

Re: IIS 6 Anonymous / SUS always 401.3

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-05/0316.html>

From: David Wang [Msft] (someone_at_online.microsoft.com)

Date: 05/27/05

Date: Fri, 27 May 2005 12:30:21 -0700

401.3 when you ONLY have anonymous authentication enabled suggests that IIS successfully logged in as the configured anonymous user account (whatever it is). However, this user identity lacks access to the requested resource.

1. I would check the IIS configuration to determine the EXACT user identity used as the anonymous user account. IIS defaults to IUSR_machinename, but applications can define and use their own identity.
2. Then, I would look at the filesystem ACLs on /autoupdate/getmanifest.asp and make sure that the identity in #1 has read access to the file. You can also check using FileMon from www.sysinternals.com to see what user identity IIS is using to fail to read this file
3. Finally, I would look at objects inside of the ASP page and make sure the identity in #1 can instantiate them.

The request to /clientwebservice/SusServerVersion.xml return 404 with Win32 error 3, ERROR_FILE_NOT_FOUND. So, it looks like the client is looking for files that are not on your server. I have no idea what /clientwebservice/SusServerVersion.xml does nor whether this is normal.

Have you verified that SUS is supported in your particular server configuration (is this domain/stand-alone server, Domain controller?) , and is SUS supposed to support anonymous access and if so, is there special configuration you need to make?

--

//David

IIS

<http://blogs.msdn.com/David.Wang>

This posting is provided "AS IS" with no warranties, and confers no rights.

//

"JoesCat" <JoesCat@discussions.microsoft.com> wrote in message news:84E8D792-122B-4E1A-8EA6-ADD8EC0A34CD@microsoft.com...

I've been at this one for several days now, checking everything I can find. I've posted in the SUS group, but now I think it's more an IIS specific issue.

My IIS 6 in Server 2003 is hosting only SUS, no other websites. It used to work fine with Automatic Updates, but something changed that is now preventing anonymous access to any website. Possibly SP1 for W2003, or maybe

I inadvertently changed something?

I have set the SUSAdmin site to use only Integrated Windows Authentication, and it works fine logging on locally as an Administrator. But, of course I

microsoft.public.inetsrvr.iis.security: Re: IIS 6 Anonymous / SUS always 401.3

need the Autoupdate site to use anonymous. I'm seeing many anonymous successful logons (and I'm not seeing failures) in the security event log. But, the IIS log shows 401.3, particularly with getmanifest.asp.

```
2005-05-27 12:07:03 W3SVC1 192.168.0.4 GET /wutrack.bin
V=1&U=29e8b22700465f4e9940622358c81679&C=au&A=d&I=&D=&P=5.0.893.2.0.1.0&L=en
-US&S=f&E=80190191&M=&X=050527120704143
80 - 192.168.0.109 Industry+Update+Control 200 0 0
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET
/clientwebservice/SusServerVersion.xml 0505271207 80 - 192.168.0.90
Industry+Update+Control 404 0 3
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD /iuident.cab 0505271207 80 -
192.168.0.90 Industry+Update+Control 200 0 0
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET /iuident.cab 0505271207 80 -
192.168.0.90 Industry+Update+Control 200 0 0
2005-05-27 12:07:46 W3SVC1 192.168.0.4 HEAD /iuident.cab 0505271207 80 -
192.168.0.90 Industry+Update+Control 200 0 0
2005-05-27 12:07:46 W3SVC1 192.168.0.4 GET /iuident.cab 0505271207 80 -
192.168.0.90 Industry+Update+Control 200 0 0
2005-05-27 12:07:46 W3SVC1 192.168.0.4 POST /autoupdate/getmanifest.asp - 80
- 192.168.0.90 Mozilla/4.0+(compatible;+Win32;+WinHttp.WinHttpRequest.5) 401
3 5
```

As a sidenote, I'm not sure what /clientwebservicess is, I see no such website.

I also get a 401.3 by manually trying to go to <http://servername/autoupdate/getmanifest.asp> . If I set it up to use logon, and login AS AN ADMINISTRATOR, I can access the page without 401.3.

Of course, check the permissions on the files - which I've done over and over and over again - I'm convinced they are fine! The website is set to use

the IUSR_machinename account, it is not disabled, and has Read and Execute to

the entire wwwroot folder and folders/files below. I even added ANONYMOUS LOGON to have the same permissions. Admins FC, System FC. NETWORK SERVICE, ASPNET, IIS_WPG, Users all have Read/Execute to the wwwroot tree, ASPNET . Still 401.3.

I've followed completely through KB812614.

I've uninstalled and reinstalled SUS and IIS.

I am seeing logons to the system when trying to access the /autoupdate/getmanifest.asp page:

Event Type: Success Audit

Event Source: Security

Event Category: Account Logon
Event ID: 680
Date: 5/27/2005
Time: 9:47:34 AM
User: BKUP01\IUSR_BKUP01
Computer: BKUP01
Description:
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon account: IUSR_BKUP01
Source Workstation: BKUP01
Error Code: 0x0

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 552
Date: 5/27/2005
Time: 9:47:34 AM
User: NT AUTHORITY\NETWORK SERVICE
Computer: BKUP01
Description:

Logon attempt using explicit credentials:
Logged on user:
User Name: NETWORK SERVICE
Domain: NT AUTHORITY
Logon ID: (0x0,0x3E4)
Logon GUID: -
User whose credentials were used:
Target User Name: IUSR_BKUP01
Target Domain: BKUP01
Target Logon GUID: -
Target Server Name: localhost
Target Server Info: localhost
Caller Process ID: 1328
Source Network Address: -
Source Port: -

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 540
Date: 5/27/2005
Time: 9:47:34 AM
User: BKUP01\IUSR_BKUP01
Computer: BKUP01
Description:

Successful Network Logon:
User Name: IUSR_BKUP01
Domain: BKUP01
Logon ID: (0x0,0x85BE5)
Logon Type: 8
Logon Process: Advapi
Authentication Package: Negotiate
Workstation Name: BKUP01
Logon GUID: -
Caller User Name: NETWORK SERVICE
Caller Domain: NT AUTHORITY
Caller Logon ID: (0x0,0x3E4)
Caller Process ID: 1328
Transited Services: -
Source Network Address: -
Source Port: -

I'm currently setting up auditing the getmanifest.asp file, to see if the security log picks up any failures to access it, nothing so far adding the

microsoft.public.inetserver.iis.security: Re: IIS 6 Anonymous / SUS always 401.3

IUSR_, NETWORK SERVICE, ANONYMOUS LOGON and such users for full auditing. There's got to be something simple I've overlooked. I'm leaning more towards something in the local policy that is awry, as I've been over the file permissions so thoroughly (or so I think).
--
-Joe