How do I use NTLM authentication with Active Directory

Asked 16 years, 4 months ago Modified 11 years, 1 month ago Viewed 47k times

7

I am trying to implement NTLM authentication on one of our internal sites and everything is working. The one piece of the puzzle I do not have is how to take the information from NTLM and authenticate with Active Directory.

There is a good description of NTLM and the encryption used for the passwords, which I used to implement this, but I am not sure of how to verify if the user's password is valid.

I am using ColdFusion but a solution to this problem can be in any language (Java, Python, PHP, etc).

Edit:

I am using ColdFusion on Redhat Enterprise Linux. Unfortunately we cannot use IIS to manage this and instead have to write or use a 3rd party tool for this.

Update - *I got this working and here is what I did*

I went with the JCIFS library from samba.org.

> Note that the method below will only work with NTLMv1 and **DOES NOT** work with NTLMv2. If you are unable to use NTLMv1 you can try Jespa, which supports NTLMv2 but is not open source, or you can use Kerberos/SPNEGO.

Here is my web.xml:

```
<web-app>
    <display-name>Ntlm</display-name>

    <filter>
        <filter-name>NtlmHttpFilter</filter-name>
        <filter-class>jcifs.http.NtlmHttpFilter</filter-class>

        <init-param>
            <param-name>jcifs.http.domainController</param-name>
            <param-value>dc01.corp.example.com</param-value>
        </init-param>
        <init-param>
            <param-name>jcifs.smb.client.domain</param-name>
```

```
            <param-value>CORP.EXAMPLE.COM</param-value>
        </init-param>
    </filter>

    <filter-mapping>
        <filter-name>NtlmHttpFilter</filter-name>
        <url-pattern>/admin/*</url-pattern>
    </filter-mapping>
</web-app>
```

Now all URLs matching `/admin/*` will require NTLM authentication.

http authentication coldfusion active-directory ntlm

Share

Improve this question

Follow

edited Jan 11, 2012 at 19:00

community wiki
9 revs, 4 users 60%
Jon Works

7 Answers

Sorted by: Highest score (default)

19

What you're really asking is: Is there any way to validate the "WWW-Authenticate: NTLM" tokens submitted by IE and other HTTP clients when doing Single Sign-On (SSO). SSO is when the user enters their password a "single" time when they do Ctrl-Alt-Del and the workstation remembers and uses it as necessary to transparently access other resources without prompting the user for a password again.

Note that Kerberos, like NTLM, can also be used to implement SSO authentication. When presented with a "WWW-Authenticate: Negotiate" header, IE and other browsers will send SPNEGO wrapped Kerberos and / or NTLM tokens. More on this later but first I will answer the question as asked.

The only way to validate an NTLMSSP password "response" (like the ones encoded in "WWW-Authenticate: NTLM" headers submitted by IE and other browsers) is with a NetrLogonSamLogon(Ex) DCERPC call with the NETLOGON service of an Active Directory domain controller that is an authority for, or has a "trust" with an authority for, the target account. Additionally, to properly secure the NETLOGON communication, Secure Channel encryption should be used and is required as of Windows Server 2008.

Needless to say, there are very few packages that implement the necessary NETLOGON service calls. The only ones I'm aware of are:

1. Windows (of course)

2. Samba - Samba is a set of software programs for UNIX that implements a number of Windows protocols including the necessary NETLOGON service calls. In fact, Samba 3 has a special daemon for this called "winbind" that other programs like PAM and Apache modules can (and do) interface with. On a Red Hat system you can do a `yum install samba-winbind` and `yum install mod_auth_ntlm_winbind`. But that's the easy part - setting these things up is another story.
3. Jespa - Jespa (http://www.ioplex.com/jespa.html) is a 100% Java library that implements all of the necessary NETLOGON service calls. It also provides implementations of standard Java interfaces for authenticating clients in various ways such as with an HTTP Servlet Filter, SASL server, JAAS LoginModule, etc.

Beware that there are a number of NTLM authentication acceptors that do not implement the necessary NETLOGON service calls but instead do something else that ultimately leads to failure in one scenario or another. For example, for years, the way to do this in Java was with the NTLM HTTP authentication Servlet Filter from a project called JCIFS. But that Filter uses a man-in-the-middle technique that has been responsible for a long-standing "hiccup bug" and, more important, it does not support NTLMv2. For these reasons and others it is scheduled to be removed from JCIFS. There are several projects that have been unintentionally inspired by that package that are now also equally doomed. There are also a lot of code fragments posted in Java forums that decode the header token and pluck out the domain and username but do absolutely nothing to actually validate the password responses. Suffice it to say, if you use one of those code fragments, you might as well walk around with your pants down.

As I eluded to earlier, NTLM is only one of several Windows Security Support Providers (SSP). There's also a Digest SSP, Kerberos SSP, etc. But the Negotiate SSP, which is also known as SPNEGO, is usually the provider that MS uses in their own protocol clients. The Negotiate SSP actually just negotiates either the NTLM SSP or Kerberos SSP. Note that Kerberos can only be used if both the server and client have accounts in the target domain and the client can communicate with the domain controller sufficiently to acquire a Kerberos ticket. If these conditions are not satisfied, the NTLM SSP is used directly. So NTLM is by no means obsolete.

Finally, some people have mentioned using an LDAP "simple bind" as a make-shift password validation service. LDAP is not really designed as an authentication service and for this reason it is not efficient. It is also not possible to implement SSO using LDAP. SSO requires NTLM or SPNEGO. If you can find a NETLOGON or SPNEGO acceptor, you should use that instead.

Mike

Share

Improve this answer

Follow

edited Mar 19, 2013 at 17:29

Amicable

3,091 ● 3 ● 53 ● 78

answered Jan 21, 2009 at 4:37

user8134

1,823 ● 3 ● 14 ● 10

2

As I understand it.
NTLM is one of IIS built in authentication methods. If the the Host is registered on the domain of said active directory, it should be automatic. One thing to watch out for is the username should be in one of two formats.

- domain\username
- username@domain.tld

If you are trying to go against a different active directory you should be using a forms style authentication and some LDAP code.

If you are trying to do the Intranet No Zero Login thing with IIS Integrated authentication

- the domain needs to be listed as a trusted site in IEx browser
- or use a url the uses the netbios name instead of the DNS name.
- for it to work in firefox read here

Share Improve this answer Follow

answered Aug 22, 2008 at 12:24

jason saldo

9,930 ● 5 ● 35 ● 41

2

The ModNTLM source for Apache may provide you with the right pointers.

If possible, you should consider using Kerberos instead. It lets you authenticate Apache against AD, and it's a more active project space than NTLM.

Share Improve this answer Follow

answered Sep 15, 2008 at 15:43

Matt Everson

411 ● 4 ● 9

1

Check out Waffle. It implements SSO for Java servers using Win32 API. There're servlet, tomcat valve, spring-security and other filters.

Share
Improve this answer
Follow

answered Jul 27, 2010 at 13:46

community wiki
dB.

1

You can resolve the Firefox authentication popup by performing the following steps in Firefox:

1. Open Mozilla Firefox
2. Type about:config in address bar
3. Enter network.automatic-ntlm-auth.trusted-uris in Search texfield
4. Double click preference name and key in your server name as String value
5. Close the tab
6. Restart Firefox.

Share
Improve this answer
Follow

edited Nov 8, 2013 at 13:30

community wiki
2 revs, 2 users 86%
Imran Vohra

0

Hm, I'm not sure what you're trying to accomplish.

Usually implementing NTLM on an internal site is as simple as unchecking "Enable Anonymous Access" in "Authentication and Access Control" in the "Directory Security" tab of website properties in IIS. If that is cleared, then your web application users will see a pop-up NTLM dialog.

There's no need for you to write any code that interfaces with Active Directory. IIS takes care of the authentication for you.

Can you be more specific about what you're trying to do?

Share Improve this answer Follow

answered Aug 22, 2008 at 12:18

Portman
32k ● 25 ● 83 ● 101

0

i assume that you are wanting get to some of the attributes that are set against the LDAP account - role - department etc.

for coldfusion check this out
http://www.adobe.com/devnet/server_archive/articles/integrating_cf_apps_w_ms_active_directory.html

and the cfldap tag http://livedocs.adobe.com/coldfusion/6.1/htmldocs/tags-p69.htm#wp1100581

As to other languages - others will do it with there respective APIs

Share

Improve this answer

Follow

edited Aug 22, 2008 at 12:31

answered Aug 22, 2008 at 12:25

littlegeek