SANGFOR

IAM

WEB SSO Troubleshooting Guide

Version 12.0.18

Change Log

Date	Change Description
Nov 2, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Confirm the environment deployment

1. The web server is in the internal network area of the IAM. Because the data does not pass through the IAM device when accessing the web server, the traffic needs to be mirrored to the IAM.

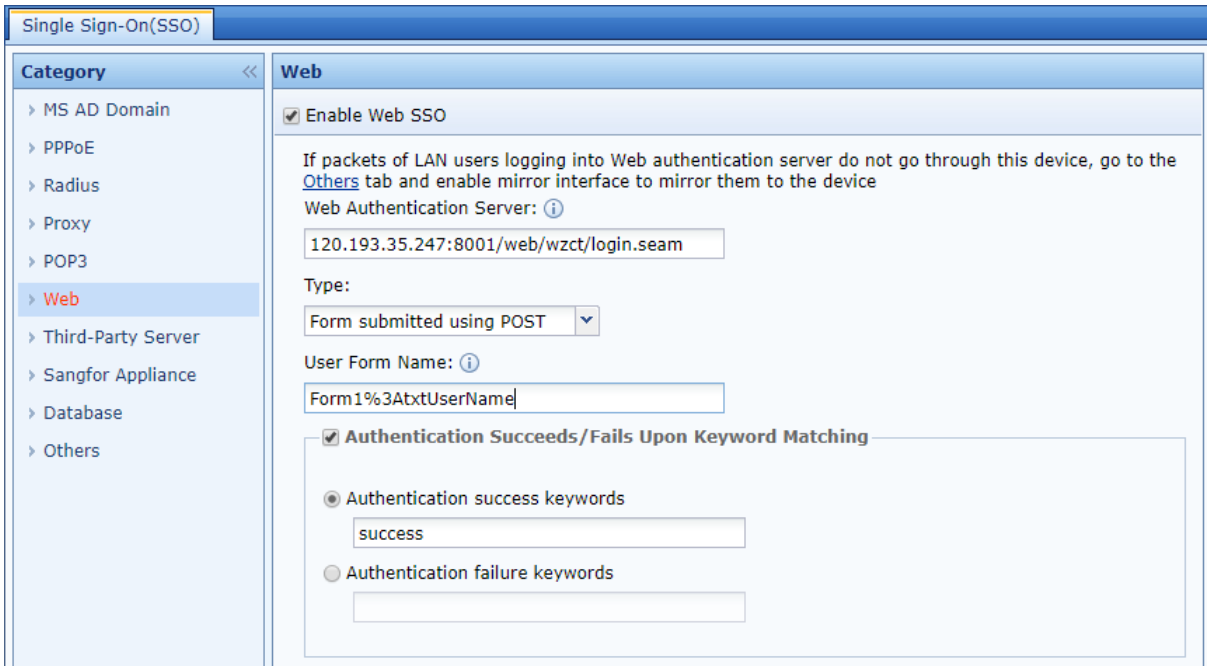
2. The web server is on the external network of IAM. At this time, the web login data passes through IAM. You only need to confirm that you can catch the correct login keywords.

3. Some data streams are going to special scenarios, such as when a PC accesses data from a web single sign-on server, first go to the exit router, and then return to the web single sign-on server. In this case, web single sign-on is unsuccessful.

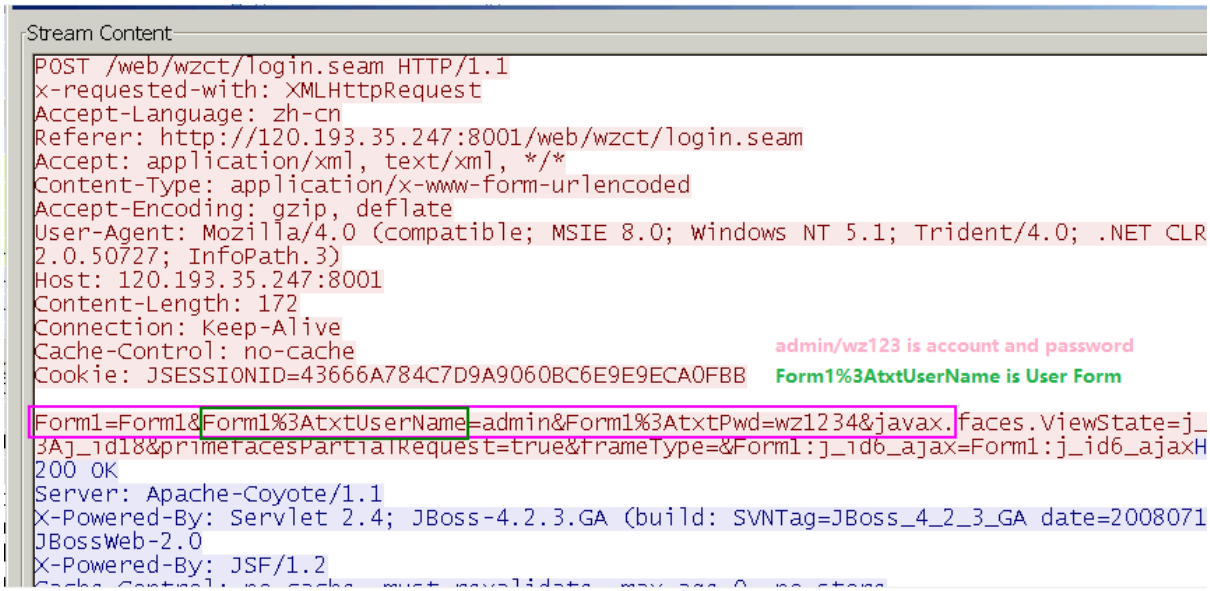
Chapter 2 Common problem

1. The IP address of the Web authentication server cannot be filled in the global exclusion list of the IAM device. Adding IAM will not process the data of the Web authentication server.

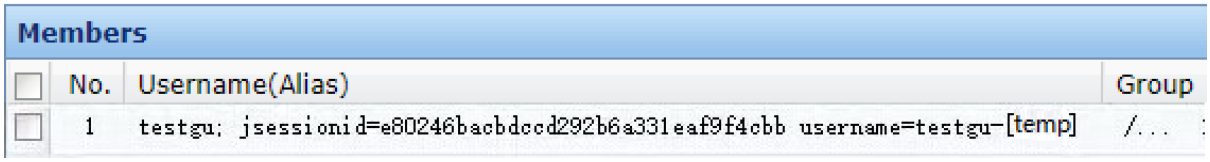
2. If the web server address is in the form of IP or IP: port, you must also select " Before authentication, added to group(Users accessing any HTTP content must be authenticated)" in other authentication options, and confirm the policy permissions of the root group. Pass the data of this IP and port.



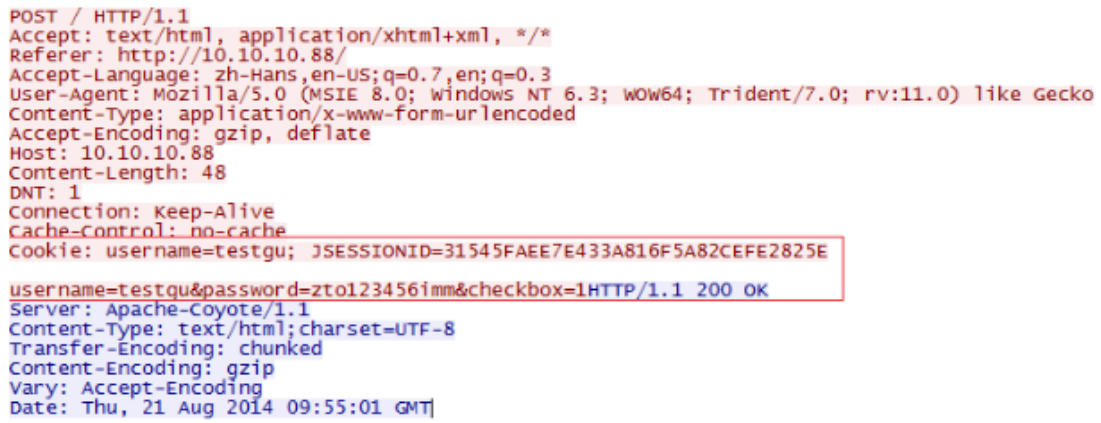
3. The user form name needs to be completed. Through packet capture analysis, the fields before the user name are taken until the ampersand, and the user name field is looked forward to the ampersand. As shown below:



4. The authentication method using WEB single sign-on is used, but the obtained user name is abnormal, as shown below:



Capture the authenticated data packet and view the contents of the post data packet. The data packet screenshot is as follows:



The theory of WEB single sign-on to obtain a user name is:

After detecting the user form name (username in this example), the content behind the form name will be intercepted as the user name, and the detected ampersand will end.

The user name will not only detect the content of the http post data packet, but also the cookie content when the data packet contains a cookie.

Through the data package, you can see that the upload has a cookie, and the cookie has the username form name, but the form name does not end with an ampersand, but ends with a semicolon. Because the device cannot recognize the end character, continue to the next until the ampersand in the post content is matched. So we see that long list of usernames in the online user list.

[Solution]: This problem is that the client's web server does not meet our standards. It is recommended that the client change the terminator of the form name in the cookie to an ampersand.

3. if encounter unsuccessful web single sign-on and confirm that there are no problems with successful keywords and configuration. You can test with: symbols and; symbols as keywords to test, because general web page posts will be included, if it still does not work, you can type debug logs and Capture

and analyze the data packets, and confirm that there is no problem, if the problem still exist, you can feedback to the R&D there.

SANGFOR