ABILITARE L'AUDITING SUL DNS IN WINDOWS 2003 SERVER

1. INTRODUZIONE

Uno degli aspetti principali della sicurezza è il mantenimento e per farlo correttamente l'amministratore deve essere in grado di tenere traccia delle modifiche che sono state svolte per l'ambiente. Ci sono un sacco di sfide in questo settore e una delle più grande sfida è quella di registro ciò che deve essere connesso senza sopraffare il server.

Quando stavo lavorando nel team di piattaforme mi ricordo che ho ricevuto una chiamata da un cliente dicendo che vuole sapere chi ha cancellato un record per la sua zona DNS. Prima domanda era: hai una politica di revisione contabile per consentire DNS? Era come: che cos'è? Dopo la revisione del suo ambiente ho visto che il controllo è stato abilitato, ma non per gli oggetti di Active Directory (la sua zona DNS è stato integrato in AD).

Questo post verrà a piedi attraverso la configurazione di revisione di una zona DNS (AD integrata) in Windows Server 2003.

2. PREPARARE L'AMBIENTE

Ci sono tre passi per preparare l'ambiente:
1. Verificare se la politica di controllo denominato audit Directory Service Access è attivata e che cosa è l'impostazione.
2. Permesso di Auditing sulla Zona DNZ che si desidera controllare.
3. Utilizzare il Visualizzatore eventi per scoprire quale oggetto di modifica (in questo caso l'esempio sarà una eliminazione di oggetto).

3. LA CONFIGURAZIONE DEL CRITERIO DI CONTROLLO

Aprire la predefiniti controller di dominio, e verificare se la politica ha evidenziato di seguito è stato selezionato proprio così:

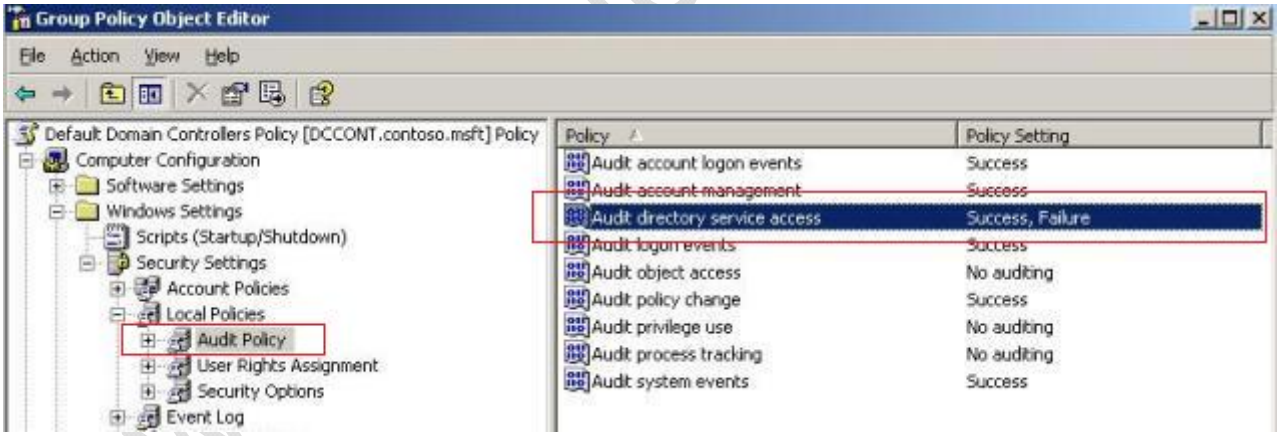

Fig.1

Nel mio caso ho cambiato di audit successo e il fallimento, ma la configurazione finale sarà in base alle vostre esigenze.

4. LA CONFIGURAZIONE DEL DNS ZONE

Ora che abbiamo attivato la politica di controllo a tutti i controller di dominio nel dominio, abbiamo bisogno di cambiare la zona DNS. Per fare che seguire la seguente procedura:

1) Aprire ADSIEdit (Start / Esegui / ADSIEdit.msc)
2) Fare clic su ADSI Edit e fare clic su Connect To ...
3) Nella finestra Impostazioni di connessione, configurare come mostra di seguito:

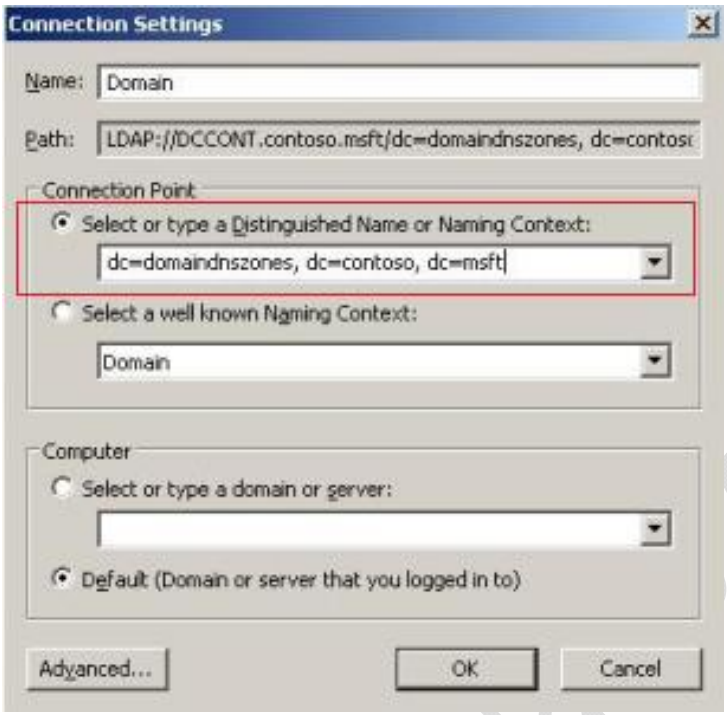

Fig.2

Nota: Modificare il dc = per riflettere il nome del dominio.

4) Dopo di che fare clic su OK.
5) Ora, espandere il contenitore fino ad arrivare allo stesso nodo come mostrato di seguito:

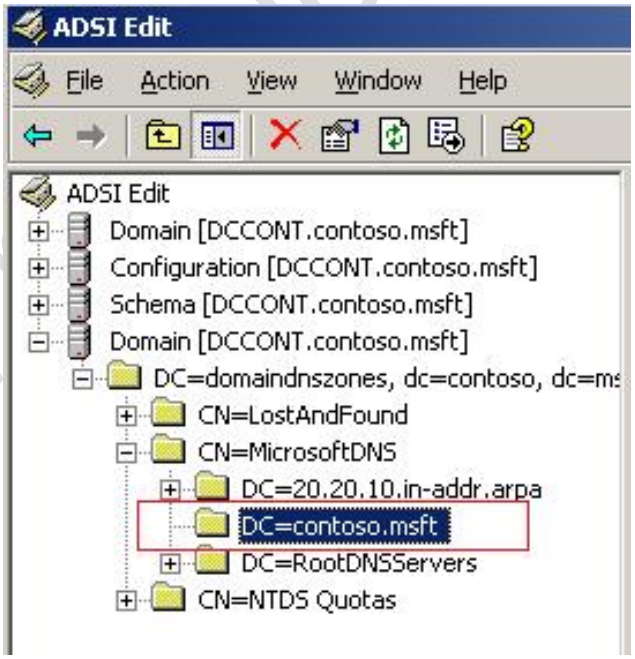

Fig.3

5) Right click in nome della zona situata sotto CN = MicrosoftDNS e fare clic su Proprietà.
6) Fare clic su Protezione e quindi su Avanzate.
7) Fare clic in Auditing e fare clic su Aggiungi.
8) Digitare Everyone e fare clic su OK. Aggiungere il seguente tipo di accesso:
• Scrivi tutte le proprietà
• Elimina

• Elimina sottostruttura

9) Fare clic su OK su tutte e tre finestre.

Ora siamo pronti ad accedere!

5. TEST

Per provare a cancellare il record chiamato work01 ed ecco che cosa si dovrebbe vedere il registro degli eventi di sicurezza:

```
Event Type:       Success Audit
Event Source:     Security
Event Category:             Directory Service Access
Event ID:           566
Date:                3/5/2008
Time:                7:33:51 PM
User:                CONTOSO\Administrator
Computer:         DCCONT
Description:
Object Operation:
            Object Server:   DS
            Operation Type:            Object Access
            Object Type:      dnsNode
            Object Name:
DC=work01,DC=contoso.msft,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=msft
            Handle ID:          -
            Primary User Name:       DCCONT$
            Primary Domain:            CONTOSO
            Primary Logon ID:          (0x0,0x3E7)
            Client User Name:         Administrator
            Client Domain:  CONTOSO
            Client Logon ID:             (0x0,0x19062D)
            Accesses:           Write Property

            Properties:
            Write Property
                        Default property set
                                    dnsRecord
                                    dNSTombstoned
            dnsNode

            Additional Info:
            Additional Info2:
            Access Mask:    0x20
```

Nota: i seguenti punti in rosso (dall'alto verso il basso):
• Il tipo di evento: l'utente è stato in grado di eseguire correttamente questa operazione.
• Categoria: l'oggetto è stato classificato come un oggetto DS.
• User: il nome dell'utente che ha effettuato questa operazione.
• Nome oggetto: il percorso completo da dove l'oggetto si trovava.
• dNSTombstoned: questo è probabilmente l'unico che non è amichevole. Questo attributo viene registrato ogni volta che un oggetto viene eliminato. Per ulteriori informazioni, consultare il DNS-tombstoned attributo a MSDN.

6. CONLCUSIONE

Questa semplice azione può aiutare a tenere traccia delle modifiche sulla zona DNS e prevenire problemi di conformità di sicurezza quando revisori approccio a rivedere il proprio ambiente.