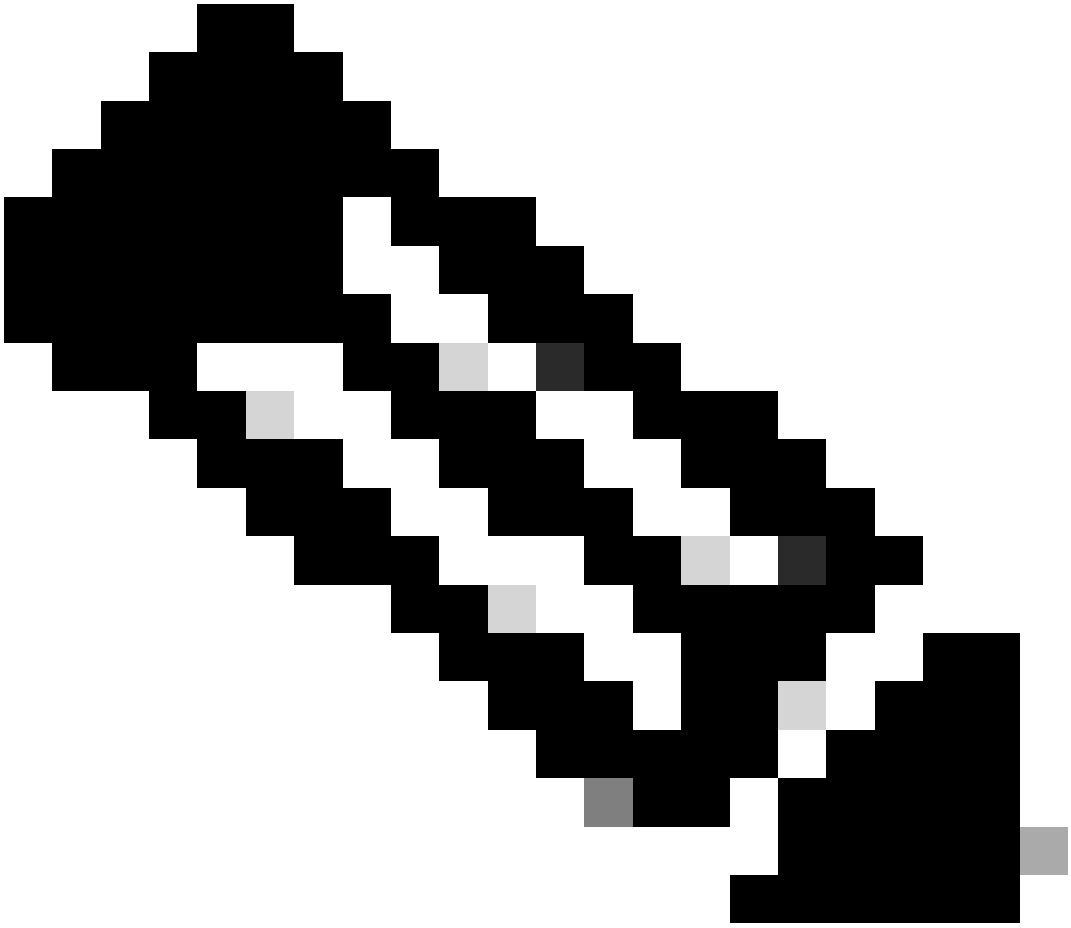
Identificação e Solução de Problemas de Evento 4662 (Windows 2008) ou EventID 566 (Windows 2003) - Tipo: Auditoria com Falha

Contents

Introdução

Este documento descreve a ID de evento de segurança 566 e a ID de evento de segurança 4662, e que ação pode ser tomada ao encontrá-las. Esses eventos podem ocorrer em Controladores de Domínio ou em um servidor membro em execução como parte da implantação do Umbrella Insights.



Note: Estes acontecimentos são de esperar e normais. A ação preferida e suportada é não fazer nada e ignorar esses eventos.

```
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
```

Ou você recebe a ID de segurança de evento 4662 do Windows 2008.

```
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}
```

Causa

O Windows 2008 introduziu um novo conjunto de propriedades chamado Private Information que inclui as propriedades msPKI*. Por design, essas propriedades são protegidas de forma que somente o objeto SELF possa acessá-las. Você pode usar o comando DSACLS para verificar as permissões no objeto conforme necessário.

Uma investigação rápida pode levá-lo a acreditar que esse evento de auditoria está sendo causado por uma tentativa de escrever nessas propriedades restritas. Isso é evidente pelo fato de que esses eventos ocorrem sob a política de auditoria padrão da Microsoft, que audita apenas as alterações (gravações), e não audita tentativas de ler informações do Ative Diretory.

No entanto, esse não é o caso, o evento de auditoria lista claramente a permissão que está sendo solicitada como Acesso de Controle (0x100). Infelizmente, você não pode conceder a permissão CA (Acesso de Controle) ao conjunto de propriedades Informações Particulares.

Solução

Você pode ignorar essas mensagens com segurança. Isto é por projeto.

Não é recomendável executar nenhuma ação para impedir o aparecimento desses eventos. No entanto, elas serão apresentadas como opções se você optar por implementá-las. Nenhuma solução alternativa é recomendada: use por sua conta e risco.

Soluções

Método 1

Desabilite toda a auditoria no Ative Diretory desabilitando a configuração de auditoria do Serviço de Diretório na política padrão do Controlador de Domínio.

Método 2

O processo subjacente que gerencia a permissão Acesso de Controle utiliza o atributo searchFlags que é atribuído a cada propriedade (ou seja: msPKIRoamingTimeStamp). searchFlags é uma máscara de acesso de 10 bits. Ele usa o bit 8 (contando de 0 a 7 em uma máscara de acesso binário = 10000000 = 128 decimal) para implementar o conceito de Acesso Confidencial. Você pode modificar manualmente esse atributo no Esquema do AD e desabilitar o Acesso Confidencial dessas propriedades. Isso evita que os logs de auditoria de falha sejam gerados.

Para desabilitar o Acesso Confidencial para qualquer propriedade no AD, use ADSI Edit para anexar ao contexto de nomeação de Esquema no DC que contém a Função de Mestre de Esquema. Localize as propriedades apropriadas a serem modificadas, seus nomes podem ser ligeiramente diferentes do que é mostrado nos IDs de evento 566 ou 4662.

Para determinar o valor correto a ser inserido, subtraia 128 do valor atual de searchFlags e insira o resultado como o novo valor de searchFlags, portanto 640-128 = 512. Se o valor atual de searchFlags for < 128, você poderá não fazer nada, pode ter a propriedade incorreta ou Acesso Confidencial não está causando o evento de auditoria.

Faça isso para cada propriedade listada na descrição da ID de evento 566 ou 4662.

Force a replicação do Mestre de esquema para os outros controladores de domínio e, em seguida, verifique se há novos Eventos.

Modifique a diretiva de auditoria de domínio para não auditar falhas nestas propriedades:

A desvantagem desse método é que o desempenho pode ser prejudicado devido ao alto número de entradas de auditoria que precisam ser adicionadas.

Mais informações:

Traduzir GUID para nomes de objetos é fácil usando o google ou outro mecanismo de busca. Aqui está um exemplo de como pesquisar usando o google.

Exemplo: site:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = Conjunto de Propriedades de Informações Particulares
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = Atributo ms-PKI-RoamingTimeStamp

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.