

RADIUS & Hi-Tech, FISMA Compliant Authentication

by Michael Ivy
25-OCT-10

HI-TECH, FISMA, GLBA, PCI... Two-factor authentication is becoming more required from a compliance standpoint in daily information systems operation. These generally unfunded mandates require strategic leverage of existing technologies. Let's explore one example below – enabling two-factor authentication with Oracle and RADIUS.

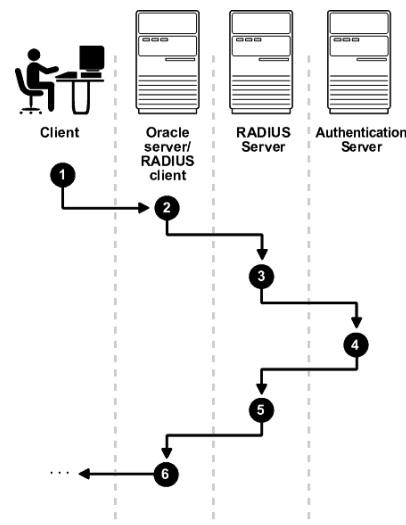
What is RADIUS authentication:

RADIUS (Remote Access and Dial In User Service) is a widely used and supported protocol that allows authentication decisions be passed to a centralized "Authentication Server" for credential validation. Because RADIUS does not require Active Directory, Kerberos Realm or other directory memberships to function it can be used with network switches, VPN concentrators or systems that typically run platforms that are incompatible. In the case of many companies, where two-factor authentication is required across multiple disparate services, utilizing RADIUS to pass authentication decisions to a single two-factor authentication "Authentication Server" or cluster of servers seems to fit best with their mixture of operating systems and devices. Again, since RSA SecurID tokens and RSA Access Manager are likely in use already, extending this authentication service to Oracle (and these other systems) is both time and cost efficient. What would this look like in respect to an Oracle authentication decision?

In this scenario, the Oracle server would act as a RADIUS client of the RSA server. With RSA SecurID tokens, RADIUS authentication is in what is known as "synchronous" mode. Synchronous authorization works like the following:

1. A user logs in by entering a connect string, pass code, or other value. The client system passes this data to the Oracle database server.
2. The Oracle database server, acting as the RADIUS client, passes the data from the Oracle client to the RADIUS server (RSA in this case).
3. The RADIUS (RSA) server passes the data to the appropriate authentication server (RSA Access Manager software) for validation.
4. The authentication server (RSA Access Manager) sends either an "Access Accept" or an "Access Reject" message back to the RADIUS (RSA) server.

5. The RADIUS (RSA) server passes this response back to the Oracle database server/RADIUS client.
6. The Oracle database server/RADIUS client passes the response back to the Oracle client.



Again, because RADIUS is a widely used and supported protocol, its implementation is also extensible. In fact, advanced features can be enabled and configured to allow the Authentication Server to hold group or role membership data, providing authorization services. Additionally, if supported by the Authorization Server, centralized accounting can be enabled with RADIUS Accounting. This then provides authentication, authorization and accounting from a centralized location. Caution and diligence must be used in evaluating the implementation of these extended attributes, as RADIUS accounting may not be able to fully capture all actions taken by users and centralizing authorization decisions may short circuit the user administration function by shifting the responsibility to the Network/Security admin team and away from the DBA/Oracle security admin teams.

To configure RADIUS authentication on the Oracle Server with Advanced Security:

1. Obtain the RADIUS secret key from the RADIUS server. For each RADIUS client, the administrator of the RADIUS server creates a shared secret key, which must be longer than 16-characters.

Delivering What Matters: RADIUS & Hi-Tech, FISMA Compliant Authentication

2. On the Oracle database server, create a directory:
 1. (UNIX) \$ORACLE_HOME/network/security
 2. (Windows) ORACLE_BASE\ORACLE_HOME\network\security
3. Create the file radius.key to hold the shared secret copied from the RADIUS server. Place the file in the directory you created in Step 2.
4. Copy the shared secret key and paste it (and nothing else) into the radius.key file created on the Oracle database server.

For security purposes, change the file permission of radius.key to read only, accessible only by the Oracle owner. Oracle relies on the file system to keep this file secret.

To Configure RADIUS parameters on the Oracle Server using Oracle Net Manager:

1. Navigate to the Oracle Advanced Security profile. The Oracle Advanced Security tabbed window is displayed.
2. Click the Authentication tab.
3. From the Available Methods list, select RADIUS.
4. Move RADIUS to the Selected Methods list by choosing the right-arrow (>).
5. To arrange the selected methods in order of desired use, select a method in the Selected Methods list, and select Promote or Demote to position it in the list. For example, if you want RADIUS to be the first service used, put it at the top of the list.
6. Click Other Params tab
7. From the Authentication Service list, select RADIUS.
8. In the Host Name field, accept the localhost as the default primary RADIUS server, or enter another host name.
9. Ensure that the default value of the Secret File field is valid.
10. Select File, Save Network Configuration.
11. The sqlnet.ora file is updated with the following entries:
 1. SQLNET.AUTHENTICATION_SERVICES = RADIUS
 2. SQLNET.RADIUS_AUTHENTICATION = RADIUS_server_{hostname|IP_address}

Next, configure the initialization parameter file, located in \$ORACLE_HOME/admin/db_name/pfile with the following values:

```
REMOTE_OS_AUTHENT=FALSE  
OS_AUTHENT_PREFIX=""
```

If you are using an alternate RADIUS server for fault tolerance,

set these parameters in the sqlnet.ora file using any text editor:

```
SQLNET.RADIUS_ALTERNATE=(hostname or ip address of alternate radius server)  
SQLNET.RADIUS_ALTERNATE_PORT=(1812)  
SQLNET.RADIUS_ALTERNATE_TIMEOUT=(number of seconds to wait for response)  
SQLNET.RADIUS_ALTERNATE_RETRIES=(number of times to re-send to radius server)
```

On the RADIUS Server (RSA) register the Oracle server as an Agent Host, create users (and roles if desired), assign tokens and you are ready to test.

As a test, create a user on the Oracle server, then attempt to connect as the user with its assigned SecurID token:

```
Sql> create user test identified externally;  
Sql> grant create session to user test;
```

Of course, much more can be found online and in the respective vendors' support documentation. For a good primer on RADIUS authentication and Oracle in general see:

[HOW TO Secure and Audit Oracle 10g and 11g](#)

For Oracle's own documentation see:

http://download.oracle.com/docs/cd/B19306_01/network.102/b14268/asoradus.htm#ASOAG040

There you have it, two factor authentication using intelligent leverage of existing technologies. The principles can be extended to nearly every networking device, service and application. At Rook, we're committed to delivering what matters. For more information about how Rook can deliver what matters to you, give us a call.

How We Help Companies Succeed

Rook provides IT Risk Advisory services that support log management initiatives for organizations at various phases of maturity in their overall monitoring program. Whether your organization is dealing with an emerging regulatory compliance effort, or if you are looking to improve upon your existing program, Rook can provide the methodology and team members with the technical, audit, and management strategy expertise required for success.

Readiness Review - We assess the current state of controls to the desired state of controls to support management strategy, sales enablement, or general compliance efforts. Whether for HIPAA, HITECH, ISO 27002, SOX, PCI, GLBA, FISMA, NIST, or a myriad of other regulations and standards, we provide the knowledge and experience necessary to identify the approach best fit to your organization and prioritized to guide compliance efforts.

Requirement Definition - Working closely with your management and technical teams, we provide experienced professionals who identify the business and technical requirements necessary to a successful log management initiative.

Data Mapping - Whether the scope is known or unknown, we work closely with process owners, system owners, and data owners to determine the data flows for critical and sensitive data, then identify the infrastructure that is in scope

based on the data location when at rest, in use, or as it traverses the network.

Control Identification - When the data mapping is complete and in-scope infrastructure has been identified, controls are identified throughout the process. Identified controls are compared to the desired future state in a gap analysis, and then gaps are documented, and prioritized based on the requirements, budgetary constraints, existing technology, and human factors such as knowledge and internal politics.

Vendor Selection - Requirements are utilized to create Engineering Requirements and a resultant vendor selection matrix. Vendors are reviewed to determine adequacy based on analyst guidance, past experience, internal contacts, and marketing materials. Vendor capabilities are documented, analyzed, the proposal process managed through vendor selection, contract evaluation, and project plan creation.

Health Check - The existing implementation is reviewed to determine if the end-to-end process, team members, and technology (comprising of the Monitoring Program) is operating at optimal efficiency. Areas for improvement are identified, technical configurations are updated, process improvements are managed, documentation updated, and training conducted.