

Re: Security Logging in ADAM

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg01747

- *From:* "Lee Flight" <lef@xxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 20 Feb 2007 22:02:21 -0000
-

Hi

the audit events

Successful Network Logon:
User Name: ADAM_Manager
Domain: XXXXXXXX
Logon ID: (0x0,0x16BFCCA)
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: XXXXXXXX

are audits of domain accounts logons you get these with "Audit logon events" enabled in the security policy of the server. For the ADAM native users logons to be audited you need "Audit account logon events" enabled in the server security policy.

Lee Flight

"LM" <merrittf@xxxxxxxx> wrote in message
<news:1171994024.170916.154990@xx>

On Feb 16, 7:23 am, "Joe Kaplan"
<joseph.e.kap...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Can you explain what you mean by your Tomcat app doing an anonymous login to authenticate the user? On the surface, that seems to be a conflicting statement. How does an anonymous login authenticate anyone?

If a bind was performed against ADAM, there should be a matching audit event in the security event log on the ADAM machine assuming that logon events

Re: Security Logging in ADAM

are audited and the service account has the privilege enabled to generate security audits.

Joe K.

Joe Kaplan—MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming" <http://www.directoryprogramming.net>
—"LM" <merri...@xxxxxxx> wrote in message

news:1171583540.883253.301550@xx

On Feb 15, 2:58 pm, "Lee Flight" <l...@xxxxxxxxxxxxxxxx> wrote:

Hi

what security events are you referring to, logon events?
If so have you enabled logon events audit in the security policy of the ADAM instance server?

If that's not what you are asking please post an example of the event that you are seeing when you get positive.

Thanks
Lee Flight

"LM" <merri...@xxxxxxx> wrote in message

news:1171562913.937503.58860@xx

Re: Security Logging in ADAM

Trying to run down a problem connecting I poted about earlier, I've been looking at the Windows Security event log. I'm a little bewildered.

I have the ADAM service account user granted permission to log security events, and when I log in as that user using ADSI edit, I get Security events describing all that from the ADAM service account.

However, when I run a webapp under Tomcat, and succesfully authenticate against ADAM, I get NO security ((or ADAM) events from the ADAM service account. Since authentication is succeeding (here on my local machine), I'm pretty confident the Tomcat JNDI realm is establishing a connection and doing the lookup. Shouldn't I be getting security events for this?

I'm wondering if there is something I need to configure in ADAM to get more detailed logging. Also,

Re: Security Logging in ADAM

wondering if there are
objects in the
Configuration partition that
I can examine to get useful
information.

Any thoughts?

Many thanks,

Im- Hide quoted text -

- Show quoted text -

Logon events are what I had in mind, yes.

When I log in using ADSI edit, on my local machine here in
San Diego,
I get an event like this:

Successful Network Logon:
User Name: ADAM_Manager
Domain: XXXXXXXX
Logon ID: (0x0,0x16BFCCA)
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: XXXXXXXX
Logon GUID:
{00000000-0000-0000-0000-000000000000}

And similarly logoff:

Re: Security Logging in ADAM

User Logoff:
User Name: ADAM_Manager
Domain: XXXXXXXXXX
Logon ID: (0x0,0x16BFCCA)
Logon Type: 3

I had to email an Admin person back east to grant perm to the ADAM service account there, and haven't heard back.

But, as you see, when I log in with ADSI Edit, I get a security event as one might expect.

However, when the login takes place as an anonymous login from my Tomcat JNDI realm, to authenticate a user of my web application (which succeeds, so I have to assume the connection happened) no entry of any kind from the ADAM service account appears in the Security log, the ADAM event log, or elsewhere, as far as I can tell.

I was hoping to use the information to determine if ADAM was rejecting the Tomcat connection, or if the communication never took place at all, or what have you.

Of course, in the longer term I'm going to have to learn more about monitoring and maintaining my directory instance in any case.

Thanks for getting back to me.

Re: Security Logging in ADAM

Lincoln– Hide quoted text –

– Show quoted text –

When you configure the JNDI_Realm for Tomcat to use to AuthN/AuthZ users against a directory, you provide the information needed to operate against the directory on a context. As in:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Context>
<Realm
className="org.apache.catalina.realm.JNDIRealm"
debug="99"
connectionURL="ldap://localhost:389/
userPattern="cn={0}.cn=Users.ou=SomeOU,o=SomeO"
roleBase="cn=Groups.OU=SomeOU,O=SomeO"
roleName="cn"
roleSearch="member={0}">
</Realm>
</Context>
```

If you are using Declarative Security (which is to say, security on containers through Tomcat), Tomcat will put up a login dialogue when an attempt is made to access the resource through a browser, to collect the username and password.

You can provide credentials in the realm for login, or leave them out and, if anonymous login is enabled in ADAM, it will bind anonymously and authenticate the logged in user using the password provided and return the assigned roles in the request object. This anonymous login is probably (let's say certainly) not best practice, but we are just getting started and it was quick.

BTW, we also bind to ADAM at Tomcat startup to pull some certs out that we have in there, and I don't see that in the log either. However, as I said, it all seems to work, so the connection is happening somehow. I'm mystified.

Thanks for your reply. Other thoughts are most welcome.

Regards,

Lincoln