

Re: Basic Authentication fails with Error 401.2 where Integrated s

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetsrvr.iis.security/2007-10/msg00085.html>

- *From:* Jude Fisher <JudeFisher@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 30 Oct 2007 02:24:01 -0700
-

David,

And please verify that there is no GLOBAL ISAPI FILTER -- you only

mentioned the ISAPI Filters tab for each website but not the global ISAPI Filters tab for all website

Thank you, this was the issue.

I didn't realise the Web Sites folder in IIS manager threw up a global properties dialog. My host had helpfully installed a control panel (Matrix) which included a custom ISAPI filter called "Log In Filter". Removing that solved the problem immediately. It would have been nice, of course if the host (Fasthosts) could have told me about this but all their support was able to do was offer to restore the server from scratch in order to repair the problem they were certain I had caused. Not useful.

Thanks also to Roger for the time spent on this.

Jude Fisher / JcFx.Eu

"David Wang" wrote:

You want to read the URL that I mentioned in my prior response to make sure that Basic Authentication is allowed to function on your server.

I suspect the problem is either:

1. some security module running on network packets stripping off Authorization: Basic header and causing IIS to return 401.2 before even invoking any security login code of IIS
2. some security lockdown performed on the colo server that is preventing basic authentication (and probably other things - we just don't know what) from working within IIS

Re: Basic Authentication fails with Error 401.2 where Integrated s

It is harder to validate #2 because it comes down to setting-by-setting comparison of a working server with your server. I don't want to get into that situation because I'd rather have the colo server company tell me what they HAVE changed (they should have those changes listed in an automation script somewhere since they built the server for you) instead of trying to ask everyone else what could/not have changed.

#1 requires that you validate with something like Network Monitor on the server itself that the Authorization: Basic header is received by the IIS web server (and not removed by some network security module). And please verify that there is no GLOBAL ISAPI FILTER --- you only mentioned the ISAPI Filters tab for each website but not the global ISAPI Filters tab for all websites. At the same time, no Wildcard Application Mapping for *ANY* of the Application mapping settings applicable to the URL under question. There's no simple command to do this --- because we are talking about deep, internal server modifications (potentially made by other setup programs), one has to know how IIS works to uncover what other setup programs have configured.

//David
<http://w3-4u.blogspot.com>
<http://blogs.msdn.com/David.Wang>
//

On Oct 29, 3:17 am, Jude Fisher <JudeFis...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

Further to the above, here are the results of the MS Authentication & Access Control Diagnostics tool. These are from the directory I want to be working with rather than the /test one but the settings and results are identical. Where it says COMPUTERTNAME\ACCOUNTNAME, this is the account that I am trying to grant access to:

Check Permissions Results

Status Result

Verifying: D:\home\Clients\Marketing4Tradesmen\cpi*

Account: COMPUTERTNAME\ACCOUNTNAME Access type: FULL

Check of D:\home\Clients\Marketing4Tradesmen\cpi* complete, no errors

Diagnostics complete

View Permissions Results

Re: Basic Authentication fails with Error 401.2 where Integrated s

D:\home\Clients\Marketing4Tradesmen\cgi\
COMPUTERNAME\USERNAME: (OI)(CI)F
D:\home\Clients\Marketing4Tradesmen\cgi\order-postprocess.aspx
COMPUTERNAME\USERNAME: F

Diagnostics complete

View Site Configuration
W3SVC/1 Default
ServerState Server started
ServerBindings :80:
AuthFlags 5 (0x5) "AuthAnonymous | AuthNTLM"

Authentication Results Url:<http://localhost/clients/Marketing4Tradesmen/cgi/>

AnonymousUserPass logon failed Path:W3SVC

AuthType:Anonymous AnonymousPasswordSync
The current configuration requires IIS subauthentication. However, the IIS subauthentication component, iissuba.dll, is not currently configured.
Path:W3SVC

AuthType:Anonymous
AnonymousPasswordSync
The current configuration uses IIS subauthentication for anonymous authentication. This requires that the worker process be configured to run as the Local System identity, which is not recommended for security reasons.
Path:W3SVC

AuthType:Anonymous
must be domain member Path:W3SVC

AuthType:Kerberos
Basic authentication is not a secure authentication protocol. You should consider using Secure Sockets Layer (SSL) for added security.
Path:W3SVC/1/ROOT/clients/Marketing4Tradesmen/cgi
AuthType:Basic

Test Authentication

[THIS POPS A DIALOG BOX. VERIFYING THE PASSWORD FOR THE USER I AM WORKING WITH RETURNS THE RESULT 'SUCCESS'. AUTHENTICATING THIS USER RETURNS:]

Server's response: HTTP/1.1 401 Unauthorized
Learn about IIS status codes

Path:W3SVC/1/ROOT/clients/Marketing4Tradesmen/cgi
AuthType:Basic

Re: Basic Authentication fails with Error 401.2 where Integrated s

Diagnostics complete

Server Permissions Results

Verifying: C:\WINDOWS\help\iishelp\common\
Account: BUILTIN\Administrators Access type: FULL
Account: NT AUTHORITY\SYSTEM Access type: FULL
Account: COMPUTERTNAME\IIS_WPG Access type: READ
Account: BUILTIN\Users Access type: READ | EXECUTE
Check of C:\WINDOWS\help\iishelp\common\
complete, no errors

Verifying: C:\WINDOWS\IIS Temporary Compressed Files\
Account: BUILTIN\Administrators Access type: FULL
Account: NT AUTHORITY\SYSTEM Access type: FULL
Account: COMPUTERTNAME\IIS_WPG Access type: READ | WRITE
Account: CREATOR OWNER Access type: FULL
CREATOR OWNER does not have 'FULL' access to .
Check of C:\WINDOWS\IIS Temporary Compressed Files\
complete, errors
found

Verifying: C:\WINDOWS\system32\inetrv\
Account: BUILTIN\Administrators Access type: FULL
Account: NT AUTHORITY\SYSTEM Access type: FULL
Check of C:\WINDOWS\system32\inetrv\
complete, no errors

Verifying: C:\WINDOWS\system32\inetrv\
Account: BUILTIN\Users Access type: READ | EXECUTE
BUILTIN\Users does not have 'READ | EXECUTE' access to ASP Compiled
Templates
BUILTIN\Users does not have 'READ | EXECUTE' access to History
BUILTIN\Users does not have 'READ | EXECUTE' access to
MBSchema.bin.00000000h
BUILTIN\Users does not have 'READ | EXECUTE' access to
MBSchema.xml
BUILTIN\Users does not have 'READ | EXECUTE' access to MetaBase.xml
Check of C:\WINDOWS\system32\inetrv\
complete, errors found

Verifying: C:\WINDOWS\system32\inetrv\ASP Compiled Templates\
Account: COMPUTERTNAME\IIS_WPG Access type: READ
Check of C:\WINDOWS\system32\inetrv\ASP Compiled Templates\
complete, no
errors

Verifying: C:\inetpub\adminscripts\
Account: BUILTIN\Administrators Access type: FULL
Check of C:\inetpub\adminscripts\
complete, no errors

Verifying: C:\WINDOWS\system32\Logfiles\
Account: BUILTIN\Administrators Access type: FULL
Check of C:\WINDOWS\system32\Logfiles\
complete, no errors

Re: Basic Authentication fails with Error 401.2 where Integrated s

Diagnostics complete

System Information:

System time Mon, 29 Oct 2007 10:05:15 GMT
OS Windows 2003 Service Pack 2
W3SVC IIS6 – World Wide Web Publishing service is running
MSFTPSVC IIS6 – FTP Publishing service is not started
Host name COMPUTERNAME
Dns suffix jcfx.eu
Workgroup name WORKGROUPNAME
ModuleFileName C:\Program Files\IIS Resources\AuthDiag\authdiag.exe
version:
1.0:43.0

"Jude Fisher" wrote:

David,

1) Just as a check I used NET USER /ADD on my test account and as expected it told me the user account already existed.

2) No ISAPI filters are listed for any of the websites on this computer.

3) I didn't set the server up myself (this is a dedicated server from a major UK host) but I can't see anything in Local Security Settings that could be causing the issue – is there anything specific I should be looking for,?

"David Wang" wrote:

When I see weird and erratic behavior, my first question is "do you have custom ISAPI Filter installed on the server". Both global as well

Re: Basic Authentication fails with Error 401.2 where Integrated s

as per-site.

The password dialog is supposed to appear for Basic authentication *unless* the client is allowed to auto-login with Basic. That's not allowed by default for security reasons. You hardly want the browser to automatically hand over your login password to ANY website which asks for it, right?

Thinking more esoterically now -- what are the login rights assigned to your test user. IIS uses a specific login type (configurable), so ability to login via remote desktop is insufficient proof that IIS can login that user. See this URL for more info: <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Librar...>

Usually the defaults when you just create a user via NET USER name password /ADD will suffice, but sometimes Group Policies of a domain can alter this behavior (even if you've unjoined this machine from a domain).

Are you sure you don't have a proxy or network policy/device which is simply forbidding Basic authentication altogether (because it exposes the user's password)? For example, it'd be really easy for such a proxy or network device (or even ISAPI Filter...) to simply strip off the Authorization: Basic header being sent with your requests, at which point since you don't have Anonymous enabled, IIS will return 401.2 EVEN THOUGH you have basic auth enabled -- because to IIS, your

Re: Basic Authentication fails with Error 401.2 where Integrated s

request has been stripped to an anonymous
by removing the
Authorization: Basic header. You can test
this theory by temporarily
enabling Anonymous and Basic
authentication and ACL'ing files to allow
access to the IUSR.

working with fails if the
initial challenge isn't basic
authentication and(as
I understand it, and please
correct if this is wrong) IIS
will try integrated
first and basic second if both
are enabled.

Not exactly. IIS only advertises to the HTTP
Browser the
authentication protocol it requires with a
certain ordering. It is the
HTTP Browser which determines which
authentication protocol to use. IE
will choose Integrated before Basic if both
are enabled.

Brief explanation of what's going on here:

HTTP, like many network protocols, is a
give-and-take sort of
protocol. When it comes to authentication,
you can only configure the
server to REQUIRE certain authentication
protocols to get access to
secured resources. If an HTTP browser
requests the secured resource
without using the required authentication
protocol, the server simply
responds 401.2 with a list of required
protocols.

Re: Basic Authentication fails with Error 401.2 where Integrated s

At this point, the browser can either choose to ignore the server's suggestion (not wise), choose an authentication protocol to negotiate (and pop up the login dialog as necessary by security/Internet Zone settings), or auto-login with some credentials in a proprietary algorithm. Now, since the browser is attempting to authenticate with a requested authentication protocol, the server either replies:

- 401.1 if the username/password is incorrect
- 401.3 if the credentials are alright but the NTFS ACLs deny the authenticated credentials access to the secured resource
- 401.4/401.5 if the credentials are alright but an ISAPI Filter/ISAPI Extension denied access for arbitrary reason
- Anything else indicates the credentials are alright and action according to HTTP status code was performed on the server

//David
<http://w3-4u.blogspot.com>
<http://blogs.msdn.com/David.Wang>
//

On Oct 26, 1:23 am, Jude Fisher
<JudeFis...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote:

Roger,

Yes, to restate the setup is as follows:

Test directory with simple static test page in it.

On the IIS directory security tab, anonymous access is disabled, digest authentication is disabled, integrated authentication is disabled and basic authentication only is enabled. The two text boxes at the bottom (domain and realm) are empty.

On the windows explorer security dialog for the folder, the test user account created has full permissions for the folder and the file that's in it.

I've tested that the user account can log on through remote desktop connection and once logged on can open that directory and file using windows explorer, so

...

read more ;– Hide quoted text –

– Show quoted text –