Passing User Credentials to an Upstream Proxy

Novell Cool Solutions: Feature
By B Thavamani Rajan

Digg This - Slashdot This

Posted: 28 Apr 2005

Introduction

The Novell BorderManager proxy is now enhanced with a new feature called X-Authenticated-User Header Support. This feature enables user information to be passed to the upstream proxy or to the origin webserver.

This article discusses the features of X-Authenticated-User header in various authentication scenarios. It also discusses the changes that need to be made in the NBM Proxy in order to enable this feature.

How the Process Works

Suppose that a user issues an HTTP request where he has already been authenticated and the NBM proxy knows the authenticated user name. In this case, the proxy can assemble an Auth-User-URI and send a base-64 encoded version of it as a value of the X-Authenticated-User header.

Syntax

```
X-Authenticated-User-Header = "X-Authenticated-User:  base64-encoded(Auth-User-UR
Auth-User-URI =  LDAP://Auth-user-path
```

Example

The X-Authenticated-User HTTP header that will be generated for user admin.novell will be:

```
X-Authenticated-User: base64-encoded(LDAP://x.x.x.x/CN=admin,O=novell )
```

Note: Values are in plain text, not base-64 encoded. Also, the IP address of LDAP Server is x.x.x.x

Process Flow: SSL Authentication

Here are the steps in the process, using SSL authentication:

1. The client issues an HTTP request.
2. With SSL authentication enabled, the proxy sends either a Java applet or an HTML form (default) to be presented to the user, to collect user credentials.
3. The user submits the eDirectory username and password.
4. On successful authentication and access-control, the proxy sends the request to the upstream proxy or origin webserver. The X-Authenticated-User-header value is X-Authenticated-User: base64-encoded (LDAP://x.x.x.x/CN=admin,O=novell).
5. The proxy gets the HTTP data from the upstream proxy or origin webserver.
6. The proxy sends the HTTP data to the client browser.

This process, with SSL authentication, is pictured below.

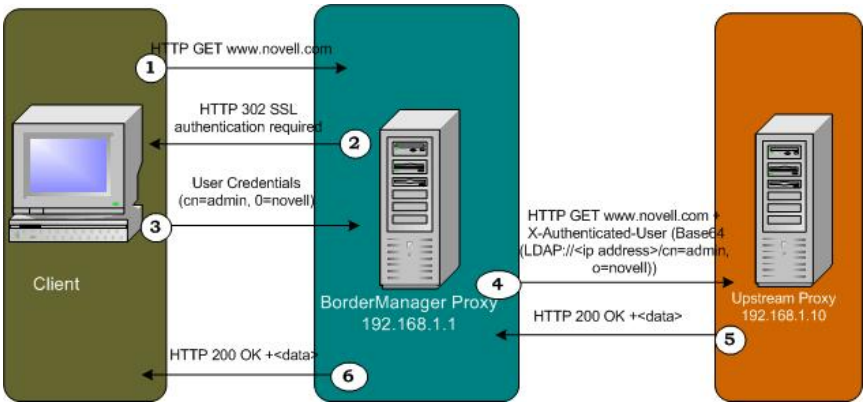

Figure 1: Sequence flow diagram of the X-Authenticated-User Header using SSL Authentication

Process Flow: Single Sign-On

Here are the steps in the process, using Single Sign-On:

1. With Single Sign-On (SSO), the user logs in to the tree containing the BorderManager server.
2. SSO requires the clients to run a background process (CLNTRUST.EXE), which is usually invoked from the login script.
3. When an HTTP request is received from the client, proxy verifies whether the user is already authenticated to the Novell client.
4. On successful authentication and access-control, proxy sends the request to the upstream proxy or origin webserver with X-Authenticated-User-header value as X-Authenticated-User: base64-encoded (LDAP://x.x.x.x/CN=admin,O=novell).
5. The proxy gets the HTTP data from the upstream proxy or origin webserver.
6. The proxy sends the HTTP data to the client browser.

This process, with Single Sign-On, is pictured below.

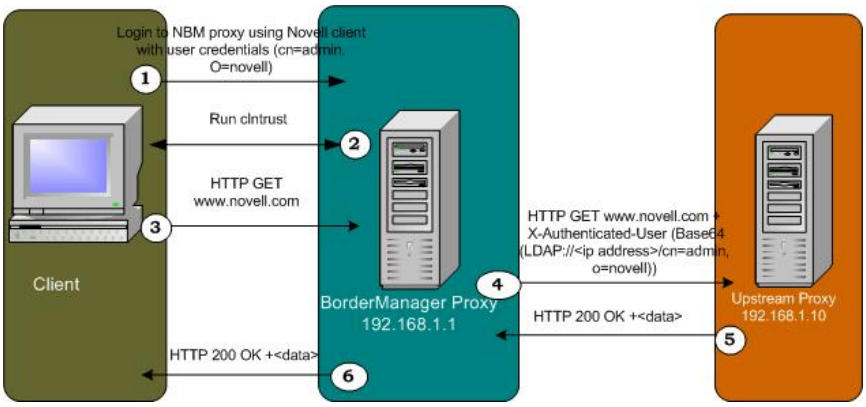

Figure 2. Sequence flow diagram of the X-Authenticated-User Header using Proxy SSO

Configuring X-Authenticated-User header in NBM

Here are the switches that need to be configured in the sys:\etc\proxy.cfg file for the X-Authentication-User header feature in the NBM proxy:

```
[X-Authenticated-User]
EnableXAuthenticatedUserHTTPHeader=1
LDAPServer=X.X.X.X
LDAPTypeUserName=1
```

where X.X.X.X is the IP address of the LDAP server. Note that LDAPTypeUserName differentiates for "," (comma) or "." (dot) as the field separator (delimiter) between the Common name and the Organizational unit.

Tip: For Webwasher* to work properly with NBM proxy, set LDAPTypeUserName=1.

After configuring the switches,

Make sure authentication is enabled for the proxy.

Configure the ICP Parent or upstream proxy IP address in NWADMIN32.

Unload and load the proxy.nlm for new changes to take effect.

Packet Capture - Comma-Delimited

Below is an example of packet capture using comma delimiters (for LDAPTypeUserName=1).

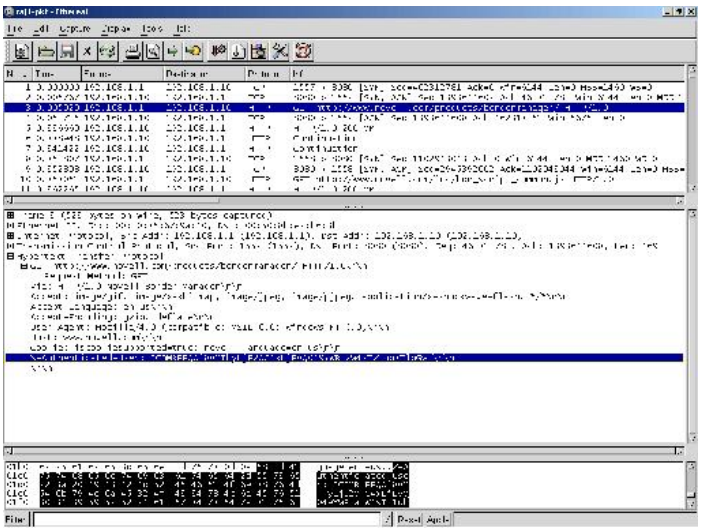

Figure 3. Packet capture - comma-delimited (Larger image)

In the above packet capture, the packet #3 HTTP request from the NBM proxy (192.168.1.1) to the upstream proxy (192.168.1.10) contains the X-Authenticated-User header value as:

```
X-Authenticated-User: base64-encoded(LDAP://192.168.1.1/CN=admin,O=novell)
```

Note: "cn=admin,o=novell" - Object with Common Name admin, under the Organization Novell. Here the Common name and Organization delimiter is ",", because LDAPTypeUserName=1. For Webwasher to work properly with NBM, LDAPTypeUserName should be set to 1.

Packet Capture - Period-Delimited

Below is an example of packet capture using period delimiters (for LDAPTypeUserName=0).

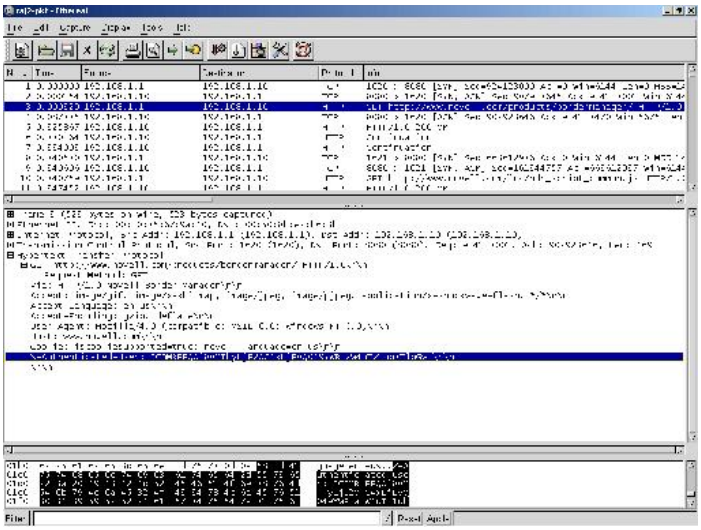
(Larger image)

Figure 4: Packet Capture - Period-Delimited

In the above packet capture, packet #3 HTTP request from the NBM proxy (192.168.1.1) to the upstream proxy (192.168.1.10) contains the X-Authenticated-User header value as:

```
X-Authenticated-User: base64-encoded(LDAP://192.168.1.1/CN=admin.O=novell)
```

Note: "cn=admin.o=novell" - Object with Common Name admin, under the Organization Novell. Here the Common name and the Organization delimiter is ".", because LDAPTypeUserName=0

Conclusion

This article has discussed the use of the X-Authenticated-User header in the NBM Proxy. It has also explained how to enable and configure this feature provided in Novell BorderManager, available with latest support patches. The facts and figures provided in this article are strictly from test scenarios; there can be deviations from these figures in real-world scenarios. Novell recommends that you verify configuration changes on a simulated test network before you deploy any of these configuration changes directly in a production environment.

*Webwasher is a product of Webwasher AG, a wholly owned division of CyberGuard Corporation.