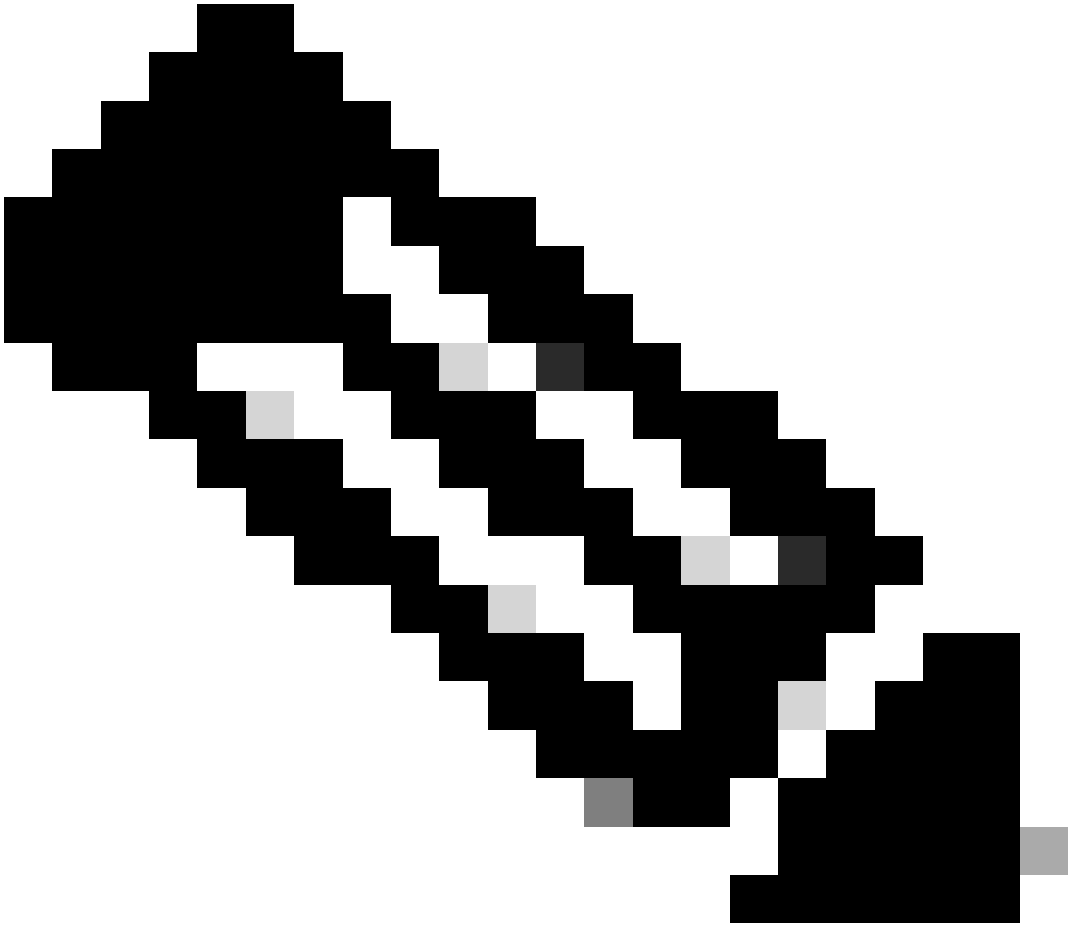
EventID 4662(Windows 2008) 또는 EventID 566(Windows 2003) 문제 해결 - 유형: 실패 감사

목차

소개

이 문서에서는 Security Event ID 566 및 Security Event ID 4662에 대해 설명하고, 이와 마주쳤을 때 수행할 수 있는 작업에 대해 설명합니다. 이러한 이벤트는 Umbrella Insights 배포의 일부로 실행되는 도메인 컨트롤러 또는 구성원 서버에서 발생할 수 있습니다.



참고: 이러한 이벤트는 예상된 일이며 정상입니다. 기본 설정 및 지원되는 작업은 아무 작업도 수행하지 않고 이러한 이벤트를 무시하는 것입니다.

```
Event ID: 566
Source: Security
Category: Directory Service Access
Type: Failure Audit
Description:
Object Operation:
Object Server:  DS
Operation Type: Object Access
Object Type:    user
Object Name:   CN=USER1,OU=MyOU,DC=domain,DC=net
Handle ID:        -
Primary User Name:     DC1$
Primary Domain:           DOMAIN1
Primary Logon ID:        (0x0,0x3E7)
Client User Name:        COMPUTER1$
Client Domain:  DOMAIN1
Client Logon ID:           (0x0,0x19540114)
```

```
Accesses:         Control Access
Properties:

Private Information

msPKIRoamingTimeStamp
msPKIDPAPIMasterKeys
msPKIAccountCredentials
msPKI-CredentialRoamingTokens
Default property set
unixUserPassword

user
Additional Info:
Additional Info2:
Access Mask:   0x100
```

또는 이 Windows 2008 이벤트 보안 ID 4662를 수신합니다.

```
Event ID: 4662
Type: Audit Failure
Category: Directory Service Access

Description:

An operation was performed on an object.

Subject :

Security ID:     DOMAIN1\COMPUTER1$
Account Name:     COMPUTER1$
Account Domain:     DOMAIN1

Logon ID:     0x3a26176b

Object:

Object Server:     DS
Object Type:     user
Object Name:     CN=USER1,OU=MyOU,DC=domain,DC=net

Handle ID:     0x0

Operation:

Operation Type:     Object Access
Accesses:     Control Access
Access Mask:     0x100

Properties:     ---

{91e647de-d96f-4b70-9557-d63ff4f3ccd8}
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05}
{b3f93023-9239-4f7c-b99c-6745d87adbc2}
{b8dfa744-31dc-4ef1-ac7c-84baf7ef9da7}
{b7ff5a38-0818-42b0-8110-d3d154c97f24}
{bf967aba-0de6-11d0-a285-00aa003049e2}
```

원인

Windows 2008에서는 msPKI* 속성을 포함하는 Private Information이라는 새 속성 집합을 도입했습니다. 기본적으로 이러한 속성은 SELF 개체만 액세스할 수 있는 방식으로 보호됩니다. DSACL 명령을 사용하여 필요에 따라 개체에 대한 권한을 확인할 수 있습니다.

엄밀한 조사를 통해 이 감사 이벤트가 이러한 제한된 속성에 대한 쓰기 시도에 의해 발생한다고 생각할 수 있습니다. 이러한 이벤트는 변경 사항(쓰기)만 감사하고 Active Directory에서 정보를 읽으려는 시도는 감사하지 않는 기본 Microsoft 감사 정책에서 발생한다는 사실에서 알 수 있습니다.

그러나 감사 이벤트에는 Control Access(0x100)로 요청된 권한이 명확하게 나열되어 있지 않습니다. 그러나 Private Information 속성 집합에 CA(Control Access) 권한을 부여할 수 없습니다.

솔루션

이러한 메시지를 안전하게 무시할 수 있습니다. 이것은 설계에 의한 것입니다.

 이러한 이벤트가 나타나지 않도록 어떤 조치도 취하지 않는 것이 좋습니다. 그러나 이러한 옵션은 구현을 선택하는 경우 옵션으로 표시됩니다. 두 방법 모두 권장되지 않습니다. 위험을 감수하고 사용하십시오.

해결 방법

방법 1

기본 도메인 컨트롤러 정책에서 디렉터리 서비스 감사 설정을 비활성화하여 Active Directory의 모든 감사를 비활성화합니다.

방법 2

Control Access 권한을 관리하는 기본 프로세스는 각 속성에 할당된 searchFlags 특성을 사용합니다. msPKIRoamingTimeStamp). searchFlags는 10비트 액세스 마스크입니다. 비트 8(이진 액세스 마스크에서 0~7까지 계산 = 10000000 = 128 십진수)을 사용하여 기밀 액세스 개념을 구현합니다. AD 스키마에서 이 속성을 수동으로 수정하고 이러한 속성의 기밀 액세스를 비활성화할 수 있습니다. 그러면 장애 감사 로그가 생성되지 않습니다.

AD의 모든 속성에 대해 기밀 액세스를 비활성화하려면 ADSI Edit를 사용하여 스키마 마스터 역할을 보유한 DC의 스키마 명명 컨텍스트에 연결합니다. 수정할 적절한 속성을 찾습니다. 속성 이름은 이벤트 ID 566 또는 4662에 표시된 것과 약간 다를 수 있습니다.

현재 searchFlags 값에서 빼기 128을 입력하는 올바른 값을 결정하고, 결과를 searchFlags의 새 값으로 입력하여 640-128 = 512를 입력합니다. searchFlags의 현재 값이 128보다 작으면 아무 작업

도 하지 않을 수 있습니다. 잘못된 속성이 있거나 Confidential Access로 인해 감사 이벤트가 발생하지 않을 수 있습니다.

이벤트 ID 566 또는 4662 설명에 나열된 각 속성에 대해 이 작업을 수행합니다.

스키마 마스터를 다른 도메인 컨트롤러로 강제 복제한 다음 새 이벤트를 확인합니다.

다음 속성에서 오류를 감사하지 않도록 도메인 감사 정책을 수정합니다.

이 방법의 단점은 추가해야 하는 감사 항목 수가 많아 성능이 저하될 수 있다는 것입니다.

추가 정보:

Google 또는 다른 검색 엔진을 사용하여 GUID를 개체 이름으로 쉽게 변환할 수 있습니다. 다음은 google을 사용하여 검색하는 방법의 예입니다.

예: 사이트:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = 개인 정보 속성 집합
{6617e4ac-a2f1-43ab-b60c-11fbd1ffacf05} = ms-PKI-RoamingTimeStamp 특성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.