

Re: Display All Locked Accounts in an OU

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.scripting/2005-10/msg00162.html>

- *From:* "Al Dunbar [MS-MVP]" <alan-no-drub-spam@xxxxxxxxxxxxx>
 - *Date:* Sat, 8 Oct 2005 18:04:12 -0600
-

"script-newb" <drweb@xxxxxxxxxxxxx> wrote in message
news:1128732766.377807.144940@xx

- > Hey All,
- >
- > I have this script below I used from its source
- > <http://www.rlmuller.net>
- >
- > I am having a very hard time to alter this to make it search a
- > particular OU and its sub-ou's for locked out accounts.

How are you trying to do this?

Richard's script uses the WinNT provider, likely because it is simpler for this particular task. But WinNT knows nothing of OU's – for that you will need the LDAP provider. But it might (or might not) still be simpler to determine the lockout status using WinNT.

- > I cannot
- > search the entire domain like this script is doing due to logistics.

You mean that you cannot search all domain controllers, or that you cannot search outside of your own OU(s)?

- > FWIW:
- > I know that when a user gets locked out in my domain it simultaneously
- > gets locked on a local DC and on our Root DC then takes 10–15 minutes
- > to show locked on all other DC's (10 total). I see this script is
- > getting all attributes from all DC's but I only would need it to look
- > at the 2 out of my 10 DC's since I know they would be the two most
- > accurate.

What accuracy means depends on what it is you are looking for. If you are simply looking for all those accounts (in a certain OU) that are locked out, you need only look at one domain controller. The only reason to look at more domain controllers (or all, as Richard's script does) is to determine when (and where) the last failed password attempt took place.

Re: Display All Locked Accounts in an OU

If you are concerned that checking one domain controller might result in your missing an account that locked itself a minute ago, but whose status has not yet replicated to the DC in question, then just wait 15 minutes before running the script. Trying to get an absolutely accurate picture of the state of all accounts at a particular instant in time does not seem to be something that has any particular importance.

- > **I only mentions the above^^^, due to not wanting to take too much
- > bandwidth searching all DC's, if it is minuscule then disregard and
- > let me know.
- >
- > I am somewhat of a newbie at adsi-vbscript-wsh scripting so sorry for the
- > long windedness of this thread.
- >
- > Any and all help would be appreciated.
- > Anybody have an easier method? (must use vbscript)

First we need to know exactly what it is you want to do? I am guessing it is something like this: "identify all accounts within a given OU and its sub OUs that are currently locked out". If that is so, I would use an ADO query to enumerate all accounts in the given OU(s), and test each to determine if it is locked out. I'm bad at remembering details, but this might be something more easily done with WinNT than LDAP.

This would be a quite different script, so trying to modify what you have to make it what you want is likely where you are having difficulty.

/AI

- > Clay
- >
- > ----- Script -----
- > ' LockedUsers.vbs
- > ' VBScript program to find user accounts in Active Directory that are
- > ' locked out, then determine when they were locked out and on which
- > ' Domain Controller.
- > '
- > ' -----
- > ' Copyright (c) 2003 Richard L. Mueller
- > ' Hilltop Lab web site - <http://www.rlmueller.net>
- > ' Version 1.0 - March 17, 2003
- > ' Version 1.1 - May 9, 2003 - Account for error in IADsLargeInteger
- > ' property methods HighPart and Lowpart.
- > ' Version 1.2 - January 25, 2004 - Modify error trapping.
- > ' Version 1.3 - March 18, 2004 - Modify NameTranslate constants.
- > '
- > ' You have a royalty-free right to use, modify, reproduce, and
- > ' distribute this script file in any way you find useful, provided that
- > ' you agree that the copyright owner above has no warranty,
- > ' obligations, or liability for such use.

Re: Display All Locked Accounts in an OU

```
>
> Option Explicit
>
> Dim objRootDSE, strConfig, objConnection, objCommand, strQuery
> Dim objRecordSet, objDC
> Dim strDNSDomain, objShell, lngBiasKey, lngBias, k, arrstrDCs()
> Dim strDN, dtmDate, objDate, lngDate, strUser, strNTName
> Dim objList1, objList2, objList3, j, intBadCount
> Dim strBase, strFilter, strAttributes, objWinNTUser
> Dim objTrans, strNetBIOSDomain, objDomain, arrstrNTNames()
> Dim lngHigh, lngLow
>
> ' Constants for the NameTranslate object.
> Const ADS_NAME_INITTYPE_GC = 3
> Const ADS_NAME_TYPE_NT4 = 3
> Const ADS_NAME_TYPE_1779 = 1
>
> ' Determine DNS domain name.
> Set objRootDSE = GetObject("LDAP://RootDSE")
> strDNSDomain = objRootDSE.Get("defaultNamingContext")
>
> > ' Use the NameTranslate object to convert the DNS domain name
> > ' to the NetBIOS domain name.
> Set objTrans = CreateObject("NameTranslate")
> objTrans.Init ADS_NAME_INITTYPE_GC, ""
> objTrans.Set ADS_NAME_TYPE_1779, strDNSDomain
> strNetBIOSDomain = objTrans.Get(ADS_NAME_TYPE_NT4)
> > ' Remove trailing backslash.
> strNetBIOSDomain = Left(strNetBIOSDomain, Len(strNetBIOSDomain) - 1)
>
> > ' Find locked out user accounts in domain
> > ' create array of sAMAccountName's
> Set objDomain = GetObject("WinNT://" & strNetBIOSDomain)
> objDomain.Filter = Array("user")
> k = 0
> For Each objWinNTUser In objDomain
> If objWinNTUser.IsAccountLocked = True Then
> ReDim Preserve arrstrNTNames(k)
> arrstrNTNames(k) = objWinNTUser.name
> k = k + 1
> End If
> Next
>
> > If k = 0 Then
> > Wscript.Echo "No user accounts locked out in domain"
> > Wscript.Quit
> > End If
>
> > ' Use dictionary objects to track latest badPasswordTime,
> > ' badPwdCount, and Domain Controller for each locked out user.
> Set objList1 = CreateObject("Scripting.Dictionary")
```

Re: Display All Locked Accounts in an OU

```
> objList1.CompareMode = vbTextCompare
> Set objList2 = CreateObject("Scripting.Dictionary")
> objList2.CompareMode = vbTextCompare
> Set objList3 = CreateObject("Scripting.Dictionary")
> objList3.CompareMode = vbTextCompare
>
> ' Obtain local Time Zone bias from machine registry.
> Set objShell = CreateObject("Wscript.Shell")
> lngBiasKey = objShell.RegRead("HKLM\System\CurrentControlSet\Control\"
>
> & "TimeZoneInformation\ActiveTimeBias")
> If UCase(TypeName(lngBiasKey)) = "LONG" Then
> lngBias = lngBiasKey
> ElseIf UCase(TypeName(lngBiasKey)) = "VARIANT()" Then
> lngBias = 0
> For k = 0 To UBound(lngBiasKey)
> lngBias = lngBias + (lngBiasKey(k) * 256^k)
> Next
> End If
>
> ' Determine configuration context.
> strConfig = objRootDSE.Get("configurationNamingContext")
>
> ' Use ADO to search Active Directory for ObjectClass nTDSDSA.
> ' This will identify all Domain Controllers.
> Set objCommand = CreateObject("ADODB.Command")
> Set objConnection = CreateObject("ADODB.Connection")
> objConnection.Provider = "ADsDSOObject"
> objConnection.Open = "Active Directory Provider"
> objCommand.ActiveConnection = objConnection
>
> strBase = "<LDAP:// & strConfig & ">"
> strFilter = "(objectClass=nTDSDSA)"
> strAttributes = "AdsPath"
> strQuery = strBase & ";" & strFilter & ";" & strAttributes & ";subtree"
>
> objCommand.CommandText = strQuery
> objCommand.Properties("Page Size") = 100
> objCommand.Properties("Timeout") = 60
> objCommand.Properties("Cache Results") = False
>
> Set objRecordSet = objCommand.Execute
>
> ' Enumerate parent objects of class nTDSDSA. Save Domain Controller
> ' DNS host names in dynamic array arrstrDCs.
> k = 0
> Do Until objRecordSet.EOF
> Set objDC =
> GetObject(GetObject(objRecordSet.Fields("AdsPath")).Parent)
> ReDim Preserve arrstrDCs(k)
> arrstrDCs(k) = objDC.DNSHostName
```

Re: Display All Locked Accounts in an OU

```
> k = k + 1
> objRecordSet.MoveNext
> Loop
>
> ' Use ADO to retrieve all user objects from each Domain Controller.
> strFilter = "(&(objectCategory=person)(objectClass=user))"
> strAttributes = "distinguishedName,sAMAccountName,"
> & "badPasswordTime,badPwdCount"
> For k = 0 To Ubound(arrstrDCs)
> strBase = "<LDAP:// & arrstrDCs(k) & "/" & strDNSDomain & ">"
> strQuery = strBase & ";" & strFilter & ";" & strAttributes
> & ";subtree"
> objCommand.CommandText = strQuery
> On Error Resume Next
> Set objRecordSet = objCommand.Execute
> If Err.Number <> 0 Then
> On Error GoTo 0
> WScript.Echo "Domain Controller not available: " & arrstrDCs(k)
> Else
> On Error GoTo 0
> Do Until objRecordSet.EOF
> strNTName = objRecordSet.Fields("sAMAccountName")
> ' Check each user to see if in array of locked out accounts.
> For j = 0 To UBound(arrstrNTNames)
> If UCase(strNTName) = UCase(arrstrNTNames(j)) Then
> ' User locked out, retrieve badPasswordTime.
> strDN = objRecordSet.Fields("distinguishedName")
> lngDate = objRecordSet.Fields("badPasswordTime")
> intBadCount = objRecordSet.Fields("badPwdCount")
> On Error Resume Next
> Set objDate = lngDate
> If Err.Number <> 0 Then
> On Error GoTo 0
> dtmDate = #1/1/1601#
> Else
> On Error GoTo 0
> lngHigh = objDate.HighPart
> lngLow = objDate.LowPart
> If lngLow < 0 Then
> lngHigh = lngHigh + 1
> End If
> If (lngHigh = 0) And (lngLow = 0) Then
> dtmDate = #1/1/1601#
> Else
> dtmDate = #1/1/1601# + (((lngHigh * (2 ^ 32))
> + lngLow)/600000000 - lngBias)/1440
> End If
> End If
> If objList1.Exists(strDN) Then
> If dtmDate > objList1(strDN) Then
> ' Later badBadPasswordTime found, save info from this DC.
```

Re: Display All Locked Accounts in an OU

```
> objList1(strDN) = dtmDate  
> objList2(strDN) = intBadCount  
> objList3(strDN) = arrstrDCs(k)  
> End If  
> Else  
> ' First time user found, save info from this DC.  
> objList1.Add strDN, dtmDate  
> objList2.Add strDN, intBadCount  
> objList3.Add strDN, arrstrDCs(k)  
> End If  
> End If  
> Next  
> objRecordSet.MoveNext  
> Loop  
> End If  
> Next  
>  
> ' Output information on each locked out user.  
> For Each strUser In objList1  
> Wscript.Echo strUser & " ; " & objList1(strUser) & " ; "  
> & objList2(strUser) & " ; " & objList3(strUser)  
> Next  
>  
> ' Clean up.  
> objConnection.Close  
> Set objRootDSE = Nothing  
> Set objConnection = Nothing  
> Set objCommand = Nothing  
> Set objRecordSet = Nothing  
> Set objTrans = Nothing  
> Set objDomain = Nothing  
> Set objWinNTUser = Nothing  
> Set objDC = Nothing  
> Set objDate = Nothing  
> Set objList1 = Nothing  
> Set objList2 = Nothing  
> Set objList3 = Nothing  
> Set objShell = Nothing  
>  
> -----End Script-----  
>  
> Thanks again  
>
```

.

-
- **Follow-Ups:**
 - ◆ **Re: Display All Locked Accounts in an OU**

Re: Display All Locked Accounts in an OU

◇ *From: script-newb*

• *References:*

◆ *Display All Locked Accounts in an OU*

◇ *From: script-newb*

• Prev by Date: *Re: [MSH] recursive calling script*

• Next by Date: *Re: 600 User Profiles*

• Previous by thread: *Display All Locked Accounts in an OU*

• Next by thread: *Re: Display All Locked Accounts in an OU*

• Index(es):

◆ *Date*

◆ *Thread*