.

UNIX 컴퓨터가 시작될 때 seosd 데몬이 자동으로 시작하도록 구성하려면 *ACInstallDir*/samples/system.init/*sub-dir* 디렉터리를 사용하십시오. 여기서 *sub-dir* 는 운영 체제의 디렉터리입니다. 각 하위 디렉터리에는 사용하는 운영 체제에서 CA Access Control 을 자동으로 시작하는 방법에 대한 지침이 수록된 추가 정보 파일이 들어 있습니다.

참고: CA Access Control 을 시작하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

Linux s390 끝점에서 데몬을 시작할 수 없음

Linux s390 및 Linux s390x 에 해당

증상

seosd 또는 ReportAgent 데몬을 시작할 수 없습니다.

해결 방법

CA Access Control 이 끝점에서 Java 환경을 찾을 수 없습니다. 이 문제를 해결하려면 다음을 수행하십시오.

1. accommon.ini 파일의 전역 섹션에 있는 java_home 구성 설정이 Java 환경에 대한 경로를 포함하는지 확인하십시오.
2. LD_LIBRARY_PATH 환경 변수의 값을 Java 환경의 공유 라이브러리에 대한 경로로 설정하십시오.

설치 후 selang 에 연결할 수 없음

증상:

CA Access Control 을 설치한 이후에 selang 을 시작하거나 CA Access Control 데이터베이스에 연결하려고 시도하면 다음 오류 메시지가 표시됩니다.

```
오류: 초기화하지 못했습니다. 종료합니다.
(localhost)
오류: 로그인 프로시저가 실패했습니다.
오류: 터미널 example.com 에서는 이 사이트를 관리할 수 없습니다.
```

해결책:

터미널 규칙이 올바로 정의되지 않았습니다. 문제점을 파악하기 위해 터미널 규칙의 문제를 해결하십시오.

터미널 규칙의 문제를 해결하려면

1. CA Access Control 을 중지합니다.

   ```
   secons -s
   ```

2. 로컬 모드에서 selang 을 시작합니다.

   ```
   selang -l
   ```

   참고: UNIX 컴퓨터에서 로컬 모드로 selang 을 실행하려면 root 사용자여야 합니다.

3. 로컬 터미널(*terminal_name*)에 대해 TERMINAL 레코드를 만들었는지, 그리고 터미널 액세스 권한이 올바로 정의되었는지 확인하십시오.

   ```
   showres TERMINAL terminal_name
   ```

   - 레코드가 없으면 로컬 터미널에 대해 TERMINAL 레코드를 만드십시오.

     ```
     editres TERMINAL terminal_name owner(name) defaccess(accessAuthority)
     ```

     참고: 소유자는 사용자 또는 그룹일 수 있습니다. TERMINAL 레코드에 대한 기본 액세스가 "none"이므로 터미널에서 사용자가 잠기는 것을 방지하기 위해 레코드를 만들 때 기본 액세스를 지정하는 것이 좋습니다.

   - 터미널 액세스 권한이 잘못된 경우 터미널에 대한 올바른 액세스 권한을 정의하십시오.

     ```
     authorize TERMINAL terminal_name uid(name) access(accessType)
     ```

4. (UNIX) [seosd] 섹션에서 terminal_default_ignore 구성 설정의 값을 확인하십시오.

   이 구성 설정은 관리 액세스 권한을 부여할 때 CA Access Control 이 _default TERMINAL 및 특정 TERMINAL 레코드의 값을 고려할지 여부를 결정합니다.

   참고: terminal_default_ignore 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

5. (UNIX) 다음과 같이 참조(lookaside) 데이터베이스가 터미널을 반영하는지 확인합니다.

   a. 호스트 이름 고유의 참조(lookaside) 데이터베이스를 빌드합니다.

      ```
      sebuilda -h
      ```

   b. 참조(lookaside) 데이터베이스에서 터미널 항목과 호스트 이름이 같은지 확인합니다.

      ```
      sebuilda -H | grep hostname
      ```

      호스트 참조(lookaside) 데이터베이스 파일의 내용이 나열됩니다.

6. CA Access Control 을 시작합니다.

   - (UNIX) seload
   - (Windows) seosd -start

참고: 여전히 selang 을 시작할 수 없거나 CA Access Control 데이터베이스에 연결할 수 없는 경우 사용하는 OS 에 대한 호스트 파일을 수정해야 할 수 있습니다. 이 경우 시스템 관리자 또는 네트워크 관리자에게 도움을 요청하십시오.

Solaris 10 로그 파일에 표시되는 메시지

Solaris 10 에서 유효

증상

"secons -s"를 사용하여 CA Access Control 을 중지하자 Solaris 10 컴퓨터의 "/var/adm/messages" 로그 파일에 CA Access Control 메시지가 표시됩니다. 컴퓨터의 SEOS_use_streams 구성 설정이 'yes'로 설정되어 있습니다.

해결 방법

이 메시지는 정보 제공용이며 실패나 오류를 나타내지 않습니다. 어떠한 조치를 할 필요는 없습니다. 메시지와 그 해석은 다음과 같습니다.

- "SEOS: Restored tcp wput" "SEOS: Restored strrhead rput"

  이 메시지는 SEOS_syscall 함수가 네트워크 후크를 비활성화하였음을 나타냅니다.

- "SEOS: Replaced tcp wput" "SEOS: Replaced strrhead rput"

  이 메시지는 SEOS_syscall 함수가 네트워크 후크를 활성화하였음을 나타냅니다.

제거 중 직접 레지스트리 키를 삭제할 때 오류 발생

Windows 에 해당

증상:

CA Access Control 을 제거할 때 레지스트리 키를 삭제하면 다음과 같은 오류 메시지가 표시됩니다.

데이터를 열 수 없습니다: 키를 여는 동안 오류가 발생했습니다.

해결책:

RemoveAC.exe 유틸리티를 실행하여 CA Access Control 레지스트리 키와 디렉터리를 제거하십시오. RemoveAC.exe 유틸리티는 제품을 제거하는 용도로 사용되지 않지만 컴퓨터에서 모든 CA Access Control 레지스트리 키와 디렉터리가 확실히 제거되도록 도움을 줍니다.

참고: RemoveAC.exe 유틸리티는 CA Access Control 설치 패키지에 포함되어 있지 않습니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

ProductExplorer 가 시작되지 않음

증상

광학 드라이브에 Windows 용 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣으면 ProductExplorer 가 시작되지 않습니다.

해결 방법

다음 작업을 수행하십시오.

- 광학 디스크 드라이브 디렉터리로 이동하여 ProductExplorerx86.EXE 파일을 두 번 클릭합니다.
- ProductExplorer 가 자동으로 시작되도록 자동 실행을 활성화합니다.

CA Licensing 1.9.04 로 업그레이드할 때 라이선스 오류가 발생

UNIX 에 해당

증상

CA Access Control 로 업그레이드할 때 새로운 CA Licensing rpm 스크립트(1.9.04)가 먼저 실행됩니다. 그런 다음 이전 rpm 스크립트에 대한 제거 프로그램이 실행된 후 UNIX syslog 에 다음과 같은 오류 메시지가 기록됩니다.

```
<Error opening lic98.err - /opt/CA/SharedComponents/ca_lic/lic98.err, original
code=5000>2E2U eTrust Access Control for UNIX <Error opening lic98.err -
/opt/CA/SharedComponents/ca_lic/lic98.err, original code=5000>  LRF=2E2U,
000000000000, Linux_x86.64_1_*, ismelx84, 0
```

해결 방법

CA Licensing 버전 1.9.03 이하 설치 관리자는 이 오류로 인해 링크와 폴더를 제거합니다. 업그레이드를 수행하는 것은 권장되지 않으며, 대신 바로 CA Licensing 버전 1.9.04 를 설치할 것을 권장합니다.

다음 단계를 수행하십시오.

1. CA Access Control 이 실행 중인 경우 관리자로 로그인한 후 다음 명령을 입력하여 종료합니다.

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. 임시 폴더에 다음 파일을 백업합니다.
   - /etc/profile
   - /etc/profile.CA
   - /etc/csh_login.CA
   - 다음 항목에 대한 모든 심볼 링크 정보를 기록합니다.
     - /usr/local/CAlib
     - /opt/CA/CAlib
     - $CASHCOMP/CAlib
     - /ca_lic
     - /opt/CA/ca_lic
     - $CASHCOMP/ca_lic
     - $CASHCOMP/lib

3. 모든 심볼 디렉터리를 백업합니다.
4. Support 웹 사이트에서 최신 CA Licensing 패키지를 다운로드합니다.
5. 압축 파일의 내용을 임시 디렉터리에 추출합니다.
6. 새로운 lic98_install 디렉터리로 이동합니다.
7. 다음 명령을 입력하여 CA Licensing 을 설치합니다.

   ```
   ./install <install directory>
   ```

8. 다음 명령을 입력하여 /etc/profile 을 소싱합니다.

   ```
   ./etc/profile
   ```

9. 다음 단계를 수행하여 ca.olf 파일을 복원합니다.
   a. 다음 명령을 실행합니다.

      ```
      rpm -e --nodeps ca-lic
      ```

   b. 2 단계에서 백업한 디렉터리를 다음 디렉터리로 복원합니다.

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   c. 2(d) 단계에서 기록한 심볼 기록을 다음 디렉터리로 복원합니다.

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   d. 백업한 /etc/profile, /etc/profile.CA, /etc/csh_login.CA 파일을 다음 디렉터리로 복원합니다.

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   CA Licensing 1.9.04 가 성공적으로 설치되었고 이제 등록된 모든 CA 제품을 사용할 수 있습니다.

제 3 장: 정책 및 액세스 권한 만들기

이 섹션은 다음 항목을 포함하고 있습니다.

네트워크 드라이브와 공유 드라이브에 대한 사용자 액세스 차단

Windows 에 해당

증상

시스템 드라이브에 대한 사용자 액세스를 차단할 수 있지만 네트워크 및 공유 드라이브에 대한 사용자 액세스는 차단할 수 없습니다.

해결 방법

Windows 2008 에서 네트워크 및 공유 드라이브에 대한 사용자 액세스를 차단하려면 다음 selang 명령을 정책에 추가하십시오.

```
newres FILE \Device\Mup\*
```

Windows 2003 에서 네트워크 및 공유 드라이브에 대한 사용자 액세스를 차단하려면 다음 selang 명령을 정책에 추가하십시오.

```
newres FILE \Device\LanmanRedirector\*
```

사용자가 보호된 리소스에 액세스할 수 있음

증상:

리소스에 대해 기본 액세스 권한을 'none'으로 설정했는데 superuser 가 여전히 이 리소스에 액세스할 수 있습니다.

해결책:

리소스 액세스 문제를 해결하십시오 (페이지 120).

읽기 액세스 검사가 /etc/passwd 및 /etc/group 파일을 바이패스함

UNIX 에 해당

증상:

/etc/passwd 및 /etc/group 파일에 대해 기본 액세스 권한 none 이 지정된 규칙을 만들었지만 여전히 이러한 파일에 읽기 액세스가 허용됩니다.

해결책:

기본적으로 CA Access Control 권한 부여 엔진은 /etc/passwd 및 /etc/group 시스템 파일에 대한 읽기 액세스 검사를 바이패스합니다. CA Access Control 이 시스템 파일에 대해 읽기 액세스 검사를 바이패스하지 않도록 하려면 seos.ini 파일의 [seosd] 섹션에 있는 value of bypass_system_files 의 값을 no 로 변경하십시오.

중요! CA Access Control 이 시스템 파일에 대해 읽기 액세스 검사를 바이패스하지 않도록 지정하는 경우 권한 부여가 올바른지 확인하십시오. 권한 부여가 잘못된 경우 읽기 액세스 바이패스를 중지하면 CA Access Control 관리자 및 root 사용자를 포함한 사용자가 시스템에 액세스할 수 없거나 중요한 시스템 프로세스가 실패할 수 있습니다.

기업 사용자 또는 그룹이 리소스에 액세스할 수 없으나 올바른 액세스 규칙이 설정됨

Windows 에 해당

증상

기업 사용자 또는 그룹에 리소스 액세스 권한이 있지만 리소스에 액세스할 수 없습니다.

해결 방법

기업 계정이 재사용되었고 데이터베이스의 사용 권한이 이름은 같지만 SID 가 다른 새 계정이 아니라 이전 계정에 적용될 수 있습니다. 이 경우를 확인하려면 재사용 기업 계정을 확인하십시오.

참고: 재사용된 엔터프라이즈 저장 계정에 대한 자세한 내용은 *Windows 용 끝점 관리 안내서*를 참조하십시오.

로그인에 실패해도 사용자가 잠기지 않음

UNIX 에 해당

증상:

지정된 횟수 이상 로그인 시도가 실패하면 암호 PMD 에서 사용자가 비활성화되도록 serevu 를 구성했습니다. 사용자가 올바로 로그인하지 못하는 경우 CA Access Control 이 이 사용자를 잠그지 않습니다. pam_failed_logins.log 파일을 보기 위해 nodaemon 옵션을 사용하여 serevu 를 시작하면 서버가 응답하지 않습니다.

해결책:

seos.ini 파일의 [seos] 섹션에 있는 passwd_pmd 의 값이 잘못되었습니다. passwd_pmd 의 값을 sepass 가 암호 업데이트를 보내는 암호 PMD 의 이름으로 설정하십시오.

사용자가 시간 제한 없이 명령을 실행할 수 있음

증상:

그룹에 시간 제한을 설정했지만 그룹 구성원들이 허용되는 시간 이외의 시간에도 CA Access Control 명령을 실행할 수 있습니다.

해결책:

제한된 기간 중에 CA Access Control 은 사용자가 새 로그인 세션을 시작할 수 없도록 만들지만 사용자의 연결을 끊을 수는 없습니다. 제한된 기간 중에 사용자가 리소스 또는 명령에 액세스할 수 없도록 하려면 시간 제한을 포함하도록 해당 리소스 또는 명령에 대한 리소스 레코드를 변경하십시오.

참고: CA Access Control 은 사용자가 속한 GROUP 또는 XGROUP 에 시간 제한이 있는지 확인하기 전에 사용자의 USER 또는 XUSER 레코드에 시간 제한이 있는지 먼저 확인합니다.

CA Access Control 이 모든 사용자를 root 로 인식함

UNIX 에 해당

증상:

root 가 아닌 사용자에 대해 sewhoami 유틸리티를 실행하면 CA Access Control 이 이 사용자를 root 로 인식합니다.

해결책:

이 문제를 해결하려면 로그인 응용 프로그램의 LOGINAPPL 레코드에서 다음을 확인하십시오.

- LOGINAPPL 레코드의 이름이 로그인 응용 프로그램의 이름입니다.
- LOGINAPPL 레코드의 LOGINPATH 매개 변수가 로그인 응용 프로그램에 대한 올바른 전체 경로를 지정합니다.

  로그인 응용 프로그램에 대한 경로를 파악하려면 추적을 실행 (페이지 124)한 다음 로그인 응용 프로그램을 사용하여 CA Access Control 에서 로그인 및 로그아웃합니다. 추적을 검토하여 경로를 파악합니다.
- LOGINAPPL 레코드의 LOGINSEQUENCE 매개 변수가 로그인 응용 프로그램에 대한 올바른 로그인 시퀀스를 지정합니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

참고: CA Access Control 은 타사 로그인 응용 프로그램에 대한 LOGINAPPL 레코드를 정의하지 않습니다. 타사 로그인 응용 프로그램을 사용하는 경우 이 응용 프로그램에 대한 LOGINAPPL 레코드를 직접 정의하십시오.

하나의 그룹에 대해서만 사용자를 암호 관리자로 추가할 수 없음

증상:

한 사용자를 특정 그룹에 대한 암호 관리자로 만들고 싶지만 다음 명령을 실행하면 이 사용자가 모든 그룹의 암호 관리자가 됩니다.

```
editusr userName pwmanager
```

해결책:

다음과 같이 암호 관리자로 사용자를 추가할 그룹의 이름을 지정하십시오.

```
join userName group(groupName) pwmanager
```

Windows 관리자가 CA Access Control 암호를 변경할 수 있음

Windows 에 해당

증상:

Windows 관리자가 CA Access Control-보호된 Windows 환경에서 CA Access Control 암호를 변경할 수 있습니다.

해결책:

CA Access Control 에서 지정한 사용자만 CA Access Control 암호를 변경할 수 있도록 하려면 다음 키에서 EnforceViaeTrust 레지스트리 항목의 값을 1 로 설정하십시오.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd
```

이 레지스트리 항목은 CA Access Control 을 사용해서만 사용자 암호를 만들고 업데이트할 수 있도록 지정합니다. 이 레지스트리 항목의 기본값은 0 으로, 사용자 암호를 업데이트하거나 변경하기 위해 반드시 CA Access Control 을 사용할 필요가 없음을 의미합니다.

전역 암호 정책이 사용자를 보호된 시스템에서 잠금

증상:

전역 암호 정책을 구현할 때 암호 정책이 CA Access Control 에 의해 보호되는 시스템에서 사용자를 잠급니다.

해결책:

CA Access Control-보호되는 시스템에 액세스해야 하는 사용자에 대해 별도의 암호 정책을 만드십시오. 이러한 사용자에 대한 암호를 만들려면 프로필 그룹을 사용하십시오.

다음 프로세스는 프로필 그룹을 사용하여 암호 정책을 구현하는 방법을 설명합니다.

1. 프로필 그룹을 만듭니다.
2. 프로필 그룹에 대한 암호 정책을 설정합니다.
3. 사용자를 이 프로필 그룹에 할당합니다.

   지금 프로필 그룹에 대해 설정한 암호는 이제 프로필 그룹과 관련된 사용자에게 적용됩니다.

대화형 응용 프로그램에 대한 작업 위임이 중지됨

Windows 에 해당

증상

사용자들이 대화형 Windows 응용 프로그램(예: notepad.exe)을 실행할 수 있는 작업 위임 규칙을 작성했습니다. 사용자가 이 응용 프로그램을 실행하면 작업 위임이 중지됩니다.

해결 방법

대화형 플래그는 사용자가 응용 프로그램을 실행하도록 허용하는 SUDO 클래스 레코드에 대해 설정되어야 합니다. 대화형 Windows 응용 프로그램을 실행하기 위해 작업 위임을 사용하는 경우 대화형 플래그가 설정되지 않았으면 응용 프로그램이 백그라운드로 실행되고 대화형으로 작업할 수 없게 됩니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. SUDO 레코드에 대한 대화형 플래그를 설정합니다:

   ```
   er SUDO resourceName interactive
   ```

   resourceName

   사용자가 응용 프로그램을 실행할 수 있도록 하는 리소스 레코드의 이름을 지정합니다.

   대화형 플래그는 지정된 리소스에 대해 설정됩니다.

2. 다음과 같이 작업 위임 서비스를 다시 시작합니다:

   a. 대화형 응용 프로그램을 중지(kill)gkqslek.

   b. 작업 위임이 아직 중지되어 있는 경우 CA Access Control 을 다시 시작합니다.

참고: 작업 위임 및 SUDO 레코드 정의에 대한 자세한 내용은 *Windows 용 끝점 관리 안내서*를 참조하십시오.

제 4 장: CA Access Control 데이터베이스를 제거합니다.

이 섹션은 다음 항목을 포함하고 있습니다.

selang 쿼리가 최대 100 개 레코드를 반환함

증상:

100 개 이상의 레코드를 반환해야 할 selang 쿼리를 실행하면 CA Access Control 에서 다음 메시지가 표시됩니다.

```
경고: 100 개(쿼리 크기 제한) 항목만 표시됩니다.
```

해결책:

query_size 구성 설정의 기본값은 100 입니다. CA Access Control 이 selang 쿼리에 대해 반환하는 레코드의 수를 늘리려면 query_size 구성 설정의 값을 변경하십시오.

query_size 구성 설정은 다음 위치에서 찾을 수 있습니다.

- (UNIX) seos.ini 파일의 [lang] 섹션
- (Windows) 다음과 같은 lang 하위 키

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang
  ```

데이터베이스 백업 후 감사 로그의 UTimes 및 거부된 레코드

증상:

CA Access Control 이 실행될 때 OS 백업 도구를 사용하여 CA Access Control 데이터베이스를 백업하면 CA Access Control 다음 메시지와 유사한 항목을 감사 로그에 전달합니다.

```
03 Mar 2008 15:58:01 D FILE            UTimes     69 10
/opt/CA/AccessControl/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

참고: 위의 예는 UNIX 매개 변수를 사용하여 작성되었지만 Windows 컴퓨터에서도 해결 방법은 동일합니다.

해결책:

이 감사 메시지는 CA Access Control 이 백업 작업이 UTimes 파일 날짜 스탬프를 업데이트하는 것을 방지함을 의미합니다. CA Access Control 은 백업 자체를 방지하지는 않습니다.

감사 로그에 이 메시지가 나타나지 않도록 하려면 다음을 수행하십시오.

- superuser 가 아닌 사용자가 백업 프로그램을 실행한 경우 이 사용자에게 OPERATOR 특성이 있는지 확인하십시오.
- superuser 가 백업 프로그램을 실행한 경우 pgmtype(backup) 속성이 있는 SPECIALPGM 레코드가 백업 프로그램에 있는지 확인하십시오.

데이터베이스가 올바로 백업되도록 하려면 dbmgr 유틸리티를 사용하여 백업을 수행하십시오.

CA Access Control 데이터베이스가 손상됨

UNIX 에 해당

증상:

CA Access Control 오류 로그에서 다음과 유사한 메시지를 찾았습니다.

```
seoswd: [ID 973226 auth.error] seosd 와의 통신 시간이 초과되었습니다. seosd 를 실행하는
중입니다.
치명적 오류!
Inseosrt_InitDatabase (0x270)
경고: Access Control/seosdb/seos_cdf.dat 의 경로가 손상되었습니다.
```

해결책:

다음 절차에 따라 데이터베이스 손상을 수정하십시오.

참고: 이 절차에서는 데이터베이스가 기본 설치 위치인 /opt/CA/AccessControl/에 설치되어 있다고 가정합니다.

CA Access Control 데이터베이스 손상을 수정하려면

1. CA Access Control 을 중지합니다.

   ```
   secons -s
   ```

2. (선택 사항) 필요한 경우 기술 지원부에 제공할 수 있도록 데이터베이스를 다른 위치에 백업합니다.

3. 데이터베이스가 닫힌 상태로 표시되었는지 확인합니다.

   ```
   cd /opt/CA/AccessControl//seosdb

   dbmgr -util -close
   ```

   참고: CA Access Control 이 올바로 종료되지 않은 경우 데이터베이스가 열린 상태로 표시됩니다.

4. 데이터베이스를 검사합니다.

   ```
   dbmgr -util -check
   ```

5. 다음 작업 중 *하나*를 수행합니다.

   - 데이터베이스를 검사할 때 오류 메시지가 표시되지 않으면 6 단계로 이동합니다.
   - 데이터베이스를 검사할 때 오류 메시지가 표시되면 6 단계와 7 단계를 수행하지 말고 데이터베이스를 다시 빌드 (페이지 127)하십시오.

6. 데이터베이스 파일을 빌드합니다.

   ```
   dbmgr -util -build all
   ```

7. 데이터베이스를 다시 검사합니다.

   ```
   dbmgr -util -check
   ```

8. CA Access Control 을 시작합니다.

   ```
   seload
   ```

참고: 데이터베이스가 여전히 손상된 경우 추가적인 조사가 필요합니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

제 5 장: 원격 PMDB 에 연결 중...

이 섹션은 다음 항목을 포함하고 있습니다.

원격 컴퓨터에 연결할 수 없음

증상:

원격 CA Access Control 컴퓨터에 연결할 수 없습니다.

해결책:

연결 문제를 해결하십시오 (페이지 121).

syslog 에 계속 seosd 와의 통신 시간 초과가 표시됨

Windows 에 해당

증상:

CA Access Control 을 실행할 때 컴퓨터가 때때로 느려지고 syslog 에 다음 메시지가 나타납니다.

```
seoswd: seosd 와의 통신 시간이 초과되었습니다. seosd 를 실행하는 중입니다.
seoswd: seosd 와의 통신 문제로 5378 [Success]이(가) 반환되었습니다.
seoswd: 설명: seosd 와의 통신 시간이 초과되었습니다.
```

해결책:

컴퓨터에 있는 바이러스 백신 소프트웨어로 인해 CA Access Control 의 시간 만료가 발생합니다. 바이러스 백신 소프트웨어에서 다음을 수행하십시오.

- 실시간 검색에서 CA Access Control 디렉터리를 제외시킵니다.
- CA Access Control 디렉터리에 대해 실시간 검색(액세스할 때 검사)을 중단합니다.

CA Access Control 은 기본적으로 CA Access Control 레지스트리 키, 파일, 설치 디렉터리를 보호하므로 앞의 작업으로 인해 컴퓨터에 대한 바이러스 감염 가능성을 높이지 않습니다.

바이러스 백신 소프트웨어에 대한 SPECIALPGM 레코드를 만들고 이 SPECIALPGM 레코드에 대한 PGMTYPE 속성을 pbf 로 설정하는 것이 좋습니다. pbf 프로그램 유형은 이벤트를 처리하는 파일에 대한 데이터베이스 검사를 바이패스합니다.

처음 들어오는 FTP 연결이 제어되지 않음

UNIX 에 해당

증상:

CA Access Control 을 시작하면 vsftpd 에서 처음 들어오는 FTP 연결을 제어하지 않습니다. FTP 에 대한 TCP 규칙과 vsftpd 에 대한 HOST 규칙을 만들었고 이러한 TCP 또는 HOST 규칙에 따라 CA Access Control 이 vsftpd 에서 들어오는 모든 이후 FTP 연결을 제어합니다.

해결책:

CA Access Control 을 시작하기 전에 vsftpd 를 시작하면 vsftpd 가 들어오는 FTP 연결에 대한 시스템 호출 승인에 후크를 배치합니다. 이 후크는 CA Access Control 이 처음 들어오는 FTP 연결을 차단하기 전에 vsftpd 가 이 연결을 처리함을 의미합니다.

vsftpd 가 FTP 연결을 처리한 이후에는 다음 FTP 연결에 대비하기 위해 시스템 호출 승인을 호출하려고 시도합니다. 하지만 CA Access Control 이 이 시스템 호출을 차단하고 모든 이후 FTP 연결을 제어하게 됩니다.

처음 들어오는 FTP 연결을 차단하려면 다음 해결 방법 중 하나를 사용하십시오.

- vsftp 를 시작하기 전에 CA Access Control 을 시작하십시오.
- inetd 또는 xinetd 와 같은 슈퍼 서버 데몬을 사용하여 vsftpd 를 시작합니다.

  참고: 슈퍼 서버 데몬을 구성하는 방법에 대한 자세한 내용은 OS 공급업체에 문의하십시오.
- CA Access Control 을 시작한 이후에 tripAccept 유틸리티를 실행합니다.

  tripAccept 유틸리티를 실행하려면 seos.ini 파일의 [SEOS_syscall] 섹션에서 call_tripAccept_from_seload 토큰을 활성화해야 합니다. tripAccept 유틸리티를 실행하기 전에 이 유틸리티에 대한 SPECIALPGM 레코드를 정의하는 것이 좋습니다.

로컬 호스트와 대상 호스트의 대상 페이지가 다름

UNIX 에 해당

증상:

CA Access Control 호스트에 연결을 시도하면 다음 메시지가 표시됩니다.

```
경고: 로컬 시스템의 코드 페이지가 대상 호스트의 코드 페이지와 다릅니다.
```

해결책:

seos.ini 파일의 [seos] 섹션에 있는 로캘 구성 설정의 값이 로컬 호스트 및 대상 호스트에서 동일한지 확인하십시오.

selang 을 사용하여 끝점에 연결할 수 없음

증상:

selang 을 사용하여 끝점에 연결하려고 하면 다음과 유사한 오류 메시지가 표시됩니다.

데이터 압축을 풀지 못했습니다.

해결책:

구성 요소 간 통신을 보호하기 위해 사용된 암호화에 문제가 있습니다. CA Access Control 컴퓨터에서 암호화 키와 암호화 방법에 대한 최근 변경 사항을 확인하십시오.

참고: 암호화 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

제 6 장: PMD 로부터 규칙 배포

이 섹션은 다음 항목을 포함하고 있습니다.

구독자 PMDB 가 마스터 PMDB 로부터 업데이트를 받지 못함

증상:

계층적 PMDB 아키텍처를 사용합니다. 구독자 PMDB 가 마스터 PMDB 로부터 업데이트를 받지 않습니다. 마스터 PMDB 의 오류 로그에 다음과 같은 메시지가 있습니다.

```
상위가 아닌 PMDB 에서 업데이트를 수락할 수 없습니다.
```

해결책:

구독자 PMDB 가 마스터 PMDB 로부터 업데이트를 받지 않으면 다음 절차에 따라 문제를 해결하십시오.

PMDB 업데이트 문제를 해결하려면

1. 마스터 PMDB(*master_pmdb_name*)의 구독자와 그 상태를 나열합니다.

   ```
   sepmd -L master_pmdb_name
   ```

   참고: 이 명령은 마스터 PMDB 컴퓨터에서 실행하십시오.

2. 구독자의 목록을 검토하여 사용할 수 없는 구독자를 파악합니다.

3. 각 사용할 수 없는 구독자에 대해 parent_pmd 구성 설정의 값이 올바른지 확인합니다.

   parent_pmd 구성 설정은 다음 위치에 있습니다.

   - (UNIX) seos.ini 및 pmd.ini 파일의 [seos] 섹션
   - (Windows) 다음 레지스트리 키

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl

   참고: parent_pmd 토큰에 지정하는 호스트 이름은 마스터 PMDB 의 호스트 이름과 정확히 일치해야 합니다. 호스트 이름 확인이 올바로 구성되었는지 확인하는 것으로 이 문제가 해결될 수 있습니다. UNIX 컴퓨터를 사용하는 경우 sehostinf 유틸리티를 사용하여 마스터 PMDB 의 호스트 이름을 찾을 수 있습니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

문제가 계속되면 다음을 수행하십시오.

1. 마스터 PMDB 오류 로그를 표시합니다.

   ```
   sepmd -e master_pmdb_name
   ```

2. 오류 로그를 검토하여 사용할 수 없는 구독자에 대해 보고된 오류 코드를 확인합니다.
3. 사용할 수 없는 각각의 구독자에 대해 이 오류 코드를 사용하여 문제를 해결합니다.

문제가 계속되면 다음을 수행하십시오.

1. 마스터 PMDB 가 유지 관리하는 사용할 수 없는 구독자의 목록에서 문제가 있는 구독자를 제거합니다.

   ```
   sepmd -r pmdb_name subscriber_name
   ```

   부모 PMDB 가 구독자에게 업데이트를 보내려고 시도합니다.

2. 이전 절차를 반복합니다.
3. 구독자의 목록 또는 부모 PMDB 오류 로그에 변경 사항이 있는 경우 이 변경 사항을 사용하여 문제를 해결합니다.

구독자 끝점의 감사 로그에 실패한 이벤트가 있음

증상:

구독자가 마스터 PMDB 로부터 업데이트를 받지 않습니다. 구독자의 CA Access Control 감사 로그에 *실패* 이벤트가 있습니다.

해결책:

PMDB 사용자에게 ADMIN 특성이 없습니다. PMDB 사용자에게 ADMIN 특성을 부여하려면 다음과 같이 selang 명령을 사용하여 사용자 레코드를 편집하십시오.

```
chusr userName admin
```

참고: 이 selang 명령을 실행하려면 ADMIN 특성이 있어야 합니다. CA Access Control 은 PMDB 업데이트를 구독자에게 배포할 때 TERMINAL 규칙을 바이패스합니다.

제 7 장: 정책 배포

이 섹션은 다음 항목을 포함하고 있습니다.

정책 배포 문제 해결

호스트에 정책을 할당할 때 policyfetcher 가 배포 작업을 검색하고 정책 스크립트를 실행할 때까지 정책은 할당된 끝점에 배포되지 않습니다. 따라서 정책이 전송되거나 끝점에 배포될 때 다양한 이유로 배포 오류가 발생할 수 있습니다.

정책 배포 오류를 해결하기 위해 고급 정책 관리에는 문제 해결 작업을 제공합니다. 이러한 작업은 CA Access Control 엔터프라이즈 관리 또는 policydeploy 유틸리티를 사용하여 수행할 수 있습니다. CA Access Control 엔터프라이즈 관리에서 문제 해결 작업은 "정책 관리" 탭의 "정책" 하위 탭에 있습니다.

문제 해결 작업은 다음과 같습니다.

- **재배포** - 정책 스크립트를 포함하는 새 배포 작업을 만들어 끝점에 배포합니다.

  정책을 끝점에 배포할 때 오류가 발생하는 경우 이 옵션을 사용하십시오. 즉, selang 정책 스크립트 실행이 실패하는 경우입니다. 정책을 재배포하려면 먼저 끝점에서 스크립트 오류의 원인을 수동으로 수정해야 합니다.

  참고: 이 옵션은 CA Access Control 엔터프라이즈 관리에서만 사용할 수 있으며 policydeploy 유틸리티에서는 지원되지 않습니다.

- **배포 취소** - 해당 호스트에서 정책을 할당 취소하지 않고 지정된 끝점에서 정책의 배포를 취소합니다.

  DMS 에 있는 호스트에 할당되지 않은 끝점에서 정책을 제거하려면 이 옵션을 사용하십시오.

- **다시 설정** - 끝점을 다시 설정합니다. CA Access Control 은 호스트 상태를 재설정하고, 모든 유효 정책을 배포 취소하며, 모든 GPOLICY, POLICY, RULESET 개체를 삭제합니다.

  DMS 에서 끝점과 그 상태를 삭제하려면 모든 정책 배포에서 이 옵션을 사용하십시오.

  참고: 감사를 위해 필요할 수도 있으므로 이 옵션은 끝점 또는 DMS 에서 DEPLOYMENT 또는 GDEPLOYMENT 개체를 제거하지 않습니다. 끝점을 다시 설정한 후에 dmsmgr -cleanup 기능을 사용하여 DEPLOYMENT 및 GDEPLOYMENT 개체를 제거할 수 있습니다. 끝점을 다시 설정한 이후에 정상적으로 끝점에 정책을 할당할 수 있습니다.

- **복원** - 지정된 호스트에서 모든 정책의 배포를 취소한 다음, 새 배포 작업을 만들어 실행을 위해 호스트에 이 작업을 전달함으로써 호스트에 배포(할당 또는 직접 배포됨)해야 할 모든 정책을 복원합니다.

  DMS 가 해당 끝점에서 유효한 것으로 나타내는 모든 정책을 다시 배포하려면 끝점에서 CA Access Control 또는 운영 체제를 다시 설치할 때 또는 백업에서 끝점을 복원할 때 이 옵션을 사용하십시오.

모든 끝점에서 정책이 성공적으로 배포되지 않음

증상

호스트 그룹에 정책을 배포했습니다. 정책이 호스트 그룹의 일부 호스트에는 성공적으로 배포되었지만 다른 호스트에서는 배포했을 때 오류가 발생했습니다.

해결 방법

이 문제를 해결하려면 다음 중 하나를 수행하십시오.

- 정책이 적은 수의 호스트에서 실패한 경우 이 호스트에서 정책을 다시 배포하십시오.

  정책을 재배포하려면 먼저 호스트에서 배포 오류의 원인을 수동으로 수정해야 합니다.

- 많은 수의 호스트에서 정책이 실패한 경우 각 끝점에서 policydeploy -fix 기능을 실행하십시오.

  policydeploy -fix 기능은 지정된 배포 작업 또는 패키지를 수정하고 다시 배포합니다. 이 기능을 사용하려면 배포 작업의 이름이 필요합니다.

참고: policydeploy 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: policydeploy -fix 기능

다음 예는 끝점에서 지정된 배포 패키지를 수정합니다.

```
policydeploy -fix -task 1266471565#0f6a3cec-a37d-47d9-bde3-0112a49b714a
```

DH 또는 재해 복구 DMS 를 다시 구독하지 못함

증상:

재해 복구 프로세스의 일부로서 DH 를 DMS 에 다시 구독하거나 재해 복구 DMS 를 프로덕션 DMS 에 다시 구독하려고 시도합니다. 다음과 같은 메시지가 나타납니다.

subscriber 을(를) *dms@host* 에 다시 구독하지 못했습니다.
복원 작업을 완료하려면 오프셋 *value* 를 사용하여 *subscriber@host* 를 *dms@host* 에서 직접 구독하십시오.

해결책:

이 메시지는 DH 또는 재해 복구 DMS 를 현재 실행되고 있지 않은 부모 DMS 에 다시 구독할 때 나타납니다. DH 를 DMS 에, 또는 재해 복구 DMS 를 DMS 에 직접 다시 구독하려면 메시지의 오프셋 값을 사용해야 합니다. 오프셋 값을 지정하면 복원될 때 데이터베이스에 존재하지 않았던 명령만 구독자에게 전달됩니다.

DH 또는 재해 복구 DMS 를 부모 DMS 에 다시 구독하려면 부모 DMS 호스트에서 다음 명령을 실행하십시오.

```
sepmd -s parent_name child_name@host offset
```

예: DH 를 DMS 에 구독

다음 예는 오프셋 18028 을 사용하여 DH__@test.com 을 DMS__에 구독합니다. 이 명령은 DMS__에서 실행하십시오.

```
sepmd –s DMS__ DH__@test.com 18028
```

정책이 "실행되지 않음" 상태임

증상:

정책 확인을 활성화했습니다. 정책을 배포할 때 정책이 배포되지 않고 정책 상태가 "실행되지 않음"입니다.

해결책:

정책 확인 중 정책에서 하나 이상의 오류를 발견했습니다. 정책을 성공적으로 배포하려면 먼저 이 오류를 해결해야 합니다.

정책을 성공적으로 배포하려면 다음 단계를 수행하십시오.

1. 오류를 검토합니다.

   문제를 해결하려면 오류가 정책에서 발생하는지 또는 CA Access Control 데이터베이스에서 발생하는지 여부를 파악해야 합니다.

   a. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "배포" 트리를 확장한 다음 "배포 감사"를 클릭합니다.

      "배포 감사" 페이지가 나타납니다.

   b. 검색 범위를 정의하고 "실행"을 클릭합니다.

      정의한 검색 범위와 일치하는 배포 작업 목록이 나타납니다.

   c. 배포되지 않은 배포 작업의 이름을 클릭합니다.

      정책의 오류 목록을 포함하여, 배포에 대한 정보가 표시됩니다.

2. (선택 사항) CA Access Control 데이터베이스에서 오류가 발생한 경우 다음을 수행합니다.

   a. CA Access Control 데이터베이스에서 오류를 수정합니다.

   b. 다음 작업 중 *하나*를 수행합니다.

      - 배포 작업 문제를 해결하려면 policydeploy 유틸리티를 사용하십시오.

        배포 작업의 문제를 해결하면 배포 작업에 대한 "실패" 상태가 제거되고, 배포가 성공하는 경우 끝점에서 배포 상태가 "배포됨"으로 변경됩니다.

      - 정책을 다시 배포하려면 CA Access Control 엔터프라이즈 관리 또는 policydeploy 유틸리티를 사용하십시오.

        정책을 다시 배포하면 또 다른 배포 작업이 만들어집니다. 오류가 발생했던 이전 배포 작업의 상태는 계속 "실패"로 유지됩니다. 배포가 성공하면 끝점에서 배포 상태가 "배포됨"이 됩니다.

3. (선택 사항) 정책에서 오류가 발생한 경우 다음을 수행합니다.

   a. 오류가 없는 새 정책 버전을 만듭니다.

   b. 정책을 업그레이드하려면 CA Access Control 엔터프라이즈 관리 또는 policydeploy 유틸리티를 사용하십시오.

정책 상태가 배포 취소될 때 오류 발생

증상

끝점에서 정책의 배포 취소를 시도한 후 상태가 "배포 취소되었지만 오류 발생"으로 설정되었습니다.

해결 방법

"배포 취소되었지만 오류 발생" 상태는 정책이 배포 취소 스크립트에 있는 하나 이상의 규칙을 사용하여 배포 취소되었지만 끝점에서 실행되지 않음을 의미합니다. 이 정책 상태는 CA Access Control 엔터프라이즈 관리에서 제거할 수 없습니다.

이 문제를 해결하려면 정책 버전의 상태를 직접 제거하십시오.

추가 정보:

정책 버전의 상태를 제거할 수 없음 (페이지 58)

정책 버전의 상태를 제거할 수 없음

증상

정책 버전이 호스트에서 효과가 없지만 이 정책 버전의 상태를 제거할 수 없습니다. 이로 인해 정책 버전을 삭제할 수 없습니다.

해결 방법

이 문제를 해결하려면 정책 상태를 직접 제거해야 합니다.

정책 상태를 직접 제거하려면 다음을 수행하십시오.

1. 끝점에서 정책 버전의 상태를 제거합니다.
   a. 끝점에서 다음 selang 명령을 실행합니다.

      ```
      sr HNODE __local__
      ```

   b. 출력의 정책 상태 섹션에서 정책의 이름을 찾고 '업데이트한 사람' 사용자를 메모합니다.
   c. 끝점에서 다음 selang 명령을 실행합니다.

      ```
      er HNODE __local__ policy(name(policyName#policyVersion) status(undeployed)
      updator(userName))
      ```

      policyName#policyVersion

      삭제할 정책 버전의 이름과 버전 번호를 정의합니다.

      userName

      '업데이트한 사람' 사용자의 이름을 정의합니다.

      끝점에서 정책 버전의 상태가 제거됩니다.

2. DMS 에서 정책 버전의 상태를 제거합니다.
   a. DMS 에서 다음 selang 명령을 실행합니다.

      ```
      sr HNODE hnodeName
      ```

      hnodeName

      정책 버전이 배포된 호스트의 이름을 정의합니다.

   b. 출력의 정책 상태 섹션에서 정책의 이름을 찾고 '업데이트한 사람' 사용자를 메모합니다.
   c. DMS 에서 다음 selang 명령을 실행합니다.

      ```
      er HNODE hnodeName policy(name(policyName#policyVersion) status(undeployed)
      updator(userName))
      ```

   DMS 에서 정책 버전의 상태가 제거됩니다.

예: 끝점에서 정책 버전의 상태 제거

다음 예는 끝점에서 이름이 mypolicy 인 정책의 버전 01 에 대한 상태를 제거합니다.

```
AC> sr HNODE __local__
(localhost)
Data for HNODE '__local__'
-----------------------------------------------------------
Defaccess         : R
Audit mode        : Failure
Owner             : Domain\Administrator (USER)
Create time       : 28-Feb-2010 12:34
Update time       : 04-Mar-2010 05:10
Updated by        : +policyfetcher (USER)
Effective UID     : superadmin
Policy Status     :
    mypolicy#01   : Deployed              Updated by: superadmin  On: 04-Mar-2010
05:10
    Deviation     : Unset                  Updated on: N/A

AC> er HNODE __local__ policy(name(mypolicy#01) status(undeployed)
updator(superadmin))
(localhost)
HNODE __local__을 성공적으로 업데이트했습니다.
```

변수가 있는 규칙이 끝점에서 배포되지 않음

증상

변수가 있는 규칙을 포함하는 정책을 만들어 끝점에 배포했지만 이 규칙이 끝점에서 구현되지 않았습니다.

해결 방법

다음 절차에 따라 정책 배포 문제를 해결하십시오.

1. 끝점의 policyfetcher 섹션에서 policyfetcher_enabled 구성 설정의 값이 1 인지 확인합니다.

   이 구성 설정에서 값 1 은 policyfetcher 를 실행하도록 지정합니다. policyfetcher 가 실행 중이지 않은 경우 정책을 끝점으로 전달할 수 없습니다.

2. policyfetcher 로그에서 오류를 검토합니다.

   참고: policyfetcher 로그는 *ACInstallDir*/Log 디렉터리에 있습니다. 여기서 *ACInstallDir* 는 CA Access Control 이 설치된 디렉터리입니다.

3. CA Access Control 끝점 관리를 사용하여 변수가 끝점에서 정의되어 있는지 확인합니다.

   참고: 변수가 끝점에서 정의되어 있지 않으면 정책은 "배포 보류" 상태가 됩니다.

   끝점에 변수가 정의되어 있지 않으면 변수를 정의하는 selang 규칙을 포함하는 새 정책 버전을 만들어 끝점에 배포하십시오.

4. 다음 사항을 확인합니다.

   - 정책이 끝점에 할당되었는지 확인합니다.

     정책이 끝점에 할당되지 않은 경우 CA Access Control 엔터프라이즈 관리를 사용하여 정책을 할당하십시오.

   - 정책에 대한 배포 스크립트에 오류가 없는지 확인합니다.

     정책에 대한 배포 스크립트에 오류가 있는 경우 이 오류를 수정하는 새 정책 버전을 만들어 끝점에 배포하십시오.

   - 정책 상태가 "동기화되지 않음"이 아닌지 확인합니다.

     정책 상태가 "동기화되지 않음"인 경우 변수 값이 CA Access Control 끝점에서 변경되었을 수 있습니다. 정책을 다시 배포하여 "동기화되지 않음" 상태를 지웁니다.

5. 배포 정보를 감사하여 다음을 확인합니다.

   - 끝점이 정책을 올바로 컴파일했는지 확인합니다.
   - 정책에 대한 DEPLOYMENT 개체에 배포 오류가 없는지 확인합니다.

   정책이 올바로 컴파일되지 않았거나 DEPLOYMENT 개체에 오류가 있는 경우 이 오류를 수정하고 정책을 다시 배포하십시오.

6. CA Access Control 을 다시 시작합니다.

기본 제공된 변수가 새로 고쳐지지 않음

증상

CA Access Control 끝점에서 시스템 설정을 변경했지만 기본 제공되는 변수의 값이 새 시스템 설정의 값으로 변경되지 않았습니다.

해결 방법

다음 절차에 따라 이 문제를 해결하십시오.

1. 끝점의 policyfetcher 섹션에서 policyfetcher_enabled 구성 설정의 값이 1 인지 확인합니다.

   이 구성 설정에서 값 1 은 policyfetcher 를 실행하도록 지정합니다. policyfetcher 가 실행 중이지 않은 경우 CA Access Control 데이터베이스에서 업데이트된 변수를 확인할 수 없습니다.

2. 다음과 같이 시스템 설정을 변경한 이후에 policyfetcher 가 하트비트를 보냈는지 확인하십시오.

   a. CA Access Control 엔터프라이즈 관리에서 "월드 뷰"를 클릭한 다음 "월드 뷰" 작업을 클릭합니다.

      검색 화면이 나타납니다.

   b. 필요한 경우 검색 기준을 정의하여 특정 데이터 하위 집합을 검색하고 "실행"을 클릭합니다.

      정의한 기준과 일치하는 결과가 범주별로 표시됩니다.

   c. "마지막 상태" 열의 업데이트 시간이 시스템 설정을 변경한 시간 이후인지 확인합니다.

      끝점에 대한 "마지막 상태" 열의 업데이트 시간이 시스템 설정을 변경한 시간 이전인 경우 policyfetcher 가 하트비트를 보내지 않았으며 업데이트된 변수 값을 아직 확인하지 않은 것입니다.

      참고: endpoint_heartbeat 구성 설정을 변경하여 하트비트 간격을 변경할 수 있습니다.

3. CA Access Control 을 다시 시작하고 시스템 설정이 변경되었는지 확인합니다.

DNSDOMAINNAME 변수에 값이 없음

증상

기본 제공되는 <!DNSDOMAINNAME> 변수에 값이 없습니다.

해결 방법

끝점에 DNS 도메인이 있는지 확인하십시오.

Windows 끝점에 DNS 도메인이 있는지 확인하려면 다음을 수행하십시오.

1. 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   ipconfig/all
   ```

2. 주 DNS 접미사가 올바른 값으로 설정되었는지 확인합니다.

UNIX 끝점에 DNS 도메인이 있는지 확인하려면 /etc/resolv.conf 파일을 열고 도메인이 올바른 값으로 설정되어 있는지 확인하십시오.

DOMAINNAME 변수에 값이 없음

증상

기본 제공되는 <!DOMAINNAME> 변수에 값이 없습니다.

해결 방법

끝점이 도메인에 연결되어 있는지 확인하십시오.

Windows 끝점이 도메인에 연결되어 있는지 확인하려면 다음을 수행하십시오.

1. "내 컴퓨터"를 마우스 오른쪽 단추로 클릭하고 "속성"을 클릭한 다음 "컴퓨터 이름" 탭을 클릭하고 "변경"을 클릭합니다.
2. "도메인" 필드에 도메인이 표시되는지 확인합니다.

UNIX 끝점이 도메인에 연결되어 있는지 확인하려면 다음을 수행하십시오.

1. 다음 명령을 실행합니다.

   ```
   ypcats hosts
   ```

2. 끝점이 NIS 도메인에 연결되어 있는지 확인하십시오.

HOSTNAME 변수에 값이 없음

증상

기본 제공되는 <!HOSTNAME> 변수에 값이 없거나 정규화된 이름이 사용되지 않았습니다.

해결 방법

끝점에 정규화된 호스트 이름이 있는지 확인하십시오.

Windows 끝점에 정규화된 호스트 이름이 있는지 확인하려면 다음을 수행하십시오.

1. 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   ipconfig/all
   ```

2. 주 DNS 접미사가 올바른 값으로 설정되었는지 확인합니다.

UNIX 끝점이 도메인에 연결되어 있는지 확인하려면 다음 파일에서 호스트 이름이 정의되어 있고 정규화된 이름이 사용되었는지 확인하십시오.

- /etc/hosts
- /etc/resolv.conf

HOSTIP 변수에 값이 없음

증상

기본 제공되는 <!HOSTIP> 변수에 값이 없거나 끝점에 대한 모든 IP 주소가 없습니다.

해결 방법

끝점에 IP 주소가 있는지 확인하십시오.

Windows 끝점에 IP 주소가 있는지 확인하려면 다음을 수행하십시오.

1. 명령 프롬프트를 열고 다음 명령을 실행합니다.

   ```
   ipconfig/all
   ```

2. IP 주소가 올바른지 확인합니다.

UNIX 끝점에 IP 주소가 있는지 확인하려면 다음을 수행하십시오.

1. 다음 명령을 실행합니다.

   ```
   ifconfig -a
   ```

2. IP 주소가 올바른지 확인합니다.

운영 체제 변수에 값이 없음

증상

끝점에 있는 위치를 가리키도록 CA Access Control 운영 체제 변수를 정의했습니다. 이 변수를 정책에 있는 규칙에 사용하면 운영 체제 변수에 값이 없으므로 CA Access Control 이 이 규칙을 시행하지 않습니다.

해결 방법

끝점에서 운영 체제에 환경 변수가 있는지 확인하십시오.

운영 체제에 변수가 있는지 확인하려면

1. CA Access Control 변수가 운영 체제 변수(OSVAR 유형)로 정의되어 있는지 확인합니다.
2. 다음과 같이 운영 체제에 운영 체제 변수가 있는지 확인합니다.
   - (Windows) 명령 프롬프트 창을 열고 다음 명령을 실행합니다.

     ```
     set
     ```

   - (UNIX) 명령 프롬프트 창을 열고 다음 명령을 실행합니다.

     ```
     env
     ```

     참고: 이 명령을 실행하려면 root 사용자여야 합니다.

레지스트리 변수에 값이 없음

Windows 에 해당

증상

끝점에 있는 위치를 가리키도록 CA Access Control 레지스트리 변수를 정의했습니다. 이 변수를 정책에 있는 규칙에 사용하려고 하면 레지스트리 변수에 값이 없으므로 CA Access Control 이 이 규칙을 시행하지 않습니다.

해결 방법

레지스트리 변수(REGVAL 유형 변수)는 REG_SZ 또는 REG_EXPAND_SZ 레지스트리 유형을 가리켜야 합니다. 레지스트리 변수에 지정된 레지스트리 값이 REG_SZ 또는 REG_EXPAND_SZ 유형인지 확인합니다.

제 8 장: 감사 레코드 수집

이 섹션은 다음 항목을 포함하고 있습니다.

수집 서버가 일부 감사 로그 메시지를 받지 못함

UNIX 에 해당

증상:

로컬 감사 로그를 중앙 로그 수집 서버로 전달하도록 CA Access Control 의 끝점을 구성했지만 서버가 일부 감사 로그를 받을 수 없습니다. selogrd 가 감사 레코드를 내보내고 selogrcd 가 감사 레코드를 수집하도록 구성했습니다.

해결책:

CA Access Control 로그 라우팅 시스템의 송신기 데몬인 selorgd 의 문제를 해결하려면 다음을 수행하십시오.

- selogrd.cfg 파일을 검토합니다. 이 파일은 CA Access Control 이 중앙 로그 수집기로 어떤 감사 메시지를 라우팅할지 여부를 결정합니다.

- 각 끝점에서 감사 로그를 검토합니다. 감사 로그에 감사 이벤트가 없으면 audit.cfg 파일을 검토하십시오. audit.cfg 파일은 CA Access Control 이 감사 로그에 어떤 감사 이벤트를 기록할지 여부를 결정합니다. audit.cfg 파일이 CA Access Control 이 감사 이벤트를 감사 로그에 기록하는 것을 방지하는 경우 감사 이벤트가 라우팅되지 않습니다.
- 로그 라우팅 시스템의 송신기 데몬인 selogrd 를 구성하여 디버그 메시지를 출력한 다음 문제를 재현합니다. selogrd 이 디버그 메시지를 출력하도록 구성하려면 다음 명령을 사용하십시오.

  ```
  selogrd -d
  ```

수집 서버가 감사 로그 메시지를 받지 못함

UNIX 에 해당

증상:

로컬 감사 로그를 중앙 로그 수집 서버로 전달하도록 CA Access Control 의 끝점을 구성했지만 서버가 어떠한 감사 로그도 받을 수 없습니다. selogrd 가 감사 레코드를 내보내고 selogrcd 가 감사 레코드를 수집하도록 구성했습니다.

해결책:

selogrcd 가 로그 수집 서버에서 실행 중인지 확인하십시오.

참고: selogrcd 가 오랫동안 실행되지 않으면 끝점이 감사 이벤트를 삭제할 수 있습니다.

SID 해석 실패(이벤트 뷰어 경고)

Windows 에 해당

증상

Windows 이벤트 뷰어의 응용 프로그램 로그에 특정 SID 를 계정 이름으로 해석하지 못했다는 CA Access Control 의 경고 이벤트가 있습니다.

해결 방법

*SID(보안 식별자)*는 운영 체제에 대해 사용자 또는 그룹을 식별하는 숫자 값입니다. DACL(시스템 액세스 제어 목록)에 있는 각 항목은 액세스가 허용, 거부 또는 감사되는 사용자 또는 그룹을 식별하는 SID 가 있습니다.

이 경고는 운영 체제가 SID 를 계정 이름으로 변환하지 못할 때(예: SID 가 참조하는 사용자 또는 그룹이 더 이상 존재하지 않는 경우) 표시됩니다. 문제가 있는 시스템과 그 도메인 컨트롤러가 SID 를 해석할 수 있도록 올바로 구성되어 있는지 확인하십시오.

SID 해석 제한 시간 초과(이벤트 뷰어 경고)

Windows 에 해당

증상

Windows 이벤트 뷰어의 응용 프로그램 로그에 특정 SID 를 계정 이름으로 해석하는 동안 제한 시간을 초과했다는 CA Access Control 의 경고 이벤트가 있습니다.

해결 방법

*SID(보안 식별자)*는 운영 체제에 대해 사용자 또는 그룹을 식별하는 숫자 값입니다. DACL(시스템 액세스 제어 목록)에 있는 각 항목은 액세스가 허용, 거부 또는 감사되는 사용자 또는 그룹을 식별하는 SID 가 있습니다.

이 경고는 운영 체제가 정의된 제한 시간 내에 SID 를 계정 이름으로 변환하지 못할 때 표시됩니다. 다음을 확인하십시오.

- 문제가 있는 시스템과 그 도메인 컨트롤러가 SID 를 해석할 수 있도록 올바로 구성되어 있는지 여부
- 네트워크 설정이 올바로 구성되어 있는지 여부

또한 다음 레지스트리 키에서 DefLookupTimeout 구성 설정을 변경하여 제한 시간을 늘릴 수 있습니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\SeOSD
```

참고: SID 해석 제한 시간을 늘리면 CA Access Control 의 성능이 저하될 수 있습니다.

selogrd 를 시작하려고 할 때 오류 코드 4631 을 받음

UNIX 에 해당

증상:

selogrd 를 시작하려고 시도합니다. selogrd 가 시작되지 않고 다음 오류 메시지를 받습니다.

`/opt/CA/AccessControl/bin/selogrd 을(를) 초기화하는 동안 4631 (0x1217) 오류가 발생했습니다.`

해결책:

selogrd 를 시작하기 전에 로컬 호스트 이름을 확인하십시오. 호스트 이름을 확인하려면 호스트 이름을 운영 체제 호스트 파일에 추가하거나 호스트 이름을 NIS 또는 DNS 에 정의하십시오.

감사 파일 크기가 2 GB 를 초과하는 경우 감사 로깅이 중단됨

증상:

감사 파일 크기가 2 GB 를 초과하면 CA Access Control 이 감사 레코드를 감사 파일에 기록하는 것을 중단합니다.

해결책:

CA Access Control 은 감사 파일의 크기가 2 GB 를 초과하는 경우 감사 파일에 감사 레코드를 기록할 수 없습니다. CA Access Control 감사 파일의 최대 크기는 logmgr 섹션의 audit_size 구성 설정에서 KB 단위로 지정됩니다.

seos.audit 파일의 최대 크기를 2 GB 로 설정하려면 logmgr 섹션의 audit_size 구성 설정의 값을 2097151 로 설정하십시오.

CA Access Control 이 감사 로그에 기록할 때 시스템이 느려짐

증상:

CA Access Control 이 감사 로그에 기록할 때 컴퓨터가 느려집니다.

해결책:

CA Access Control 이 감사 및 추적 데이터를 기록하는 동안 시스템에서 대부분의 프로세스가 잠길 수 있습니다. CA Access Control 이 감사 데이터 및 추적 데이터를 기록할 때 소요되는 시간을 줄이려면 다음을 수행하십시오.

- 필요한 리소스 및 액세스에 대한 감사 모드만 설정합니다.
- 필요한 경우에만 추적을 엽니다.
- 감사 파일, 추적 파일 및 CA Access Control 데이터베이스 파일을 가장 빠르게 사용할 수 있는 파일 시스템에 저장합니다.

호스트에 여러 IP 주소가 할당되면 필터가 적용되지 않음

증상

호스트 이름을 사용하여 여러 IP 주소가 할당된 호스트에서 TCP 이벤트를 필터링하도록 audit.cfg 를 구성했습니다. 필터를 적용한 후 모든 IP 주소에 대한 TCP 로그를 볼 수 없습니다.

해결 방법

audit.cfg 필터를 적용할 때 감사 시스템은 호스트 이름을 호스트의 IP 주소로 확인하고 호스트 IP 주소를 호스트 이름으로 확인합니다. 여러 IP 주소로 호스트를 구성하면 audit.cfg 는 첫 번째 IP 주소만 필터링합니다.

모든 IP 주소에 audit.cfg 필터를 적용하려면 다음과 같이 호스트 이름이 아닌 필터에만 모든 IP 주소를 지정하십시오.

```
TCP;*;192.168.30.138;*;R;P
TCP;*;192.168.30.139;*R;P
```

제 9 장: 성능 튜닝

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control 이 실행될 때 성능이 저하됨

증상:

CA Access Control 이 실행될 때 컴퓨터가 느려집니다. CA Access Control 을 중지하면 컴퓨터 성능이 정상으로 돌아옵니다.

해결책:

성능 문제를 진단하여 수정하려면 성능 문제를 해결 (페이지 122)하십시오.

CA Access Control 서버의 시스템 로드가 너무 많음

증상:

CA Access Control 서버의 시스템 로드를 줄여야 합니다.

해결책:

시스템 로드를 줄이려면 다음을 수행하십시오.

- 데이터베이스에서 계층을 너무 깊게 만들지 마십시오.

  사용자 및 리소스의 계층 구조를 복잡하게 구성하면 모든 종속성을 가져오거나 확인하기 위해 시스템 로드가 필요합니다.

- 자주 사용하는 디렉터리에 대한 일반 규칙을 만들지 마십시오.

  자주 사용하는 디렉터리에 대한 일반 규칙을 정의하면 CA Access Control 이 많은 시스템 작업을 검사합니다. 예를 들어, /usr/lib/*를 보호하는 일반 보호 규칙을 만들면 CA Access Control 이 시스템의 모든 작업을 검사합니다.

- (Solaris 에만 해당) 파일이 프로세스 파일 시스템(/proc)에 속한 경우 CA Access Control 이 파일 액세스 검사를 건너뛰도록 지정하십시오.

  파일이 프로세스 파일 시스템에 속한 경우 CA Access Control 이 파일 액세스 검사를 건너뛰도록 지정하려면 seos.ini 파일의 [SEOS_syscall] 섹션에 있는 proc_bypass 구성 설정의 값이 1 인지 확인하십시오.

  참고: seos.ini 파일 토큰에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

제 10 장: UNAB 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

UNAB 설치 실패

증상

설치 패키지를 사용자 지정했는데 끝점에 UNAB 를 설치하려고 하면 설치가 실패합니다.

해결 방법

다음 절차에 따라 문제를 해결하십시오.

1. UNAB 설치 로그 파일인 uxauth_install.log 에서 오류를 검토합니다. 기본적으로 파일은 다음 디렉터리에 있습니다.

   ```
   /opt/CA/uxauth
   ```

2. UNAB 설치 로그 파일을 내보낸 다음 이 파일을 CA Support 로 보냅니다.
3. 디버그 모드에서 설치 프로세스를 실행합니다.
   - 네이티브 패키지 설치의 경우 /tmp 디렉터리에 seos_debug_on 이란 이름으로 파일을 만든 다음 이 파일에 0-9 사이의 디버그 수준을 할당합니다.
4. 디버그 모드에서 네이티브 패키지를 실행합니다.
   - AIX: 설치 명령에 -e<*log_file_name*> 플래그를 추가합니다.
   - HP-UX: swinstall 이 swjob 에 대해 생성하는 설치 로그 파일을 검토합니다.
   - Linux: -vv 플래그를 설치 명령에 추가합니다.
   - Solaris: -v 플래그를 설치 명령에 추가합니다.

UNAB 등록 문제 해결

다음 절은 Active Directory 에 UNAB 를 등록할 때 발생하는 문제를 해결하는 데 사용할 수 있는 정보를 수록하고 있습니다.

잘못된 암호로 인해 UNAB 등록 실패

증상

Active Directory 에 UNAB 를 등록할 때 다음 오류 메시지와 함께 등록이 실패합니다.

최초 자격 증명을 가져오는 동안 사전 인증이 실패했습니다. <Administrator>을(를) 사용한 Kerberos 사전 인증이 실패했습니다.

해결 방법

잘못된 관리자 암호로 인해 UNAB 등록이 실패했습니다. 이 문제를 해결하려면 관리자 암호를 확인하고 UNAB 를 등록하십시오.

잘못된 클록 차이로 인해 UNAB 등록 실패

증상

Active Directory 에 UNAB 를 등록할 때 다음 오류 메시지가 표시됩니다.

최초 자격 증명을 받는 동안 클록 차이가 너무 큽니다. Administrator>을(를) 사용한 Kerberos 사전 인증이 실패했습니다.

해결 방법

Active Directory 와 UNAB 끝점 사이의 클록 차이가 구성 값보다 커서 UNAB 등록이 실패했습니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. UNAB 끝점 클록을 Active Directory 의 클록과 수동으로 동기화합니다.
2. 시간 동기화를 자동으로 구성하기 위해 uxauth.ini 의 [Agent] 섹션 아래에서 use_time_sync 토큰 값을 yes 로 설정합니다.

잘못된 NTP 서버 구성으로 인해 UNAB 등록 실패

증상

Active Directory 에 UNAB 를 등록할 때 다음 오류 메시지가 표시됩니다.

경고: NTP 서비스 위치가 잘못 지정되었습니다.

해결 방법

NTP(Network Time Protocol) 서버가 잘못 구성되어 UNAB 등록이 실패했습니다.

이 문제를 해결하려면 uxauth.ini 의 [Agent] 섹션 아래에서 ntp_server 토큰을 NTP 서버를 가리키도록 설정하십시오.

잘못된 구성으로 인해 UNAB 등록 실패

증상

Active Directory 에서 UNAB 를 등록할 때 다음 오류 메시지가 표시됩니다.

Kerberos 5 라이브러리를 초기화하는 동안 오류가 발생했습니다. '/opt/CA/uxauth/uxauth.ini'를 확인하십시오. <Administrator>을(를) 사용한 Kerberos 사전 인증이 실패했습니다.

증상

uxauth.ini 파일에 잘못된 Kerberos 값이 수록되어 있어 UNAB 등록이 실패했습니다.

이 문제를 해결하려면 uxpreinstall 유틸리티를 실행하여 Kerberos 구성을 확인하십시오.

누락된 DNS 설정으로 인해 UNAB 등록 실패

증상

Active Directory 에 UNAB 를 등록할 때 다음 오류 메시지가 표시됩니다.

<domain_name> 도메인에서 LDAP 서비스에 대한 RR 을 찾을 수 없습니다.

해결 방법

DNS 설정이 Active Directory 에서 구성되지 않아 UNAB 등록이 실패했습니다. 이 문제를 해결하려면 다음을 수행하십시오.

1. uxpreinstall 유틸리티를 실행하여 DNS 설정을 확인합니다.
2. uxpreinstall 유틸리티의 출력을 검토하여 DNS 설정을 파악합니다.
3. 잘못된 경우 다음 파일에서 DNS 설정을 업데이트합니다.

   /etc/resolv.conf

uxconsole -register 실패

UNIX 에 해당

증상

UNAB 끝점을 등록하기 위해 uxconsole -register 를 실행하면 다음 오류 메시지가 표시됩니다.

```
Active Directory 와의 통신을 위해 DC 로 사용할 수 있는 서버가 없습니다.
[ad] 섹션에서 lookup_dc_list 및 ignore_dc_list 토큰을 확인하십시오.
```

해결 방법

uxconsole 이 UNAB 끝점을 Active Directory 에 등록할 때는 끝점의 실제 위치에 가장 가까운 Active Directory 사이트가 검색됩니다. 하지만 uxauth.ini 파일의 ad 섹션에 있는 ignore_dc_list 구성 설정은 UNAB 끝점이 통신하지 않는 도메인 컨트롤러를 나열합니다. 검색된 Active Directory 사이트의 모든 도메인 컨트롤러가 ignore_dc_list 구성 설정에 나열된 경우 등록이 실패합니다.

이 문제를 해결하려면 검색된 Active Directory 사이트에 있는 모든 도메인 컨트롤러의 이름을 ignore_dc_list 구성 설정에서 삭제하고 uxconsole 유틸리티를 다시 실행하십시오.

참고: uxconsole 유틸리티는 검색된 Active Directory 사이트의 이름을 uxauth.ini 파일의 ad 섹션에 있는 ad_site 구성 설정에 기록합니다. UNAB Active Directory 사이트 지원에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

UNAB 로그인 정책이 배포되지 않음

증상

UNAB 로그인 정책을 UNAB 끝점에 배포하려고 했지만 정책이 배포되지 않았습니다.

해결 방법

이 문제를 해결하려면 다음을 수행하십시오.

1. UNAB 가 끝점에서 실행 중인지 확인합니다.
   a. 끝점에서 명령 프로그램 창을 엽니다.
   b. 다음 명령을 실행합니다.

      ```
      ./uxauthd.sh status
      ```

   UNAB 의 현재 상태를 알리는 메시지가 나타납니다.
2. 정책이 호스트에 다운로드되었는지 확인합니다.
   a. 끝점에서 명령 프롬프트 창을 열고 다음 명령을 실행합니다.

      ```
      ./uxconsole -status -detail
      ```

   끝점에 배포된 경우 이 정보에는 정책 이름이 포함되어 있습니다.
3. 엔터프라이즈 관리 서버가 UNAB 끝점으로 보낸 정책 권한 부여 명령을 검토합니다.
   - 끝점에서 명령 프롬프트 창을 열고 다음 명령을 실행합니다.

     ```
     ./uxaudit -a
     18 Jan 2011 11:03:23 S UPDATE_____ TERMINAL__ ac_entm_pers_ 338 10
     _default___________ acmanager.forwardinc.com auth terminal _default
     xuid(yaeyu01)access(read) (OS user)
     ```

   규칙이 수정되지 않았는지 확인합니다.
4. syslog 파일에서 메시지 큐 통신 오류를 찾습니다.
5. 사용자 계정에서 로그인 권한 및 상태를 확인합니다.
6. 명령 프롬프트 창에서 다음 명령을 실행합니다.

   ```
   uxconsole –manage –show –user <AD_user_account>
   ```

ReportAgent 가 엔터프라이즈 관리 서버로 보고서를 보내지 않음

증상

UNAB 를 시작하고 ReportAgent 데몬이 실행 중임을 확인했지만 CA Access Control 엔터프라이즈 관리에서 보고서를 볼 수 없습니다.

해결 방법

다음 절차에 따라 이 문제를 해결하십시오.

1. syslog 의 'UNAB EP communication problems with ENTM' 섹션에서 메시지 큐 서버 통신 관련 오류 메시지를 확인합니다.
2. 보고서 데이터를 CA Enterprise Log Manager 로 보내려는 경우, accommon.ini 파일의 [ReportAgent] 섹션에 있는 audit_enabled 토큰이 1 로 설정되어 있는지 확인합니다.
3. ReportAgent 디버깅을 활성화합니다.
4. accommon.ini 파일의 [ReportAgent] 섹션에 있는 디버그 토큰을 1 로 설정합니다.
5. UNAB 보고서 디버그 파일인 unab2xml.log 를 검토합니다. 이 파일은 다음 디렉터리에 있습니다.

   ```
   /opt/CA/AccessControlShared/log
   ```

6. 직접 ReportAgent 를 실행하여 UNAB 데이터베이스 스냅숏을 생성합니다.

   ```
   /opt/CA/AccessControlShared/bin/ReportAgent -debug 0 -task 2 –now
   ```

   다음에 주의하십시오.

   - ReportAgent 를 직접 실행하기 전에 '/opt/CA/AccessControlShared/lob' 경로를 $LD_LIBRARY_PATH 에 추가하십시오.
   - ReportAgent 를 직접 실행하기 전에 /opt/CA/AccessControlShared/data/audit2txt/ 디렉터리에서 .dat 파일을 제거하십시오.
   - ReportAgent 유틸리티 디버그 모드에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

UNAB 호스트를 등록할 때 Kerberos 사전 인증 실패

UNIX 에 해당

증상

uxconsole -register 명령을 사용할 때 다음 오류 메시지가 표시됩니다.

krb5_set_config_files 가 /opt/CA/uxauth/uxauth.ini 에 대해 실패함: 프로필에 여는 중괄호가 없음
<Administrator>를 사용한 Kerberos 사전 인증 실패

해결 방법

uxauth.ini 파일에 설정되지 않은 구성 설정이 있습니다. 이 문제를 해결하려면 uxauth.ini 파일의 각 구성 설정에 값이 있는지 확인하십시오.

UNAB 를 등록 또는 시작할 때 오류 코드 2803 을 받음

UNIX 에 해당

증상

Active Directory 에서 UNAB 호스트를 등록하거나 UNAB 를 시작하려고 하면 다음 오류 메시지가 표시됩니다.

nss 를 열거나 nss 캐시를 만들 수 없습니다. 오류 코드 2803.

해결 방법

/var 디렉터리에 충분한 메모리가 없습니다. 이 문제를 해결하려면 /var 의 95% 미만이 사용되는지 확인하고 명령을 다시 실행하십시오.

Active Directory 사용자가 UNAB 끝점에 로그인할 수 없음

UNIX 에 해당

증상

UNIX 특성이 있는 Active Directory 사용자는 UNAB 끝점에 로그인할 수 없습니다.

해결 방법

이 문제를 해결하려면 다음을 수행하십시오.

1. 사용자의 컨테이너가 다음 중 하나인지 확인하십시오.
   - user_container 구성 설정에 지정된 컨테이너
   - user_container 구성 설정에 지정된 컨테이너 아래의 하위 컨테이너

     참고: user_container 구성 설정은 uxauth.ini 파일의 AD 섹션에 있습니다.
2. 사용자가 Active Directory 에서 UID 및 GID 가 있는지 확인합니다.
3. 사용자가 중지된 사용자가 아닌지 확인합니다.
4. UNAB 가 끝점에서 실행 중인지 확인합니다.
   a. 끝점에서 명령 프로그램 창을 엽니다.
   b. 다음 명령을 실행합니다.

      ```
      ./uxauthd.sh status
      ```

      UNAB 의 현재 상태를 알리는 메시지가 나타납니다.
5. 끝점이 Active Directory 에 등록되었는지 확인합니다.

   참고: 끝점이 Active Directory 에 등록되지 않았으면 uxconsole -register 유틸리티를 사용하여 호스트를 등록하십시오.
6. 다음과 같이 사용하는 OS 에 대한 이름 또는 암호 캐싱 데몬을 끝점에서 중지합니다.
   a. UNAB 를 중지합니다:

      ```
      ./uxauthd.sh stop
      ```
   b. NSS 캐시 데이터베이스를 삭제합니다.

      ```
      rm -rf /opt/CA/uxauth/etc/nss.db
      ```
   c. 사용하는 OS 에 대한 이름 또는 암호 캐싱 데몬이 끝점에서 실행 중인지 확인합니다.

      예를 들어, Linux 또는 Solaris 끝점의 경우 nscd 데몬이 실행 중인지 확인합니다. HP-UX 끝점의 경우 pwgrd 데몬이 실행 중인지 확인합니다.
   d. 사용하는 OS 에 대한 이름 또는 암호 캐싱 데몬이 실행 중인 경우 이 프로세스를 중지(kill)합니다.
   e. UNAB 를 시작합니다:

      ```
      ./uxauthd.sh start
      ```

7. 다른 Active Directory 사용자 계정을 사용하여 TGT(Ticket Granting Ticket)를 획득합니다.

   관리자 계정을 사용하여 다음 명령을 실행하여 Active Directory 에 연결합니다.

   ```
   ./uxconsole -krb -init Administrator
   ```

   참고: 예를 들어, 에이전트 keytab 을 사용하여 TGT 를 획득할 수 있습니다.

   ```
   ./uxconsole -krb -init -k
   ```

8. Active Directory 사용자 계정을 직접 확인합니다.

   - 다음 검색을 실행합니다.

     ```
     ./uxconsole -ldap -search "(&(objectClass=user)(sAMAccountName=johndoe))"
     ```

     예상된 사용자 계정 이름과 실제 사용자 계정 이름 사이의 차이를 확인하십시오.

9. 해당하는 경우 다른 도메인의 사용자 계정을 검색합니다.

   - 다음 명령을 실행합니다.

     ```
     ./uxconsole -ldap -search -b DC=unabca,DC=test,DC=co,DC=il
     "(&(objectClass=user)(objectCategory=person))"
     ```

10. 사용자 계정 UNIX 특성이 Active Directory 및 UNIX 에서 동일한지 확인합니다.

사용자가 UNAB 끝점에서 명령을 실행할 수 없음

증상

UNAB 끝점에 성공적으로 로그인하고 UNAB 가 내 로그인에 해당하는 uxaudit(UNAB 감사 파일)에 P('p'ermitted - 허용됨) 레코드를 만듭니다. 하지만 끝점에서 어떠한 UNIX 명령도 실행할 수 없습니다.

해결 방법

사용자가 이전에 동일한 끝점에 로그인할 때 사용자 이름은 동일한 이름을 사용했지만 UID 는 다른 UID 를 사용했으므로 사용자가 자신의 /home 디렉터리에 액세스할 수 없습니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. 사용자에 대한 /home 디렉터리를 삭제합니다.

   참고: /home 디렉터리는 일반적으로 /home/userName 에 있습니다.

2. 사용자가 끝점에 로그인하도록 요청합니다.

   이 사용자에 대해 새 /home 디렉터리가 만들어집니다. 이제 사용자가 UNAB 끝점에서 UNIX 명령을 수행할 수 있습니다.

월드 뷰에서 UNAB 끝점을 볼 수 없음

UNIX 에 해당

증상

UNAB 끝점을 관리하기 위해 CA Access Control 엔터프라이즈 관리를 사용하는데 UNAB 끝점이 월드 뷰에 표시되지 않습니다.

해결 방법

UNAB 끝점이 배포 서버와 통신할 수 있는지 확인하십시오. UNAB 끝점에서 다음을 수행합니다.

1. Distribution_Server 구성 설정의 값이 배포 서버 컴퓨터의 이름으로 설정되었는지 확인합니다.

   Distribution_Server 구성 설정은 accommon.ini 파일의 통신 섹션에 있습니다.

   예: ssl://ds.comp.com:7243

   참고: 기본적으로 배포 서버는 엔터프라이즈 관리 서버에 있습니다.

2. 메시지 큐 암호가 올바른지 확인하십시오. 끝점은 이 암호를 사용하여 배포 서버와 통신합니다. 다음 작업을 수행하십시오.

   a. 명령 프롬프트 창을 엽니다.

   b. 다음 명령을 실행합니다.

      ```
      acuxchkey -t pwd "password"
      ```

      password

      메시지 큐 암호를 정의합니다. 기본적으로 이 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 정의하는 통신 암호입니다.

3. 다음과 같이 UNAB 에이전트를 다시 시작합니다.

   a. UNAB lbin 디렉터리로 이동합니다.

      기본적으로 이 디렉터리는 /opt/CA/uxauth 에 있습니다.

   b. UNAB 에이전트를 다시 시작합니다:

      ```
      ./uxauthd.sh restart
      ```

4. 다음과 같이 메시지 큐 서버가 실행 중인지 확인합니다.

   - Windows - CA Access Control 메시지 큐 서비스가 실행 중인지 확인합니다.
   - UNIX - tibemsd 프로세스가 실행 중인지 확인합니다.

5. syslog 또는 이벤트 뷰어에서 메시지 큐 서버 통신 오류가 있는지 확인합니다.

6. 메시지 큐 서버가 통신 관련 메시지를 로그 파일에 기록하도록 설정합니다. 다음 작업을 수행하십시오.
   - UNIX:
     a. pmd.ini 파일을 엽니다.
     b. [endpoint_management] 섹션의 debug_mode 토큰을 1 로 수정합니다.
   - Windows:

   a. 다음 레지스트리 키를 탐색합니다.

      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\ DMS_NAME\endpoint_management

   b. debug_mode 토큰 값을 1 로 수정합니다.
7. 변경 사항을 적용하기 위해 엔터프라이즈 관리 서버를 다시 시작합니다. DMS 디렉터리에 있는 endpoint_management.log 파일에서 통신 메시지를 검토합니다.

   UNAB 끝점이 배포 서버와 통신할 수 있음을 확인했습니다.

Linux s390 끝점에서 데몬을 시작할 수 없음

Linux s390 및 Linux s390x 에 해당

증상

uxauthd 또는 ReportAgent 데몬을 시작할 수 없습니다.

해결 방법

UNAB 가 끝점에서 Java 환경을 찾을 수 없습니다. 이 문제를 해결하려면 다음을 수행하십시오.

1. accommon.ini 파일의 전역 섹션에 있는 java_home 구성 설정이 Java 환경에 대한 경로를 포함하는지 확인하십시오.
2. LD_LIBRARY_PATH 환경 변수의 값을 Java 환경의 공유 라이브러리에 대한 경로로 설정하십시오.

사용자가 로그인하거나 암호를 변경할 수 없음

UNIX 에 해당

증상

UNAB 끝점에서 로그인하거나 암호를 변경하려고 시도하면 다음 오류 메시지가 표시됩니다.

```
passwd: 인증 토큰 조작 오류
```

해결 방법

uxauthd 가 암호 변경 요청에 응답할 때까지 기다리는 동안 PAM 모듈이 만료되었습니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. uxauth.ini 파일의 pam 섹션에서 pam_receive_timeout 구성 설정의 값을 늘리십시오.

   예: pam_receive_timeout=100

2. UNAB 를 중지하고 다시 시작합니다.

참고: uxauth.ini 파일에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

제 11 장: PUPM 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

Break Glass 승인 워크플로

증상

사용자 관리자가 아닌, 요청이 적용되는 PUPM 끝점 시스템 관리자에게 통보가 전달되었는지 확인하기 위해 한 단계의 break glass 워크플로를 구성하고 싶습니다.

해결 방법

기본 승인자가 아닌 시스템 관리자가 break glass 요청을 승인하도록 지정하기 위해 한 단계의 break glass 워크플로를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹", "작업", "관리 작업 수정"을 선택합니다.

   "관리 작업 수정: 작업 선택" 검색 창이 열립니다.

2. 풀다운 메뉴에서 "범주"를 선택하고 텍스트 상자 영역에 *home*를 입력합니다. "검색"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 검색 조건에 맞는 작업을 표시합니다.

3. Break Glass WF 작업을 선택한 다음 "선택"을 클릭합니다.

   Break Glass WF 속성 창이 열립니다.

4. "이벤트" 탭으로 이동하여 오른쪽 방향 화살표를 클릭합니다.

   워크플로 매핑 창이 열립니다.

5. "워크플로 프로세스" 풀다운 메뉴에서 SingleStepApproval 을 선택합니다.

6. "기본 승인자" 섹션에서 다음을 수행합니다.

   a. "승인 작업" 풀다운 메뉴에서 "Break Glass 권한 있는 계정 승인"을 선택합니다.

   b. "참여자 해결 프로그램" 풀다운 메뉴에서 "사용자 지정: PrivilegedAccountOwnerResolver"를 선택합니다.

      참여자 해결 프로그램 구성 매개 변수가 설정되지 않았음을 알리는 메시지가 표시됩니다.

   c. "새 매개 변수 이름" 텍스트 상자에서 SourceObject 를 지정합니다.

   d. "값" 텍스트 상자에서 TaskAdmin 을 지정합니다.

e. "매개 변수 추가"를 클릭합니다.

CA Access Control 엔터프라이즈 관리가 승인자 작업을 추가합니다.

f. 다음 매개 변수 이름과 값을 사용하여 c 에서 e 단계를 반복합니다.

- SourceObjectAttribute - tblUser.manager
- TargetType - USER

7. "확인"을 클릭합니다.

한 단계의 break glass 워크플로를 구성했고 시스템 관리자를 승인자로서 정의했습니다.

RunAs 암호 소비자 요청 만료

Windows 에 해당

증상

사용자가 RunAs 유틸리티를 실행하여 작업을 수행하도록 Windows RunAs 암호 소비자를 구성하고 있습니다. 사용자가 RunAs 유틸리티를 실행하면 암호 요청이 만료되고 사용자가 유틸리티를 실행할 수 없습니다.

해결 방법

이 문제를 해결하려면 다음 레지스트리 항목의 값을 늘리십시오.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\plug
ins\RunAsPlg\CommunicationWaitTimeout
```

이 레지스트리 항목은 암호 소비자가 PUPM 에이전트로부터 응답을 기다리는 시간(초)을 지정합니다.

예: CommunicationWaitTimeout 레지스트리 항목의 값 변경

다음 예는 CommunicationWaitTimeout 레지스트리 항목의 값을 30 으로 늘립니다:

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\RunAsPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
토큰을 성공적으로 설정했습니다.
```

ODBC, OLEDB, OCI 데이터베이스 암호 소비자 요청 시간 만료

Windows 에 해당

증상

끝점에서 ODBC, OLEDB, OCI 데이터베이스 암호 소비자를 구성하고 있습니다. 암호 소비자는 끝점의 응용 프로그램이 데이터베이스에 연결할 때 암호를 요청합니다. 하지만 응용 프로그램이 데이터베이스에 연결을 시도하면 암호 요청 시간이 만료됩니다.

해결 방법

이 문제를 해결하려면 다음 레지스트리 항목의 값을 늘리십시오.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plug
ins\plugin\CommunicationWaitTimeout
```

plugin

연결 시도를 가로채는 플러그 인의 이름을 지정합니다.

값: OCIPlg, ODBCPlg, OLEDBPlg

이 레지스트리 항목은 암호 소비자가 PUPM 에이전트로부터 응답을 기다리는 시간(초)을 지정합니다.

예: CommunicationWaitTimeout 레지스트리 항목의 값 변경

다음 예는 OCI 데이터베이스 암호 소비자에 대해 CommunicationWaitTimeout 레지스트리 항목의 값을 30 으로 늘립니다.

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\OCIPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
토큰을 성공적으로 설정했습니다.
```

PUPM SSH 장치 시간 만료

Red Hat 5 에 해당

증상

일본어 Red Hat 5 를 PUPM SSH 장치 끝점으로 구성하고 운영 관리자 사용자 로그인 및 운영 관리자 암호를 사용하도록 지정한 이후에 끝점 작업 생성이 만료됩니다.

해결 방법

이 문제를 해결하려면 다음을 수행하십시오.

1. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

   ```
   ACServerInstallDir/Connector Server/conf/override/sshdyn
   ```

2. 편집을 위해 ssh_connector_conf.xml 파일을 엽니다.
3. <array name="oChangePassword"> 아래에 다음 항목을 추가합니다.

   ```
   <item>
       <param name="sCommand" value="set LANG=C" />
       <param name="iWait" value="500" />
       </item>
   ```

4. 파일을 저장한 후 닫습니다.

승인 워크플로가 트리거되지 않고 요청한 암호를 체크 아웃할 수 있음

SunOne 에 해당

증상

권한 있는 계정 암호에 대한 요청을 입력한 후에 매니저가 먼저 이 요청을 승인하지 않고도 암호를 체크 아웃할 수 있습니다.

해결 방법

기본적으로 SunOne 사용자 디렉터리를 사용하여 엔터프라이즈 관리 서버를 설치하면 워크플로 지원이 비활성화됩니다. 권한 있는 계정 암호에 대한 요청을 제출하도록 사용자를 지원하려면 워크플로를 활성화해야 합니다.

SunOne 디렉터리에 대한 워크플로 지원을 활성화하려면 다음을 수행하십시오.

1. 이미 수행하지 않은 경우 CA Identity Manager 관리 콘솔을 활성화합니다.
2. CA Identity Manager 관리 콘솔을 엽니다.
3. "환경", "ac-env", "고급 설정", "워크플로"를 선택합니다.

   워크플로 속성 창이 열립니다.
4. "사용" 필드 옆의 확인란을 선택합니다.
5. "저장"을 선택한 다음 "다시 시작"을 선택하여 환경을 다시 시작합니다.

   SunOne 디렉터리에 대한 워크플로 지원을 활성화했습니다.

Windows Agentless 끝점을 만들 때 액세스 거부 메시지가 표시됨

Windows 7 Enterprise Edition 에 해당

증상

Windows 7 끝점을 Windows Agentless 끝점 유형으로 정의하려고 하면 "액세스 거부됨" 메시지가 표시되고 프로세스가 실패합니다.

해결 방법

지정한 계정이 Administrator 계정이 아니지만 Administrators 그룹의 구성원이기 때문에 끝점 생성 프로세스가 실패합니다.

이 문제를 해결하려면 다음을 수행하십시오.

1. Administrators 그룹의 구성원으로서 관리할 끝점에 로그인합니다.
2. "제어판", "사용자 계정", "사용자 계정 제어 설정 변경"을 선택합니다.

   "사용자 계정 제어 설정" 창이 열립니다.
3. 알림 수준을 "기본"으로 설정한 다음 "확인"을 클릭합니다.

   변경 사항이 반영되도록 컴퓨터를 다시 시작해야 할 수 있습니다.
4. "관리 도구", "컴퓨터 관리", "서비스 및 응용 프로그램"을 선택합니다.
5. "WMI 컨트롤"을 마우스 오른쪽 단추로 클릭한 다음 "속성"을 선택합니다.

   WMI 컨트롤 속성 창이 열립니다.
6. "보안" 탭으로 이동합니다.

   네임스페이스 탐색 창이 열립니다.
7. "Root"를 선택한 다음 "Security"를 선택합니다.

   보안 대화 상자가 열립니다.
8. "그룹 또는 사용자 이름" 섹션에서 "Authenticated User"를 선택합니다.
9. "허용" 열에서 "메서드 실행" 확인란의 선택을 지웁니다.
10. [확인]을 눌러 변경 사항을 적용합니다.

제 12 장: 보고 서비스 문제 해결

이 섹션은 다음 항목을 포함하고 있습니다.

보고 서비스의 문제 해결 방법

CA Access Control 보고 서비스를 사용하면 한 위치에서 각 끝점(사용자, 그룹 및 리소스)의 보안 상태를 볼 수 있습니다. 보고 서비스의 문제를 해결할 때는 차례로 각 구성 요소를 검사합니다.

다음 프로세스는 보고 서비스의 문제를 해결하는 데 도움을 줍니다.

1. 끝점의 운영 체제에 적절한 다음 작업 중 *하나*를 수행합니다.
   - UNIX 컴퓨터에서 보고서 에이전트 문제 해결 (페이지 99)
   - Windows 컴퓨터에서 보고서 에이전트 문제 해결 (페이지 103)
2. 배포 서버의 문제를 해결합니다 (페이지 106).
3. JBoss 의 문제를 해결합니다 (페이지 108).
4. 보고서 포털의 문제를 해결합니다 (페이지 109).

UNIX 컴퓨터에서 보고서 에이전트 문제 해결

UNIX 에 해당

보고서 에이전트는 끝점에 있는 모든 정책 모델 데이터베이스(PMDB)와 로컬 CA Access Control 데이터베이스의 예약된 스냅숏을 수집하여 이 스냅숏을 XML 형식으로 배포 서버에 있는 보고서 큐로 전달합니다.

참고: 보고서 에이전트는 다른 작업도 수행합니다. 보고서 에이전트에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

UNIX 컴퓨터에서 보고서 에이전트의 문제를 해결하려면

1. 라이브러리 경로 환경 변수가 올바로 설정되었는지 확인합니다. 다음 작업을 수행하십시오.
   a. root 로 su 를 실행합니다.
   b. 라이브러리 경로 환경 변수를 *ACSharedDir*/lib 로 설정합니다. 기본적으로 *ACSharedDir* 는 다음 디렉터리입니다.

      ```
      /opt/CA/AccessControlShared
      ```

   c. 라이브러리 경로 환경 변수를 내보냅니다.
2. 다음 구성 설정이 올바른지 확인합니다. 이 구성 설정은 accommon.ini 파일의 [ReportAgent] 섹션에 있습니다.

   참고: 구성 설정의 값을 확인하기 위해 CA Access Control 끝점 관리 또는 selang 명령을 사용할 수 있습니다. 하지만 이 절차의 경우 구성 환경에서 selang 명령을 사용하여 구성 설정의 값을 변경하는 것이 좋습니다. selang 명령을 사용하면 CA Access Control 을 중지한 후 다시 시작할 필요 없이 이 절차에서 구성 설정을 변경할 수 있습니다.

   reportagent_enabled

   로컬 컴퓨터에서 보고를 활성화할지 여부를 지정합니다(1).

   기본값: 0

   중요! 보고서 에이전트가 자동으로 실행되도록 하려면 이 구성 설정의 값을 1 로 설정해야 합니다. 이 구성 설정의 값을 0 으로 설정하면 보고서 에이전트가 데이터베이스의 예정된 스냅숏을 배포 서버로 전달하지 않습니다. 하지만 이 구성 설정의 값이 0 인 경우에도 보고서 에이전트를 디버그 모드에서 실행할 수 있습니다.

   schedule

   보고서를 만들어 배포 서버로 보낼 일정을 정의합니다.

   이 설정은 time@day[,day2][...] 형식으로 지정할 수 있습니다.

   기본값: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   예: "19:22@Sun,Mon"을 지정하면 일요일과 월요일마다 오후 7:22 에 보고서가 생성됩니다.

send_queue

보고서 에이전트가 로컬 데이터베이스의 스냅숏을 보내는 배포 서버에 있는 메시지 큐의 이름을 정의합니다.

Default: queue/snapshots

중요! 이 구성 설정의 기본 값을 변경하지 마십시오.

3. 다음 구성 설정이 올바른지 확인합니다. 이 구성 설정은 accommon.ini 파일의 [communication] 섹션에 있습니다.

   참고: 구성 설정의 값을 확인하기 위해 CA Access Control 끝점 관리 또는 selang 명령을 사용할 수 있습니다. 하지만 이 절차의 경우 구성 환경에서 selang 명령을 사용하여 구성 설정의 값을 변경하는 것이 좋습니다. selang 명령을 사용하면 CA Access Control 을 중지한 후 다시 시작할 필요 없이 이 절차에서 구성 설정을 변경할 수 있습니다.

   Distribution_Server

   배포 서버 URL 을 정의합니다.

   참고: TCP 통신을 위한 기본 포트는 7222 이고 SSL 통신을 위한 기본 포트는 7243 입니다. 배포 서버 URL 이 통신 유형에 대한 올바른 포트 번호를 지정하는지 확인해야 합니다.

   기본값: none

   예: ssl://172.24.176.145:7243. 이 URL 은 보고서 에이전트가 SSL 프로토콜을 사용하여 7243 포트에서 IP 주소 172.24.176.145 로 배포 서버와 통신하도록 구성합니다.

4. seos.ini 파일의 [daemons] 섹션에 다음 줄이 있는지 확인합니다.

   ```
   ReportAgent = yes, ACSharedDir/lbin/report_agent.sh start
   ```

   이 줄은 CA Access Control 이 시작될 때 보고서 에이전트 데몬이 자동으로 실행되지 않도록 합니다.

   참고: 기본적으로 *ACSharedDir* 디렉터리는 /opt/CA/AccessControlShared 에 있습니다.

5. CA Access Control 을 중지합니다.

   ```
   secons -s
   ```

   CA Access Control 과 보고서 에이전트가 중지됩니다.

6. 다음 디렉터리로 이동합니다.

   ```
   ACSharedDir/bin
   ```

7. 다음 명령을 사용하여 디버그 모드에서 보고서 에이전트를 실행합니다.

   ```
   ./ReportAgent -debug 0 -task 0 -now
   ```

   ReportAgent

   보고서 에이전트를 실행합니다.

   -debug 0

   보고서 에이전트를 디버그 모드에서 실행하고 콘솔에 출력을 표시하도록 지정합니다.

   참고: 보고서 에이전트 데몬이 활성화된 경우 디버그 모드에서 보고서 에이전트를 실행할 수 없습니다.

   -task 0

   보고서 에이전트가 CA Access Control 데이터베이스 및 로컬 PMDB 에 대한 정보를 수집하여 배포 서버에 전달하도록 지정합니다. 이 정보는 CA Access Control 보고서를 생성하는 데 사용됩니다.

   -now

   보고서 에이전트를 지금 실행하도록 지정합니다.

8. 다음과 같이 보고서 에이전트 출력을 검토합니다.
   - 출력에서 오류가 있는지 검토합니다.
   - "보내기" 보고서 매개 변수 섹션에서 "보내기 큐" 및 "보고서 파일" 매개 변수에 올바른 이름이 지정되어 있는지 확인합니다.
9. CA Access Control 을 시작합니다.

   ```
   seload
   ```

   CA Access Control 과 보고서 에이전트가 시작됩니다.

예: 보고서 에이전트 출력

다음 보고서 에이전트 출력에는 Send Queue 및 Report File 매개 변수가 표시되어 있습니다.

```
------------------------------------------------------------------------
Send report parameters:
------------------------------------------------------------------------
Send Queue.................. queue/snapshots
Report File.................
/work/opt/CA/AccessControlShared/data/db2xml/ACDB.xml
------------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

Windows 컴퓨터에서 보고서 에이전트 문제 해결

Windows 에 해당

보고서 에이전트는 끝점에 있는 모든 정책 모델 데이터베이스(PMDB)와 로컬 CA Access Control 데이터베이스의 예약된 스냅숏을 수집하여 이 스냅숏을 XML 형식으로 배포 서버에 있는 보고서 큐로 전달합니다.

참고: 보고서 에이전트는 다른 작업도 수행합니다. 보고서 에이전트에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

Windows 컴퓨터에서 보고서 에이전트의 문제를 해결하려면

1. 다음 구성 설정이 올바른지 확인합니다. 구성 설정은 다음 레지스트리 키에 있습니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent

   참고: 구성 설정의 값을 확인하기 위해 CA Access Control 끝점 관리 또는 selang 명령을 사용할 수 있습니다. 하지만 이 절차의 경우 구성 환경에서 selang 명령을 사용하여 구성 설정의 값을 변경하는 것이 좋습니다. selang 명령을 사용하면 CA Access Control 을 중지한 후 다시 시작할 필요 없이 이 절차에서 구성 설정을 변경할 수 있습니다.

   reportagent_enabled

   로컬 컴퓨터에서 보고를 활성화할지 여부를 지정합니다(1).

   기본값: 0

   중요! 보고서 에이전트가 자동으로 실행되도록 하려면 이 구성 설정의 값을 1 로 설정해야 합니다. 이 구성 설정의 값을 0 으로 설정하면 보고서 에이전트가 데이터베이스의 예정된 스냅숏을 배포 서버로 전달하지 않습니다. 하지만 이 구성 설정의 값이 0 인 경우에도 보고서 에이전트를 디버그 모드에서 실행할 수 있습니다.

   schedule

   보고서를 만들어 배포 서버로 보낼 일정을 정의합니다.

   이 설정은 time@day[,day2][...] 형식으로 지정할 수 있습니다.

   기본값: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   예: "19:22@Sun,Mon"을 지정하면 일요일과 월요일마다 오후 7:22 에 보고서가 생성됩니다.

send_queue

보고서 에이전트가 로컬 데이터베이스의 스냅숏을 보내는 배포 서버에 있는 메시지 큐의 이름을 정의합니다.

Default: queue/snapshots

중요! 이 구성 설정의 기본 값을 변경하지 마십시오.

2. 다음 구성 설정이 올바른지 확인합니다. 이 구성 설정은 다음 레지스트리 키에 있습니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communication
```

Distribution_Server

배포 서버 URL 을 정의합니다.

참고: TCP 통신을 위한 기본 포트는 7222 이고 SSL 통신을 위한 기본 포트는 7243 입니다. 배포 서버 URL 이 통신 유형에 대한 올바른 포트 번호를 지정하는지 확인해야 합니다.

기본값: none

예: ssl://172.24.176.145:7243. 이 URL 은 보고서 에이전트가 SSL 프로토콜을 사용하여 7243 포트에서 IP 주소 172.24.176.145 로 배포 서버와 통신하도록 구성합니다.

3. CA Access Control 보고서 에이전트 서비스가 시작되었는지 확인합니다.

참고: CA Access Control 보고서 에이전트 서비스가 자동으로 시작되도록 구성하려면 reportagent_enabled 구성 설정을 1 로 설정해야 합니다.

4. 명령 프롬프트 창을 열고 CA Access Control 을 중지합니다.

```
secons -s
```

보고서 에이전트 서비스를 포함하여 CA Access Control 이 중지됩니다.

5. 다음 명령을 사용하여 디버그 모드에서 보고서 에이전트를 실행합니다.

   ```
   reportagent -debug 0 -task 0 -now
   ```

   ReportAgent

   보고서 에이전트를 실행합니다.

   -debug 0

   보고서 에이전트를 디버그 모드에서 실행하고 콘솔에 출력을 표시하도록 지정합니다.

   참고: 보고서 에이전트 서비스가 시작된 경우 디버그 모드에서 보고서 에이전트를 실행할 수 없습니다.

   -task 0

   보고서 에이전트가 CA Access Control 데이터베이스 및 로컬 PMDB 에 대한 정보를 수집하여 배포 서버에 전달하도록 지정합니다. 이 정보는 CA Access Control 보고서를 생성하는 데 사용됩니다.

   -now

   보고서 에이전트를 지금 실행하도록 지정합니다.

6. 다음과 같이 보고서 에이전트 출력을 검토합니다.
   - 출력에서 오류가 있는지 검토합니다.
   - "보내기" 보고서 매개 변수 섹션에서 "보내기 큐" 및 "보고서 파일" 매개 변수에 올바른 이름이 지정되어 있는지 확인합니다.
7. CA Access Control 을 시작합니다.

   ```
   seosd -start
   ```

   CA Access Control 이 시작되고 보고서 에이전트 서비스가 실행 중입니다.

예: 보고서 에이전트 출력

다음 보고서 에이전트 출력에는 Send Queue 및 Report File 매개 변수가 표시되어 있습니다.

```
------------------------------------------------------------------------
Send report parameters:
------------------------------------------------------------------------
Send Queue.................. queue/snapshots
Report File................. C:\Program
Files\CA\AccessControl\data\db2xml\ACDB.xml
------------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

라이브러리 경로 환경 변수 예제

다음 예는 Linux 또는 Solaris 컴퓨터에서 라이브러리 경로 환경 변수를 설정하고 내보냅니다.

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
```

다음 예는 AIX 컴퓨터에서 라이브러리 경로 환경 변수를 설정하고 내보냅니다.

```
export LIBPATH=$LIBPATH:/opt/CA/AccessControlShared/lib
```

다음 예는 HP-UX 컴퓨터에서 라이브러리 경로 환경 변수를 설정하고 내보냅니다.

```
export SHLIB_LATH=$SHLIB_PATH:/opt/CA/AccessControlShared/lib
```

배포 서버 문제 해결

배포 서버에 있는 메시지 큐는 보고서 에이전트가 끝점으로부터 보내는 정보를 받습니다. 그러면 MDB(Message-Driven Java Beans)가 메시지 큐에서 데이터를 읽어 이 데이터를 중앙 데이터베이스에 기록합니다.

배포 서버 문제를 해결하려면

1. (UNIX) 다음과 같이 Tibco EMS Administration Tool 을 시작합니다.
   a. 다음 디렉터리로 이동합니다.
      `/opt/CA/AccessControlServer/MessageQueue/tibco/ems/5.1/bin`
   b. 다음 명령을 실행합니다.
      `./tibemsadmin`
2. (Windows) 다음과 같이 Tibco EMS Administration Tool 을 시작합니다.
   a. 다음 디렉터리로 이동합니다.
      `C:\Program Files\CA\AccessControlServer\MessageQueue\tibco\ems\5.1\bin`
   b. 다음 명령을 실행합니다.
      `tibemsadmin.exe`

3. 다음 명령 중 *하나*를 사용하여 현재 환경에 연결합니다.
   - 배포 서버가 7222 포트(기본 포트)에서 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     ```
     connect
     ```

   - 배포 서버가 7243 포트에서 SSL 모드로 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     ```
     connect SSL://7243
     ```

4. 사용자 이름과 암호를 입력합니다.

   참고: 기본 사용자 이름은 admin 이고 암호는 CA Access Control 엔터프라이즈 관리 또는 배포 서버를 설치할 때 지정한 통신 암호입니다.

   배포 서버의 메시지 큐에 연결되었습니다.

5. 다음 명령을 입력합니다.

   ```
   show queues
   ```

   배포 서버에 있는 큐의 목록이 나타납니다.

6. 끝점에서 명령 프로그램 창을 엽니다.

7. (UNIX) 다음과 같이 라이브러리 경로 환경 변수를 설정합니다.
   a. root 로 su 를 실행합니다.
   b. 라이브러리 경로 환경 변수를 *ACSharedDir*/lib 로 설정합니다. 기본적으로 *ACSharedDir* 는 다음 디렉터리입니다.

      ```
      /opt/CA/AccessControlShared
      ```

   c. 라이브러리 경로 환경 변수를 내보냅니다.

8. (UNIX) 다음 디렉터리로 이동합니다.

   ```
   ACSharedDir/bin
   ```

9. 끝점에서 보고서 에이전트를 실행합니다. 다음 작업 중 *하나*를 수행합니다.

   - (Windows) 다음 명령을 실행합니다.

     ```
     ReportAgent -report snapshot
     ```

   - (UNIX) 다음 명령을 실행합니다.

     ```
     ./ReportAgent -report snapshot
     ```

   보고서 에이전트는 CA Access Control 데이터베이스와 모든 로컬 PMDB 의 스냅숏을 배포 서버의 보고서 큐로 보냅니다.

10. 보고서 에이전트가 실행될 때 tibemsadmin 유틸리티에서 queue/snapshots 란 이름의 큐를 확인합니다.

    이 큐가 증가하고 줄지 않으면 JBoss 가 실행 중이지 않은 경우일 수 있습니다. JBoss 의 문제를 해결해야 합니다.

JBoss 문제 해결

JBoss 웹 응용 프로그램 서버 환경에는 메시지 큐에서 데이터를 읽어 중앙 데이터베이스에 기록하는 메시지 구동 Java Bean(MDB)이 포함되어 있습니다. 중앙 데이터베이스는 보고 데이터를 저장합니다.

JBoss 의 문제를 해결하려면

1. 다음과 같이 JBoss 가 올바르게 시작되는지 확인합니다.

   - 명령 프롬프트에서 JBoss 를 시작하는 경우 JBoss 가 시작할 때 최초 출력을 검토하십시오. 출력에 오류가 없는지 확인합니다.
   - JBoss 를 서비스로 시작하는 경우 로그 파일 또는 tail 명령을 사용하여 JBoss 가 시작할 때 최초 출력을 검토하십시오. 출력에 오류가 없는지 확인합니다.

2. 다음 파일을 열고 오류가 있는지 검토합니다. 여기서 *JBossInstallDir* 는 JBoss 를 설치한 디렉터리입니다.

   JBossInstallDir/server/default/log/boot.log

   이 파일은 JBoss 가 마이크로커널을 부팅할 때마다 수행하는 단계를 나열합니다.

3. JAVA_HOME 변수가 올바른 위치로 설정되었는지 확인합니다.

   참고: JAVA_HOME 변수가 올바른 위치로 설정되어 있지만 JBoss 가 변수를 확인하지 못하면 JAVA_HOME 변수를 더 낮은 위치(예: JDK 설치 경로 아래의 bin 디렉터리)로 설정하십시오.

4. 다음 파일을 열고 오류가 있는지 검토합니다.

   JBossInstallDir/server/default/log/server.log

   이 파일은 JBoss 가 JBoss 웹 응용 프로그램 서버 환경에서 수행하는 작업을 나열합니다.

   참고: JBoss 는 시작할 때마다 새 server.log 파일을 만듭니다.

5. JBoss 포트가 다른 서비스에서 사용되는 포트와 충돌하지 않는지 확인합니다.

6. (선택 사항) JNP 포트가 다른 서비스와 충돌하는 경우 다음과 같이 JNP 포트를 1099 에서 다른 포트로 변경합니다.

   a. 텍스트 편집기에서 다음 파일을 엽니다.

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 다음 섹션에서 포트 번호를 변경합니다.

      ```
      <!-- The listening port for the bootstrap JNP service. Set this to -1 to run
      the NamingService without the JNP invoker listening port.-->
      <attribute name="Port">1099</attribute>
      ```

   c. 파일을 저장한 후 닫습니다.

7. (선택 사항) RMI 포트가 다른 서비스와 충돌하는 경우 다음과 같이 RMI 포트를 1098 에서 다른 포트로 변경합니다.

   a. 텍스트 편집기에서 다음 파일을 엽니다.

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 다음 섹션에서 포트 번호를 변경합니다.

      ```
      <!-- The port of the RMI naming service, 0 == anonymous -->
      <!-- attribute name="RmiPort">1098</attribute -->
      <attribute name="RmiPort">1098</attribute>
      ```

   c. 파일을 저장한 후 닫습니다.

보고서 포털 문제 해결

보고서 포털을 사용하면 배포 서버가 중앙 데이터베이스에 저장하는 끝점 데이터에 액세스하여 기본 제공 보고서를 만들거나, 데이터를 조회하거나, 사용자 지정 보고서를 만들 수 있습니다. 이때 CA Business Intelligence 가 사용됩니다.

보고서 포털의 문제를 해결하려면

1. 올바른 URL 을 사용하여 보고 인터페이스(BusinessObjects InfoView)에 액세스하는지 확인합니다. 올바른 URL 은 다음과 같습니다.

   http://*host*:*port*/businessobjects/enterprise115/desktoplaunch

2. (Windows) 올바른 메뉴 옵션을 사용하여 InfoView 에 액세스하는지 확인합니다.

   InfoView 에 액세스하려면 "시작", 프로그램", "BusinessObjects XI Release 2", "BusinessObjects Enterprise", "BusinessObjects Enterprise Java InfoView"를 차례로 클릭하십시오.

3. 다음 서비스가 시작되었는지 확인합니다.
   - Apache Tomcat
   - 중앙 관리 서버
   - 연결 서버
   - Crystal Reports 캐시 서버
   - Crystal Reports 작업 서버
   - Crystal Reports 페이지 서버
   - Desktop Intelligence 캐시 서버
   - Desktop Intelligence 작업 서버
   - Desktop Intelligence 보고서 서버
   - 대상 작업 서버
   - 이벤트 서버
   - 입력 파일 리포지토리 서버
   - 값 목록 작업 서버
   - 출력 파일 리포지토리 서버
   - 프로그램 작업 서버
   - 보고서 응용 프로그램 서버
   - 웹 인텔리전스 작업 서버
   - 웹 인텔리전스 보고서 서버

4. CA Access Control Universe 에 대한 연결을 테스트합니다.

   참고: CA Access Control Universe 가 BusinessObjects Designer 에 표시되지 않으면 보고서 패키지가 배포되지 않을 수 있습니다. 보고서 패키지를 배포하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

CA Access Control Universe 연결 테스트

CA 에서 제공하는 CA Access Control Universe 는 CA Access Control 보고 서비스 중앙 데이터베이스에서 보고서를 작성하는 일을 단순화합니다.

참고: CA Access Control Universe 에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

표준 CA Access Control 보고서를 설치한 후 보고 서비스 연결 문제가 발생하면, 필요에 따라 연결을 테스트 및 수정해야 합니다.

CA Access Control Universe 연결을 테스트하려면

1. "시작", "프로그램", "Business Objects XI Release 2", "BusinessObjects Enterprise", "디자이너"를 차례로 선택합니다.

   BusinessObjects Designer 에 로그인할 수 있는 "User Identification(사용자 ID)" 대화 상자가 나타납니다.

2. 자격 증명을 입력하고 "OK(확인)"를 클릭합니다.

   "Quick Design(빠른 디자인)" 마법사의 시작 화면이 나타납니다.

3. "Run this Wizard at Startup(시작 시 이 마법사 실행)" 확인란의 선택을 취소하고 "Cancel(취소)"을 클릭합니다.

   비어 있는 디자이너 세션이 열립니다. 사용자 이름과 리포지토리 이름이 제목 표시줄에 나타납니다.

4. "File(파일)", "Import(가져오기)"를 클릭하고, CA Access Control Universe 가 포함된 디렉터리로 이동하고, CA Access Control universe 를 선택한 다음, "OK(확인)"를 클릭합니다.

   가져오기가 성공적으로 수행되어 CA Access Control Universe 가 현재 Designer 창에 열립니다.

   참고: CA Access Control Universe 는 기본 universe 파일 저장소로 지정된 디렉터리의 CA Universe\CA Access Control 아래에 저장됩니다.

5. "Tools(도구)", "Connections(연결)"를 클릭합니다.

   "Wizard Connection(마법사 연결)" 대화 상자가 나타납니다.

6. 테스트할 Access_Control1 연결을 선택한 다음 "Test(테스트)"를 클릭합니다.

   연결이 응답함을 알리는 확인 메시지가 나타납니다. 연결이 응답하지 않으면 오류 메시지를 수신하게 됩니다.

7. 오류를 수신한 경우 "Edit(편집)"를 클릭하여 연결 설정을 수정합니다.

   - 데이터베이스 미들웨어 선택-Oracle\Oracle 10\Oracle Client
   - 유형-Secured
   - 이름-Access_Control1
   - 사용자 이름-*Oracle_adminUserName*
   - 암호-*Oracle_adminUserPass*
   - 서비스-Oracle_TNS_Name

   필요에 따라 6 단계를 반복하여 연결을 테스트합니다.

보고서 서버가 중지되었거나 연결할 수 없음

증상

CA Business Intelligence 또는 CA Access Control 엔터프라이즈 관리에서 보고서를 보려고 시도하면 다음 오류 메시지가 표시됩니다.

보고서 서버가 중지되었거나 연결할 수 없습니다.

해결 방법

이 문제를 해결하려면 다음을 수행하십시오.

1. JBoss 로그 파일을 엽니다. JBoss 로그 파일은 다음 디렉터리에 있습니다. 여기서 *JBossInstallDir* 는 JBoss 를 설치한 디렉터리입니다.

   JBossInstallDir/server/default/log/server.log

   이 파일은 JBoss 가 JBoss 웹 응용 프로그램 서버 환경에서 수행하는 작업을 나열합니다.

   참고: JBoss 는 시작할 때마다 새 server.log 파일을 만듭니다.

2. 이 로그 파일에서 오류의 원인을 찾습니다.
3. 오류에 표시된 컴퓨터의 이름을 대/소문자를 구분하여 기록하십시오.

   로그 파일에 표시된 그대로 정확히 이름을 기록해야 합니다.

4. 호스트 파일을 엽니다. 호스트 파일은 기본적으로 다음 디렉터리에 있습니다.
   - (UNIX) /etc/hosts
   - (Windows) C:\WINDOWS\system32\drivers\etc
5. 파일의 새 줄에서 IP 주소와 컴퓨터의 대/소문자가 구분된 이름을 입력합니다. 이때 각각은 공백으로 구분하십시오.

   컴퓨터 이름은 3 단계에서 기록했습니다.
6. 파일을 저장한 후 닫습니다.

예: 호스트 파일

다음 조각은 호스트 파일의 예입니다:

```
127.0.0.1       localhost
```

MS SQL 데이터베이스를 사용하여 CA Business Intelligence 에서 보고서를 볼 수 없음

증상

MS SQL 데이터베이스를 중앙 데이터베이스로 사용하고 있는데 CA Business Intelligence 에서 보고서를 볼 수 없습니다. 보고서를 보려고 시도하면 다음 오류 메시지가 표시됩니다.

연결 실패

해결 방법

다음 프로세스는 CA Business Intelligence 와 관련된 문제를 해결하는 데 도움을 줍니다.

1. 다음과 같이 BusinessObjects 버전 번호를 확인합니다.
   a. 다음 URL 을 엽니다.

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      hostname

      보고서 포털 호스트의 이름을 정의합니다.

      중앙 관리 콘솔 로그온 페이지가 나타납니다.

   b. 사용자 이름과 암호를 입력하고 "로그온"을 클릭합니다.

      중앙 관리 콘솔이 나타납니다.

   c. 서버, *hostname*, Web_IntelligenceReportServer, 메트릭을 클릭합니다.

      BusinessObjects 버전 번호가 표시됩니다.

   d. BusinessObjects 버전 번호가 11.5.8.1061 이상 또는 11.5.10.1263 이상인지 확인합니다.

2. 다음과 같이 CA Business Intelligence 버전 번호를 확인합니다.
   a. 보고서 포털에서 다음 파일을 엽니다.
      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt

   b. CA Business Intelligence 버전이 2.1.13 인지 확인합니다.

3. 다음과 같이 데이터베이스 자격 증명이 올바른지 확인합니다.
   a. "시작", "프로그램", "Microsoft SQL Server 2005", "SQL Server Management Studio"를 클릭합니다.

      SQL Server 2005 로그인 페이지가 나타납니다.

   b. CA Access Control 엔터프라이즈 관리에 대한 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 사용자 이름과 암호를 입력합니다.

   c. [연결]을 클릭합니다.

      SQL Server Management Studio 에 로그인했습니다. 로그인할 수 없으면 데이터베이스 자격 증명이 잘못된 것입니다.

4. 다음과 같이 *import_biar_config*.xml 파일에 올바른 값이 있는지 확인합니다.
   a. 보고서 포털에 보고서 패키지를 배포하기 위해 사용한 *import_biar_config*.xml 파일을 엽니다.
   b. 3 단계에서 지정한 값에 해당하는 다음 속성의 값을 확인합니다.
      - <username>은 입력한 사용자 이름과 동일합니다.
      - <password>는 입력한 암호와 동일합니다.
      - <datasource>는 입력한 데이터베이스의 이름과 동일합니다.
      - <server>는 보고서 서버 컴퓨터의 이름과 동일합니다.

Oracle 데이터베이스를 사용하여 CA Business Intelligence 에서 보고서를 볼 수 없음

증상

Oracle 데이터베이스를 중앙 데이터베이스로 사용하고 있는데 CA Business Intelligence 에서 보고서를 볼 수 없습니다. 보고서를 보려고 시도하면 다음 오류 메시지가 표시됩니다.

연결 실패

해결 방법

다음 프로세스는 CA Business Intelligence 와 관련된 문제를 해결하는 데 도움을 줍니다.

1. 다음과 같이 BusinessObjects 버전 번호를 확인합니다.
   a. 다음 URL 을 엽니다.

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      hostname

      보고서 포털 호스트의 이름을 정의합니다.

      중앙 관리 콘솔 로그온 페이지가 나타납니다.

   b. 사용자 이름과 암호를 입력하고 "로그온"을 클릭합니다.

      중앙 관리 콘솔이 나타납니다.

   c. 서버, *hostname*, Web_IntelligenceReportServer, 메트릭을 클릭합니다.

      BusinessObjects 버전 번호가 표시됩니다.

   d. BusinessObjects 버전 번호가 11.5.8.1061 이상 또는 11.5.10.1263 이상인지 확인합니다.

2. 다음과 같이 CA Business Intelligence 버전 번호를 확인합니다.
   a. 보고서 포털에서 다음 파일을 엽니다.
      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt

   b. CA Business Intelligence 버전이 2.1.13 인지 확인합니다.

3. Oracle 시스템 환경 변수가 다음과 같이 정의되었는지 확인합니다. 여기서 *Oracle_home* 은 Oracle 을 설치한 디렉터리입니다.
   - ORACLE_HOME 이 *Oracle_home* 디렉터리를 가리킵니다.
   - PATH 가 *Oracle_home*/bin 디렉터리를 포함합니다.
   - TNS_ADMIN 이 *Oracle_home*/network/admin 디렉터리를 가리킵니다.

4. 다음과 같이 TNS 가 올바르게 정의되었는지 확인합니다.
   a. 명령 프롬프트 창을 엽니다.
   b. 다음 명령을 실행합니다.

      `tnsping TNSname`

      TNSname

      TNS의 이름을 정의합니다.

      오류 메시지가 표시되면 TNS 가 올바로 정의되지 않은 것입니다.

5. 다음과 같이 올바른 자격 증명을 사용하여 데이터베이스에 액세스하는지 확인합니다.
   a. 명령 프롬프트 창을 엽니다.
   b. 다음 명령을 실행합니다.

      `sqlplus user/password@TNSname`

      사용자

      CA Access Control 엔터프라이즈 관리에 대한 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 이름을 정의합니다.

      password

      사용자 암호를 정의합니다.

      SQL 명령줄에 로그온할 수 없으면 데이터베이스 자격 증명이 잘못된 것입니다.

6. 다음과 같이 *import_biar_config*.xml 파일에 올바른 값이 있는지 확인합니다.
   a. 보고서 포털에 보고서 패키지를 배포하기 위해 사용한 *import_biar_config*.xml 파일을 엽니다.
   b. 다음 속성의 값이 5 단계에서 지정한 값과 동일한지 확인합니다.
      - <username>은 *user* 와 동일합니다.
      - <password>는 *password* 와 동일합니다.
      - <datasource>는 *TNSname* 과 동일합니다.

7. (UNIX) CA Business Intelligence 를 설치할 때 지정한 사용자로 4 단계와 5 단계의 명령을 실행합니다.

   이 사용자는 CA Business Intelligence 설치 마법사의 CMS 데이터베이스 설정 페이지에 지정합니다. 이 단계는 사용자가 전체 *Oracle_home* 디렉터리에 읽기 및 실행 액세스 권한이 있는지 확인합니다.

CA Access Control 엔터프라이즈 관리에서 보고서를 볼 수 없음

증상

CA Access Control 엔터프라이즈 관리에서 보고서를 보려고 하면 Business Objects 로그가 대화 상자에 표시되고 브라우저에 개인 정보 보고서 아이콘이 표시됩니다.

해결 방법

브라우저가 보고서 포털에서 쿠키를 차단하고 있습니다. 이 문제를 해결하려면 보고서 포털의 쿠키를 허용하도록 브라우저의 쿠키 설정을 조정하십시오.

참고: 개인 정보 보고서는 브라우저가 차단하는 쿠키에 대한 자세한 정보를 제공합니다. 개인 정보 보고서를 표시하려면 개인 정보 보고서 아이콘을 두 번 클릭하십시오.

부록 A: 문제 해결 및 유지 관리 절차

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control 이 올바로 설치되었는지 확인하는 방법

Windows 에 해당

제품을 설치한 직후 CA Access Control 이 올바로 설치되었는지 확인해야 합니다. 다음 절차는 CA Access Control 이 올바로 설치되었는지 확인하는 데 도움을 줍니다.

CA Access Control 을 성공적으로 설치한 경우 다음 변경 사항이 나타납니다.

- 새 키가 Windows 레지스트리에 추가됩니다.

  `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl`

  CA Access Control 이 실행되는 동안 CA Access Control 키 및 하위 키가 보호되며, 키를 수정하려면 CA Access Control 끝점 관리 또는 selang 명령을 사용해야 합니다. 하지만 키와 값을 읽기 위해 CA Access Control 끝점 관리 또는 selang 명령을 사용할 필요는 없습니다.
- 컴퓨터를 다시 시작할 때 새로운 몇몇 CA Access Control 서비스가 자동으로 시작됩니다. 이러한 서비스에는 Watchdog, 엔진, 에이전트 등이 포함되며 이들 서비스는 항상 설치됩니다. 작업 위임과 같은 기타 서비스는 설치 중 선택한 옵션에 따라 존재 여부가 결정됩니다. 모든 CA Access Control 서비스의 표시 이름은 "CA Access Control"로 시작됩니다. Windows 서비스 관리자를 사용하여 어떠한 서비스가 설치되었고 이러한 서비스가 실행 중인지 여부를 확인할 수 있습니다.

리소스 액세스 문제의 해결 방법

잘못된 액세스 권한은 리소스 액세스 문제의 가장 흔한 원인입니다. 리소스 액세스 문제의 한 예로는 root 사용자가 보호된 리소스에 액세스할 수 있는 반면 이 보호된 리소스에는 기본 액세스 권한으로 "none"이 할당된 경우를 들 수 있습니다. 다음 프로세스는 리소스 액세스 문제를 해결하는 데 도움을 줍니다.

1. 보호된 리소스의 감사 모드를 모두 감사로 변경합니다.

   `chres CLASS ResourceName audit(all)`

   감사 모드를 모두 감사로 변경하면 보다 쉽게 감사 로그를 읽을 수 있습니다.

2. 추적을 실행 (페이지 124)하고 문제를 다시 재현합니다.
3. 추적 파일 및 감사 로그에서 보호된 리소스에 대한 항목을 검토합니다. 이러한 파일의 정보로부터 리소스 액세스 문제의 원인을 파악하십시오.

   참고: SPECIALPGM 개체는 감사되지 않은 항목을 바이패스하지만 이러한 바이패스는 추적 파일에 나타납니다.

참고: 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

연결 문제 해결 방법

CA Access Control 컴퓨터 사이의 연결에는 많은 요인들이 영향을 줍니다. 연결 문제에는 원격 CA Access Control 컴퓨터에 연결할 수 없거나 원격 컴퓨터에 대한 연결이 만료되는 문제가 포함됩니다. 다음 프로세스는 연결 문제의 원인을 파악하는 데 도움을 줍니다.

참고: 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

1. CA Access Control 컴퓨터에서 다음에 대한 최근 변경 사항을 확인합니다.
   - 암호화 키
   - 암호화 방법
   - TCP 및 UDP 포트
2. TCP, CONNECT, HOSTNET, HOST 클래스에서 규칙이 새로 추가되었거나 최근에 변경되었는지 검토합니다.
3. 연결 문제가 있는 포트를 파악합니다.
4. 추적 기능을 실행 (페이지 124)하고 추적 파일에서 다음 사항이 있는지 검토합니다.
   - TCP 규칙 또는 다른 규칙으로 인해 CA Access Control 이 차단한 연결
   - 연결 문제가 있는 포트 번호 옆에 P('P'ermitted - 허용됨) 이외의 다른 코드
5. CA Access Control 감사 로그에서 문제가 있는 포트를 참조하는 D('D'eny - 거부) 레코드가 있는지 검토합니다.

6. 방화벽이 문제가 있는 포트를 차단하지 않는지 확인합니다.
7. 사용하는 OS 의 로그 파일에서 바인딩할 수 없는 포트로 인해 발생한 오류 메시지가 있는지 검토합니다.

추가 정보:

CA Access Control 에이전트 통신을 위한 포트 번호 변경 (페이지 128)

성능 문제 해결 방법

다음 절차는 성능 문제의 원인을 파악하는 데 도움을 줍니다.

참고: 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

1. 성능 문제가 언제 발생하는지 파악합니다. 다음 경우에 성능 문제가 있습니까?
   - OS 를 시작할 때
   - CA Access Control 을 시작할 때
   - CA Access Control 을 시작한 후 잠시 시간이 지났을 때
   - CA Access Control 또는 OS 가 예정된 프로세스를 실행할 때
   - (UNIX) CA Access Control 커널 확장이 로드될 때
   - CA Access Control 데몬 또는 서비스가 로드될 때
2. CA Access Control 로 인해 성능 문제가 발생하는 것으로 파악되면 다음 사항을 확인하십시오.
   - 성능이 저하될 때 어떤 프로세스가 가장 많은 리소스를 사용합니까?
   - CA Access Control 프로세스가 수명 주기 내내 동일한 프로세스 ID 를 유지합니까?
   - 컴퓨터에 설치된 타사 필터 드라이버가 있습니까?
   - 컴퓨터에 설치된 시스템 모니터링 응용 프로그램이 있습니까?

3. CA Access Control 데이터베이스를 검사합니다.
   a. CA Access Control 을 중지합니다.
   b. 데이터베이스를 검사합니다.

      ```
      dbmgr -util -all
      ```

   c. 데이터베이스의 인덱스를 다시 만듭니다 (페이지 126).
   d. 데이터베이스를 다시 빌드합니다 (페이지 127).
   e. CA Access Control 을 다시 시작하고 문제가 아직도 발생하는지 확인합니다.
4. (Windows) 드라이버 차단을 비활성화합니다.
   a. CA Access Control 을 중지합니다.
   b. UseFsiDrv 레지스트리 항목의 값을 0 으로 변경합니다. UseFsiDrv 레지스트리 항목은 다음 레지스트리 키에 있습니다.

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl
      ```

   c. CA Access Control 을 다시 시작하고 문제가 아직도 발생하는지 확인합니다.
5. 추적을 실행 (페이지 124)하고 문제를 다시 재현합니다. 추적 파일에서 다음 사항을 검토합니다.
   - 짧은 시간 내 반복된 이벤트. 예: 몇 초 동안 많은 파일 액세스 발생
   - 중단(kill)된 프로세스
   - 다음 값 중 하나
     - ACEEH = -1
     - U = 음수 값

     이러한 값은 CA Access Control 이 사용자 이름을 확인할 수 없거나 리소스에 값을 할당할 수 없음을 나타냅니다.

참고: UNIX 컴퓨터에서 CA Access Control 의 성능을 향상하는 방법에 대한 자세한 내용은 *UNIX 용 끝점 관리 안내서*를 참조하십시오.

추적 실행

추적을 실행하면 문제를 해결하는 데 도움이 됩니다. CA Access Control 은 *ACInstallDir*/log 디렉터리에 있는 seos.trace 파일에 추적 레코드를 기록합니다.

추적을 실행하려면

1. 추적 파일에서 모든 레코드를 제거합니다.

   ```
   secons -tc
   ```

2. 추적을 시작합니다.

   ```
   secons -t+
   ```

3. 문제를 재현합니다.
4. 추적을 중지합니다.

   ```
   secons -t-
   ```

5. 추적 파일을 검토합니다.

참고: seosd 섹션의 구성 설정은 추적 파일을 구성합니다. seosd 섹션에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control 웹 서비스 구성 요소에서 추적 실행

Windows 에 해당

CA Access Control 웹 서비스 구성 요소에서 추적을 실행하면 문제를 해결하는 데 도움이 될 수 있습니다. 예를 들어, CA Access Control 엔터프라이즈 관리가 DMS 에 연결할 수 없으면 추적을 실행하여 이러한 두 구성 요소가 주고받는 메시지를 검토할 수 있습니다.

CA Access Control 은 웹 서비스 구성 요소의 추적 레코드를 WebService 섹션의 logFileName 구성 설정에 정의된 파일에 기록합니다. 이 구성 설정의 기본값은 C:\Program Files\CA\AccessControlServer\WebService\log\WebService.log 입니다.

CA Access Control 웹 서비스 구성 요소에서 추적을 실행하려면

1. CA Access Control 및 CA Access Control 웹 서비스를 중지합니다.
2. 다음 위치에 레지스트리 키를 만듭니다.

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService\TraceEnabled`
3. 이 키의 값을 1 로 설정합니다.
4. CA Access Control 및 CA Access Control 웹 서비스를 시작합니다.

   CA Access Control 웹 서비스 구성 요소에서 추적이 시작됩니다.
5. 문제를 재현합니다.
6. CA Access Control 및 CA Access Control 웹 서비스를 중지합니다.

   CA Access Control 웹 서비스 구성 요소에서 추적이 중지됩니다.
7. 이 키의 값을 0 로 설정합니다.
8. 추적 파일을 검토합니다.

CA Access Control 데이터베이스 인덱스 다시 만들기

CA Access Control 데이터베이스에 대한 많은 업데이트로 인해 데이터베이스 파일이 조각화될 수 있습니다. 데이터베이스의 인덱스를 다시 만들고 데이터베이스를 다시 빌드 (페이지 127)하면 데이터베이스의 속도와 안정성을 최적화하는 데 도움이 됩니다. 3 개월에서 6 개월 간격으로 일상적인 유지 관리 절차 중 또는 성능 문제가 발생할 때마다 데이터베이스의 인덱스를 다시 만드십시오.

Note: 이 절차 중에 CA Access Control 데이터베이스가 기본 위치인 /opt/CA/AccessControl/seosdb (UNIX) 및 C:\Program Files\CA\AccessControl\Data\seosdb (Windows)에 설치됩니다. 이 절차를 수행하려면 root 사용자(UNIX) 또는 administrator(Windows)로 로그인해야 합니다.

CA Access Control 데이터베이스의 인덱스를 다시 만들려면

1. CA Access Control 을 중지합니다.
2. 다음 디렉터리로 이동합니다.
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. 데이터베이스를 백업합니다.

   ```
   dbmgr -backup backup_directory
   ```
4. 데이터베이스의 인덱스를 만듭니다.

   ```
   dbmgr -util -build seos_cdf.dat
   dbmgr -util -build seos_odf.dat
   dbmgr -util -build seos_pdf.dat
   dbmgr -util -build seos_pvf.dat
   ```

참고: UNIX 컴퓨터에서 데이터베이스의 크기를 더욱 줄이려면 sepurgdb 유틸리티를 사용하여 데이터베이스에서 정의되지 않은 레코드에 대한 참조를 삭제할 수 있습니다. sepurgdb 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control 데이터베이스 다시 빌드

CA Access Control 데이터베이스에 대한 많은 업데이트로 인해 데이터베이스 파일이 조각화됩니다. 데이터베이스의 인덱스를 다시 만들고 (페이지 126) 데이터베이스를 다시 빌드하면 데이터베이스의 속도와 안정성을 최적화하는 데 도움이 됩니다. 3 개월에서 6 개월 간격으로 일상적인 유지 관리 절차 중 데이터베이스를 다시 빌드하십시오.

Note: 이 절차 중에 CA Access Control 데이터베이스가 기본 위치인 /opt/CA/AccessControl/seosdb (UNIX) 및 C:\Program Files\CA\AccessControl\Data\seosdb (Windows)에 설치됩니다. 이 절차를 수행하려면 root 사용자(UNIX) 또는 administrator(Windows)로 로그인해야 합니다.

CA Access Control 데이터베이스를 다시 빌드하려면

1. CA Access Control 을 중지합니다.
2. 다음 디렉터리로 이동합니다.
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. 데이터베이스를 백업합니다.

   ```
   dbmgr -backup backup_directory
   ```
4. 데이터베이스에서 기존 규칙과 사용자 관련 데이터를 내보냅니다.

   ```
   dbmgr -export -l -f exported_filename
   dbmgr -migrate -r migrated_filename
   ```
5. 다음 디렉터리로 이동하여 seosdb_new 란 이름으로 디렉터리를 만듭니다.
   - (UNIX) /opt/CA/AccessControl
   - (Windows) C:\Program Files\CA\AccessControl\Data
6. seosdb_new 디렉터리에 데이터베이스를 만듭니다.

   ```
   dbmgr -create -cq
   ```
7. *exported_filename* 및 *migrated_filename* 파일을 seosdb_new 디렉터리에 복사합니다.
8. 기존 데이터베이스에서 내보낸 기존 규칙 및 사용자 관련 데이터를 새 데이터베이스로 가져옵니다.

   ```
   selang -l -f exported_filename
   dbmgr -migrate -w migrated_filename
   ```

9. seosdb 디렉터리의 이름을 seosdb_old 로 변경합니다.
10. seosdb_new 디렉터리의 이름을 seosdb 로 변경합니다.
11. CA Access Control 을 시작하고

CA Access Control 에이전트 통신을 위한 포트 번호 변경

CA Access Control client applications—such as selang, policydeploy, and devcalc—and the CA Access Control Agent communicate on port 8891. 이 포트는 변경하지 않는 것이 좋습니다. 이 포트를 변경해야 하는 경우 다음 절차를 따르십시오.

CA Access Control 에이전트 통신을 위한 포트 번호를 변경하려면

1. 텍스트 편집기에서 다음 파일을 엽니다.
   - (UNIX) /etc/services
   - (Windows) %SystemRoot%\drivers\etc\services
2. 다음 내용을 파일에 추가합니다.

   ```
   seoslang2 port-number/ tcp
   ```
3. 파일을 저장한 후 닫습니다.
4. CA Access Control 데몬 또는 서비스를 다시 시작합니다.

메시지 큐 TCP 포트 구성

CA Access Control 엔터프라이즈 관리를 설치할 때 기본적으로 SSL 포트(7243)를 사용하도록 메시지 큐가 구성됩니다. 이 기본 설정을 변경하여 메시지 큐가 TCP 포트(7222)를 사용하도록 구성할 수 있습니다.

메시지 큐 TCP 포트에 연결하려면

1. 엔터프라이즈 관리 서버에서 메시지 큐와 JBoss 서버를 중지합니다.
2. 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 다음 위치에 있습니다.

   ```
   C:\Program Files\CA\AccessControl\/MessageQueue/tibco/tibco/cfgmgmt/ems/data
   ```
3. listen= 항목을 찾아 값을 제거한 다음 값 tcp://7222 를 입력합니다.
4. authorization= 항목을 찾아 값을 제거한 다음 disabled 를 입력합니다.

5. 파일을 저장한 후 닫습니다.
6. factories.conf 파일을 열고 [SSLXAQueueConnectionFactory] 태그를 찾습니다.
7. url= 항목을 찾아 값을 제거한 다음 tcp://7222 를 입력합니다.
8. 파일을 저장한 후 닫습니다.
9. 편집을 위해 tibco-jms-ds.xml 파일을 엽니다. 이 파일은 다음 위치에 있습니다.

   JBoss_HOME/server/default/deploy/jms
10. SSL 포트 번호(7243)가 표시된 값을 모두 검색하여 TCP 포트 번호 7222 로 바꿉니다.
11. 값 SSLXA 를 표시하는 모든 항목을 검색하여 XA 로 바꿉니다.
12. 다음 두 항목을 주석(<!--) 처리합니다.

    ```
    com.tibco.tibjms.naming.security_protocol=ssl
    com.tibco.tibjms.naming.ssl_enable_verify_host=false
    ```
13. 파일을 저장한 후 닫습니다.
14. 메시지 큐 및 JBoss 서버를 시작합니다.

CA Support 에 제공할 정보

CA Support 에 문의할 때는 문제의 원인을 진단하는 데 도움이 될 수 있도록 환경에 대한 모든 변경 사항에 대한 정보를 제공해야 합니다. 예를 들어, 호스트 및 사용자 이름 변경 사항과 운영 체제에 대한 변경 사항은 CA Access Control 에 영향을 줄 수 있습니다. CA Support 에 문의할 때는 또한 CA Access Control 지원 유틸리티를 사용하여 추가 진단 정보를 제공해야 할 수 있습니다.

CA Support 에 문의할 때는 다음과 같은 정보를 제공해야 합니다.

- CA Access Control 버전
- 운영 체제 이름, 버전, 아키텍처, 업데이트 수준
- 컴퓨터에 설치된 모든 CA Access Control 패치 정보
- CPU 개수

참고: CA Access Control 이 지원하는 운영 체제, 버전, 아키텍처, 업데이트 수준에 대한 자세한 내용은 CA Support의 CA Access Control 제품 페이지에서 CA Access Control 호환성 표를 참조하십시오.

CA Support 에 문의할 때는 다음과 같은 질문을 받을 수 있습니다.

- 문제로 인해 어떤 영향이 있습니까?
- 언제 처음 문제가 발생했습니까?
- 문제가 반복됩니까?
- 문제가 발생하기 전에 환경에서 어떤 항목이 추가, 제거 또는 변경되었습니까?
- 문제가 발생하기 전에 컴퓨터를 다시 시작했습니까?
- 이 문제가 몇 번이나 발생했습니까?
- 이 문제가 발생할 때 시스템에 어떤 일이 발생합니까? 예를 들어, 특정 프로세스나 명령을 실행할 때 이 문제가 발생합니까?
- 문제가 지속적으로 또는 간헐적으로 발생합니까?
- CA Access Control 명령을 실행할 때 세그멘테이션 오류나 액세스 위반이 발생합니까?
- CA Access Control 로 인해 이 문제가 발생했다고 생각하는 이유는 무엇입니까?
- 이 문제가 운영 체제 문제인 경우 운영 체제 공급업체에 이 문제를 보고했습니까? 보고한 경우 운영 체제 공급업체로부터 받은 충돌 분석을 제공할 수 있습니까?

Windows 끝점에 대한 진단 정보 생성

CA Access Control 지원 유틸리티는 CA Support 가 문제의 원인을 진단하는 데 도움이 되도록 설치된 CA Access Control 에 대한 정보를 수집합니다. CA Access Control 지원 유틸리티가 수집하는 정보는 ACSupport 대화 상자에서 지정합니다.

다음과 같은 시스템 정보를 수집할 수 있습니다.

- 시스템 정보 보고서
- 이벤트 로그

다음과 같은 CA Access Control 정보를 수집할 수 있습니다.

- CA Access Control 버전, 홈 디렉터리, CA Access Control 서비스의 상태에 대한 일반 정보
- CA Access Control 레지스트리
- 감사, 추적, 공존 유틸리티에 대한 파일 구성
- 로컬 PMDB 또는 DMS 및 구현 추적에 대한 감사 로그를 포함한 감사 및 추적 로그
- 권한 부여 및 캐시 통계
- CA Access Control 실행 파일 및 컴퓨터에 설치된 DLL 의 목록
- 로컬 PMDB 및 DMS 를 포함한 CA Access Control 데이터베이스의 스냅숏

  참고: CA Access Control 데이터베이스의 사본을 수집하는 경우 CA Access Control 지원 유틸리티는 데이터베이스의 스냅숏을 만들기 전에 CA Access Control 을 중지하고 스냅숏이 완료되면 CA Access Control 을 다시 시작합니다.

Windows 끝점에 대한 진단 정보를 생성하려면

1. 다음 디렉터리로 이동합니다. 여기서 *ACInstallDir* 는 CA Access Control 이 설치된 디렉터리입니다.

   ACInstallDir\bin

2. ACSupport.exe 를 두 번 클릭합니다.

   ACSupport 대화 상자가 열립니다.

3. 대화 상자를 완료하고 "계속"을 클릭합니다.

   CA Access Control 지원 유틸리티가 설치의 스냅숏을 만들고 출력을 *ACInstallDir*\ACSupport 디렉터리에 저장합니다.

UNIX 끝점에 대한 진단 정보 생성

CA Access Control 지원 유틸리티는 CA Support 가 문제의 원인을 진단하는 데 도움이 되도록 설치된 CA Access Control 에 대한 정보를 수집합니다. 스냅숏에 CA Access Control 데이터베이스를 포함하는 경우 CA Access Control 지원 유틸리티는 데이터베이스의 스냅숏을 만들기 전에 CA Access Control 을 중지하고 스냅숏이 완료되면 CA Access Control 을 다시 시작합니다.

CA Access Control 지원 유틸리티는 항상 UNIX 끝점에 대한 다음 정보를 수집합니다.

- seos.ini - CA Access Control 초기화 파일
- tmpetc - 다음을 포함하여 CA Access Control /etc 디렉터리의 파일:
  - audit.cfg - 감사 필터 파일
  - auditroute.cfg - 감사 라우트 필터 파일
  - nfsdevs.init - 각 운영 체제의 주요 장치 번호에 대한 NFS 기본값을 포함하는 파일
  - osver - 운영 체제 버전
  - sereport.cfg - sereport 구성 파일
  - serevu.cfg - serevu 구성 파일
  - trcfilter.init - 추적 필터 파일
- versions.txt - 주요 CA Access Control 바이너리의 버전을 포함하는 파일
- 일부 운영 체제 파일(예: 일부 변수 파일)

CA Access Control 지원 유틸리티가 CA Access Control 데이터베이스에 대한 정보를 수집하도록 지정하면 이 유틸리티가 다음 정보를 수집합니다.

- seosdb - CA Access Control 데이터베이스
- seosdb.tar - CA Access Control 데이터베이스의 압축된 파일
- 그룹, 호스트, 서비스, 사용자의 참조(lookaside) 데이터베이스

CA Access Control 지원 유틸리티가 CA Access Control 로그에 대한 정보를 수집하도록 지정하면 이 유틸리티가 다음 정보를 수집합니다.

- tmplog - CA Access Control 로그 파일
- log.tar - CA Access Control 로그 디렉터리의 압축된 파일

UNIX 끝점에 대한 진단 정보를 생성하려면

1. 다음 디렉터리로 이동합니다. 여기서 *ACInstallDir* 는 CA Access Control 이 설치된 디렉터리입니다.

   ACInstallDir/lbin

2. 다음 명령을 실행합니다.

   ./support.sh [-db] [-log] [-all] [-none]

   -db

   CA Access Control 데이터베이스인 seosdb 에 대한 정보를 수집하지만 감사 로그에 대한 정보는 수집하지 않습니다.

   -log

   감사 로그에 대한 정보를 수집하지만 seosdb 에 대한 정보는 수집하지 않습니다.

   -all

   seosdb 및 감사 로그 모두에 대한 정보를 수집합니다.

   -none

   seosdb 및 감사 로그에 대한 정보를 수집하지 않습니다.

   참고: 옵션을 지정하지 않으면 CA Access Control 지원 유틸리티가 대화형 모드로 실행됩니다.

   CA Access Control 지원 유틸리티가 설치의 스냅숏을 만들고 출력을 *ACInstallDir* 디렉터리에 저장합니다.