Out-of-the-box Single Sign-On Capabilities with Oracle Universal Content Management 10gR3

This brief document describes how Oracle Content Server 10gR3 can support authentication-only single sign-on capabilities out of the box.

Overview

Oracle Content Server's web server plug-in includes an out-of-the-box capability to use the value of standard HTTP header, REMOTE_USER, as an authenticated user. This allows Content Server to support many web single sign-on environments without any need for customizations.

How to Use this Capability

Web single sign-on (SSO) products, including Oracle Access Manager, include a web server plug-in (SSO web agent) that sets various HTTP headers to specify authentication, authorization and user attribute information. Most SSO products also allow administrators to configure the SSO web agent to set additional HTTP headers. For instance, Oracle Access Manager's WebGate can be configured to set additional headers as needed. With such products, the web administrator can set the REMOTE_USER header's value to be the user ID of the authenticated user. The Content Server will automatically take that value as the authenticated user and will not issue a login prompt. In order for this to work properly, the SSO web agent has to be loaded on the web server, and has to be higher up in the web server's load order such that it intercepts the HTTP request before the Content Server's web filter. Of course, the SSO web agent has to be configured to enforce SSO on the Content Server web address.

Benefits of this Approach

This approach of setting REMOTE_USER header allows for authentication-only single sign-on scenarios to be supported without the need to customize the Content Server plug-in. Furthermore, this approach can be used on all operating systems and web servers supported by Oracle Content Server. Since most SSO products can be configured to set REMOTE_USER, this approach will work with a wide array of SSO products, including Oracle Identity Management products.

Important Considerations

The approach outlined in this document supports authentication-only SSO scenarios. Oracle Content Server still has to be configured to authorize the user against the proper LDAP/Active Directory system. User attributes also have to be mapped from the LDAP/Active Directory system. This can be done using Content Server's AD/LDAP provider. The REMOTE_USER header only sets the user ID (and thus authentication) information. If the SSO integration requirement includes the need to read authorization and other user information (e.g. attributes) from HTTP headers, then a customization of the Content Server's web server plug-in will be required.

Roadmap

Oracle Universal Content Management's 11g release is slated include out of the box capabilities to support Oracle's identity management products for single sign-on support. The plan includes ability to support all standard headers set by Oracle identity management products to allow broader SSO deployments without need for customization of the Content Server web server plug-in.