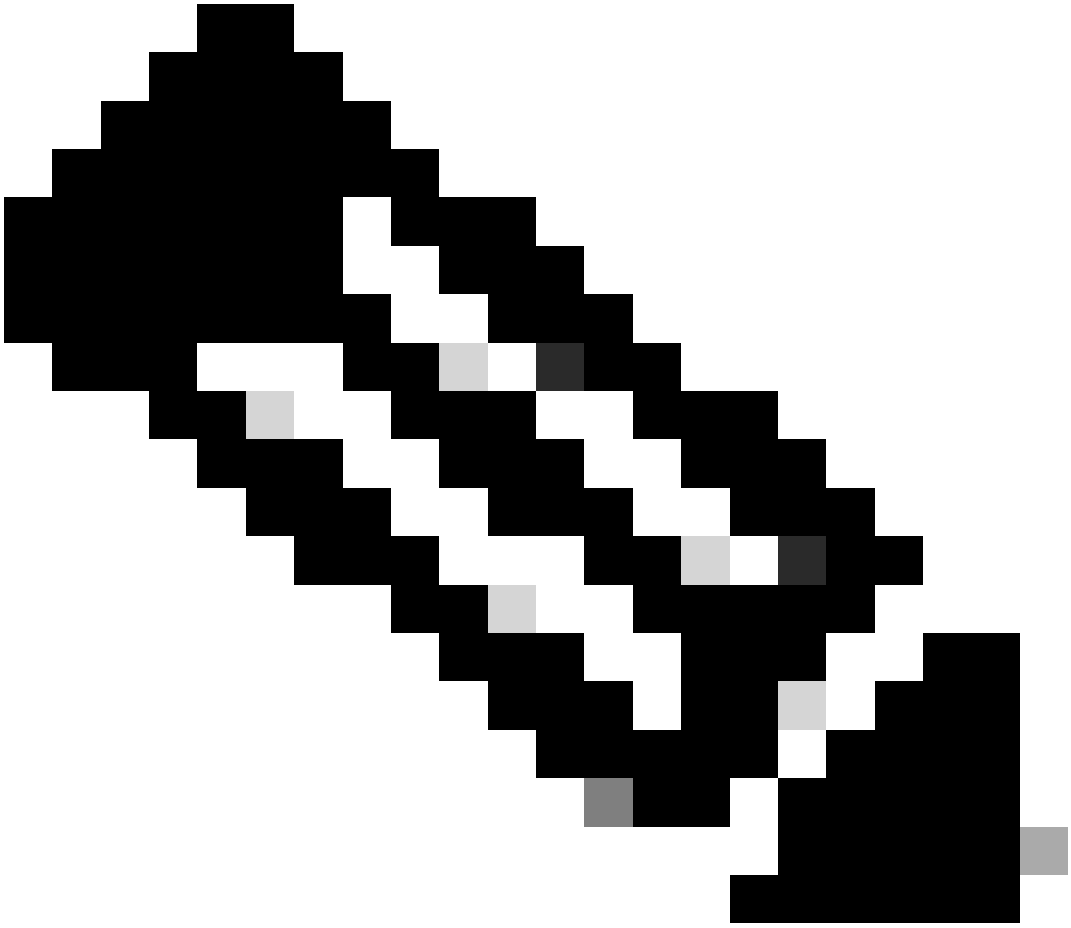
Solucionar problemas de EventID 4662 (Windows 2008) o EventID 566 (Windows 2003) - Tipo: Auditoría de fallos

Contenido

Introducción

Este documento describe el ID de evento de seguridad 566 y el ID de evento de seguridad 4662, y qué acción se puede tomar al encontrarlos. Cabe esperar que estos eventos se produzcan en controladores de dominio o en un servidor miembro que se ejecute como parte de la implementación de Umbrella Insights.



Nota: Estos acontecimientos son de esperar y normales. La acción preferida y admitida es no hacer nada e ignorar estos 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
```

O bien, recibirá el identificador de seguridad de eventos de Windows 2008 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}
```

Causa

Windows 2008 introdujo un nuevo conjunto de propiedades llamado Private Information que incluye las propiedades msPKI*. Por diseño, estas propiedades están protegidas de tal manera que sólo el objeto SELF puede tener acceso a ellas. Puede utilizar el comando DSACLS para comprobar los permisos del objeto según sea necesario.

Una investigación superficial puede hacerle creer que este evento de auditoría se debe a un intento de escribir en estas propiedades restringidas. Esto es evidente por el hecho de que estos eventos se producen bajo la directiva de auditoría predeterminada de Microsoft que sólo audita los cambios (escrituras) y no audita los intentos de leer información de Active Directory.

Sin embargo, este no es el caso, el evento de auditoría enumera claramente el permiso que se solicita como Control Access (0x100). Desafortunadamente, no puede conceder el permiso CA (Control Access) al conjunto de propiedades Private Information.

Solución

Puede tranquilamente ignorar estos mensajes. Esto es por diseño.

No se recomienda realizar ninguna acción para evitar que aparezcan estos eventos. Sin embargo, se presentan como opciones si elige implementarlas. No se recomienda ninguna solución alternativa: uso bajo su propio riesgo.

Soluciones alternativas

Método 1

Deshabilite todas las auditorías en Active Directory deshabilitando la configuración de auditoría del servicio de directorio en la directiva predeterminada del controlador de dominio.

Método 2

El proceso subyacente que administra el permiso Control Access utiliza el atributo searchFlags que se asigna a cada propiedad (por ejemplo: msPKIRoamingTimeStamp). searchFlags es una máscara de acceso de 10 bits. Utiliza el bit 8 (contando de 0 a 7 en una máscara de acceso binario = 10000000 = 128 decimal) para implementar el concepto de acceso confidencial. Puede modificar manualmente este atributo en el esquema de AD y deshabilitar el acceso confidencial de estas propiedades. Esto evita que se generen los registros de auditoría de errores.

Para deshabilitar el acceso confidencial para cualquier propiedad de AD, utilice ADSI Edit para

asociarlo al contexto de nomenclatura Esquema en el DC que tiene la función de maestro de esquema. Busque las propiedades adecuadas que desee modificar; su nombre puede ser ligeramente diferente del que se muestra en Event ID 566 o 4662.

Para determinar el valor correcto para introducir el valor 128 del valor actual de searchFlags, introduzca el resultado como el nuevo valor de searchFlags, por lo tanto 640-128 = 512. Si el valor actual de searchFlags es < 128 no hace nada, es posible que tenga la propiedad incorrecta o que Confidential Access no esté provocando el evento de auditoría.

Realice esta acción para cada propiedad enumerada en la descripción del ID de evento 566 o 4662.

Fuerce la replicación del maestro de esquema en los otros controladores de dominio y, a continuación, compruebe si hay nuevos eventos.

Modifique la directiva de auditoría de dominio para no auditar errores en estas propiedades:

La desventaja de este método es que el rendimiento puede degradarse debido al gran número de entradas de auditoría que es necesario agregar.

Más información:

Traducir GUID a nombres de objetos es fácil con google u otro motor de búsqueda. A continuación se muestra un ejemplo de cómo realizar búsquedas con google.

Ejemplo: sitio:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).