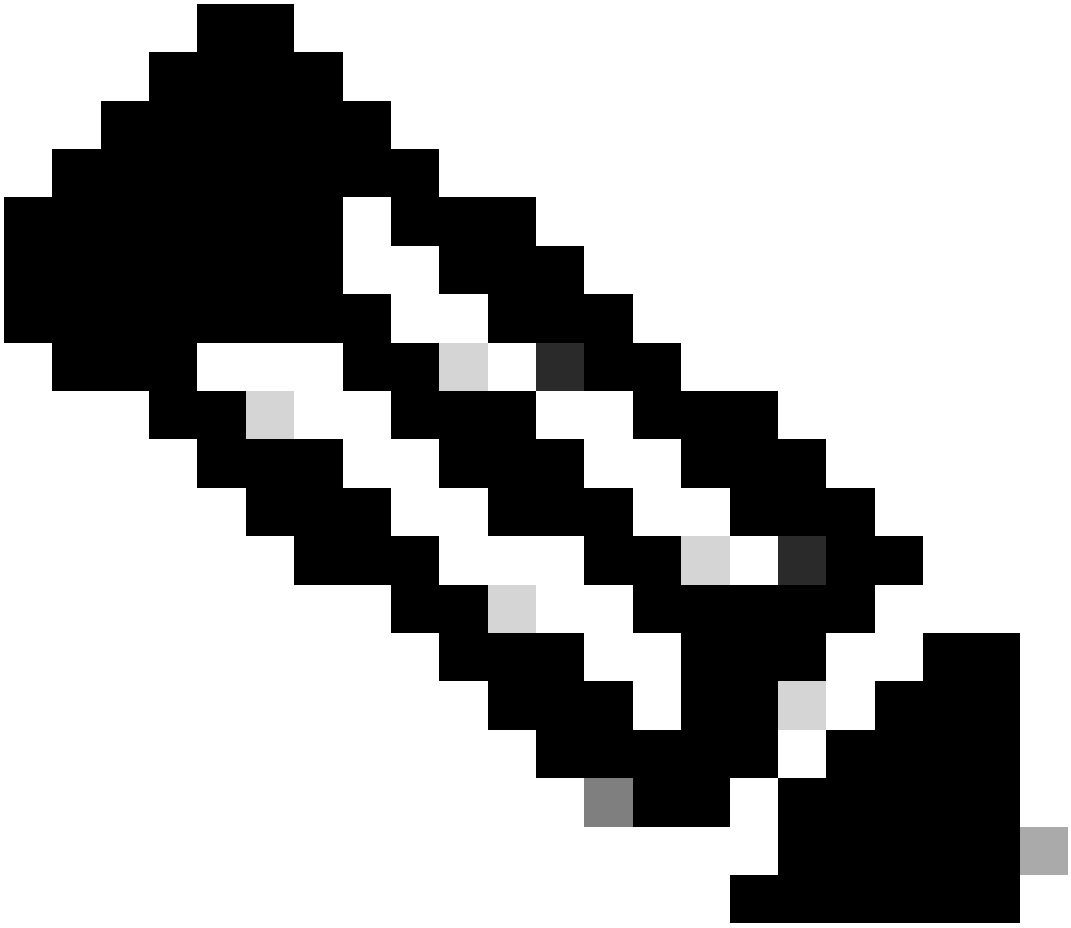
EventID 4662(Windows 2008)或EventID 566(Windows 2003)故障排除 — 类型：故障审核

目录

简介

本文档介绍安全事件ID 566和安全事件ID 4662，以及遇到它们时可以采取什么操作。这些事件可能会在作为Umbrella Insights部署的一部分运行的域控制器或成员服务器上发生。



注意：这些事件是可以预料到的，并且是正常的。首选且受支持的操作是不执行任何操作并忽略这些事件。

```
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
```

或者您收到此Windows 2008事件安全ID 4662。

```
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}
```

原因

Windows 2008引入了一个名为Private Information的新属性集，该属性集包含msPKI*属性。在设计上，这些属性受到保护，只有该SELF对象可以访问它们。您可以根据需要使用DSACLS命令验证对象上的权限。

粗略调查可能会使您相信此审核事件是由于试图写入这些受限制属性造成的。这些事件发生在默认的Microsoft审计策略下，该策略仅审计更改（写入），而不审计从Active Directory读取信息的尝试，因此可以清楚地看出这一点。

但是，实际情况并非如此，审核事件将明确列出请求的权限作为控制访问(0x100)。很遗憾，您不能向Private Information属性集授予CA(控制访问)权限。

解决方案

您可以放心地忽略这些消息。这是有意设计的。

建议您不要采取任何操作来防止这些事件出现。但是，如果您选择实施这些选项，则这些选项将作为选项显示。不建议使用以下任何解决方法：自担风险。

解决方法

方法 1

通过禁用默认域控制器策略中的目录服务审核设置，禁用Active Directory中的所有审核。

方法 2

管理Control Access权限的基础进程使用分配给每个属性(即：msPKIRoamingTimeStamp)。searchFlags是10位访问掩码。它使用位8(二进制访问掩码= 10000000 = 128十进制数从0到7)来实施机密访问的概念。您可以在AD方案中手动修改此属性并禁用这些属性的机密访问。这样会防止生成故障审核日志。

要为AD中的任何属性禁用机密访问，请使用ADSI Edit附加到拥有架构主角色的DC上的架构命名上下文。找到要修改的相应属性，其名称可能与事件ID 566或4662中显示的略有不同。

要确定正确的值，从当前searchFlags值中减去128，然后输入结果作为searchFlags的新值，因此640-128 = 512。如果searchFlags的当前值不执行任何操作，则您可能具有错误的属性或Confidential Access不会导致审核事件。

对Event ID 566 or 4662 description（事件ID 566或4662说明）中列出的每个属性执行此操作。

强制将架构主机复制到其他域控制器，然后检查是否有新事件。

修改域审核策略以不审核以下属性上的失败：

此方法的缺点是性能可能会降低，因为需要添加的审计条目数量很高。

更多信息：

使用Google或其他搜索引擎可以轻松将GUID转换为对象名称。下面是如何使用Google进行搜索的示例。

示例：站点：microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = 专用信息属性集
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = ms-PKI-RoamingTimeStamp属性

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。