

Re: Authentication Auditing

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-10/0284.html>

From: Steven L Umbach (*n9rou_at_nospam-comcast.net*)

Date: 10/22/05

Date: Fri, 21 Oct 2005 18:50:51 -0500

The failed logon for a "local" computer user for a domain computer would only show in the security log of the domain computer itself – not the domain controller assuming that auditing of logon events was indeed enabled for that domain computer. Check Local Security Policy of the computer in question to make sure that it indeed does show that auditing of logon events is enabled for success and failure. For Windows 2000 computers look at the effective setting. Then try clearing the current security log to make sure it is not full and try again. Also try a logging onto the local console for that computer to see if any logon events are recorded or not. — Steve

"Brad Baker" <brad@nospam.nospam> wrote in message news:uiKWQzn1FHA.3780@TK2MSFTNGP12.phx.gbl...

> Steven –

>

> *I think I am either misunderstanding your answer or you aren't understanding my question :-)* Perhaps an example would clarify.

>

> *We have two domain controllers: DC1, DC2*

> *A whole bunch of domain workstations: IIS1, IIS2, IIS3*

> *All of the machines above are part of a domain – lets call it dom1.*

>

> *"Audit account logon events" and "Audit logon events" are enabled for success and failures in the domain security policy for dom1.*

>

> *Now lets say that I attempt to log into a secure website on IIS1 using the dom1\administrator account and it fails.*

> *I do see an event in the DC1 or DC2 security log. (So far so good)*

>

> *Now I attempt to log into the same secure website on IIS1 using*

> *IIS1\administrator.*

> *I don't see an event in DC1, DC2 or IIS1 security log. What do I need to do to make sure this event gets logged?*

>

> *Thanks!*

> *Brad Baker*

>

>

>

microsoft.public.win2000.security: Re: Authentication Auditing

> "Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message
> news:F7CdnbW54LY82sTeRVn-uw@comcast.com...

>> You have to enable auditing of "logon events" for the domain computers
>> which could be done in Domain Security Policy. Then you will see a type 2
>> logon event recorded when a domain user logs onto the domain computer in
>> that domain computer's security log. The reason "audit logon events" does
>> not work for domain computers is because the account logon event is only
>> recorded on the computer that authenticates the user which is a domain
>> controller for domain users. --- Steve

>>
>>

>> "Brad Baker" <brad@nospam.nospam> wrote in message
>> news:e2vu5dn1FHA.164@TK2MSFTNGP10.phx.gbl...

>>> We are trying to ensure that we have auditing enabled for all login
>>> attempts
>>> to either domain or local machine accounts.

>>>

>>> I believe that we have enabled auditing for domain level accounts
>>> through
>>> GPO. We have enabled "audit account logon events" and "audit logon
>>> events"

>>> under Local Policies -> Audit Policy. I am seeing login attempts for
>>> domain

>>> accounts on our domain controller's security logs but I am not seeing
>>> login

>>> attempts for local accounts either in the domain controller's security
>>> logs

>>> or on the local machine security logs.

>>>

>>> How do we enable logging of authentication attempts against local (not
>>> domain) accounts? Is this another GPO setting? Are we looking in the
>>> wrong

>>> place? Alternatively, is there a setting at the local machine level that
>>> needs to be set? Any information or assistance would be appreciated.

>>>

>>> Thanks,

>>> Brad Baker

>>>

>>

>>

>

>