Deploying "Single-sign On" with RDC 46 OnSite: An examination of methods to allow Single-Sign-On for existing RDC 46 OnSite environments

Sunil G. Singh, Ahila Selveraj
DBMS Consulting
12 October 2010
Systems Integration
Session 15

Acknowledgements

- Many thanks to OHSUG for this opportunity to present to the OHSUG Systems Integration Focus Group.
- Many thanks to the OHSUG Systems Integration Focus Group Chairs for their infinite patience in receiving and expeditious review of this presentation.
- Many thanks to everyone who participated in the development of presentation.

Assumptions

- Audience has a working knowledge of current OC/RDC 4.6 internals/architecture.
- Nothing presented is intended to bypass any security measures or GCP SOPs for the use of RDC.

Problem Statement

- While products such as Oracle Identity Management (OIM) provide extremely robust solutions for Single-Sign On, Oracle RDC does not natively support this type of solution.
- However, enterprise customers and external site users are seeking ways to have a protected, secure public-facing RDC environment, without exposing their internal infrastructure to security risks, but still also one username and password for accessing RDC.

PreRequisites for using Oracle RDBMS authentication in RDC

- The Oracle RDBMS USERNAME must be the SAME as the LDAP or AD Username
- If Oracle RDBMS authentication is used for RDC, then there must be a way to synchronize the Oracle RDBMS password with a more general authentication source
  - Usually LDAP or AD

PreRequisites for using Oracle RDBMS authentication in RDC (2)

- This can be done by having a password verification function applied to the RDC user's profile. The function, in turn, can make a call from the RDBMS to the external authentication source
  - DBMS_LDAP can provide lookup and can delete and replace a changed password
  - On-Line example
- This method is useful since it takes into account all ways a user can change a password at the RDBMS.

PreRequisites for using Oracle RDBMS authentication in RDC (3)

- Changes from an LDAP or AD interface can be pushed into the Oracle RDBMS
  - Oracle OID/OIM is one method of accomplishing this
  - NOTE: Rules for password must then be in common between all platforms. For example, not allowing a password to start with a number is a restriction in Oracle RDBMS, but allowed in LDAP or AD. So the LDAP or AD rules must be modified to be compliant with Oracle RDBMS rules.

Scenario 1: Use external .JSP or .PHP scripts from Juniper or Cisco

- As Juniper and Cisco are both common public facing network devices which can also be used to authentic public facing users, they are both also capable of calling a .JSP or .PHP script located on the RDC Application server
- Using a concept of "tokenizing", the username and password can be stored in the logon session of the network device, and passed as a POST parameter to the .JSP or .PHP scripts
- The .JSP or .PHP script can then log into RDC OnSite automatically
- On-Line example

Scenario 1: Use external .JSP or .PHP scripts from Juniper or Cisco (2)

- Note that the POST parameters can be derived from looking at the View Source of the actual RdcLogin.do page. In the lower section, the required parameters are listed, along with their defaults. Note that some are optional and some are "HIDDEN", meaning that they could be required but are not shown in the calling browser URL. (EXAMPLE WILL FOLLOW IN FINAL PRESENTATION)
  - Computation for Date and Time have to be taken into account. Using the script on the RDC application server itself could lead to some issues in DISPLAYED time (not audit trail timestamps) since these values would then be computed from the RDC Application Server and not the user's desktop local time.

Scenario 2: Integration with SiteMinder

- Siteminder is also very common for managing public facing web applications
- Siteminder has native APIs built in for authentication to LDAP
- Using any Java tool, these APIs can be called with a similar passthrough mechanism to authenticate against the RDC instance
  - This implies a separate login page is built in Java, and then checks LDAP and then passes through to RDC
- This application can be extended to also allow resets of the password across both LDAP and RDC.
- On-Line example

Scenario 3: Changing the authentication mechanism in the Oracle RDBMS

- Given RDC 4.6 uses Oracle 11g, there are many features in Advanced Security which allow the 11g RDBMS to change the way clients authenticate:
  - Kerberos
  - PKI
  - RADIUS
- OIM also can change the default mechanism for account and user authentication if the Oracle RDBMS is connected to an OIM repository

Scenario 3: Changing the authentication mechanism in the Oracle RDBMS (2)

- In an environment that uses central authentication based on these methods, SSO is then achievable within RDC by leveraging the fact that the RDC instance no longer requires a password from the RDBMS level.
- This method is not officially supported, but there are customers using this method today.
- On-Line example

Customized Solutions for SSO with RDC

- Possible to build a customized interface or portal page
- Suggest using SPML version 2.0 standards
  - Extensible Metatagging available
- Token based SSO also possible
- Biometrics also possible

Biographies

Sunil G. Singh, President & CEO, DBMS Consulting, Inc.

- Sunil is a Global Oracle Health Sciences deployment expert for DBMS Consulting. He has been an active member of the OHSUG community since 1996 and is extremely grateful for this opportunity to makes these presentations at OHSUG 2010.

Ahila Selvaraj, Senior OHS Developer, DBMS Consulting, Inc.

- Ahila is a Senior OHS Developer for DBMS Consulting, specializing in integration of OC to other OHS systems, with over 10 years of PL/SQL experience.

Contact Information

Sunil G. Singh

DBMS Consulting, Inc

singh@clinicalserver.com

+1-860-983-5848