Upgrade Considerations for eTrust Audit and eTrust Security Command Center r8 SP2

Purpose

This document provides important information to help guide you to a decision on upgrading to r8 SP2. It outlines the upgrade tasks and scope, as balanced against the benefits associated with the upgrade. If your organization will not benefit from the new features introduced in SP2, you may decide to upgrade to (or remain at) release level r8 SP1-CR2.

Scope

This document covers upgrading your Audit/SCC environment, including the following release steps:

- Audit R1.5 to Audit R8 SP2
- Audit R8 to Audit R8 SP2
- Audit R8 SP1 CR1 to Audit R8 SP2
- Audit R8 SP1 CR2 to Audit R8 SP2

Background

A key objective of the r8 SP2 release is to provide all CA Audit core components for Solaris 10 platforms, eliminating the need for Windows Server-based components. For this reason, the Audit Policy Manager, Audit Reporter, and Audit Viewer are now completely web-based. The Win32-based server components are no longer available in SP2, even on a Windows Server platform.

These new web-based server components also introduce an all-new model for Audit policy, node, and user management. A major element of this model is the Audit Policy Manager "maker/checker" security role system, which establishes segregation of duties between users allowed to create Audit policies and users allowed to distribute and apply them. Users in SP2 are now managed through CA Embedded Entitlements Manager (EEM), which allows organizations to leverage existing user stores rather than defining user roles within the Audit product.

Current Audit customers typically separate the server components on two machines:

- One hosting the Audit Policy Manager and its Policy Manager Database (PMDB) on MS-Access
- One hosting the Audit Data Tools (commonly called the "Collector") and event database server, on either Oracle or MS-SQL Server

- When upgrading to SP2, a third server is recommended for the CA EEM installation -- this will be a new hardware requirement in many organizations

Therefore, before upgrading to SP2, you must decide whether your organization is ready for the new product components, the new processes within the components, and the new hardware requirements. The decision points outlined below will help you make an informed choice before immediately applying SP2 to your organization's existing Audit environment.

Note for SCC Customers: The SCC r8 SP2 server component continues to require Microsoft SQL 2000.

Decision points

Before upgrading to Audit SP2, you should consider the following:

1. Is the current Audit SP1 CR2 release meeting your organization and business needs?
2. Is your organization ready to change its Audit policy management workflow by creating and assigning "maker" and "checker" roles?
3. Is your organization ready to embrace the concept of segregation of duties that is bound into the "maker" and "checker" roles? If not, this feature can be disabled but this will mean you are bypassing a significant new feature enhancement. Note that the need to define and work within the "maker" and "checker" roles does not change regardless of whether or not segregation is active.
4. Is your organization ready to migrate from a Win32 interface to a web-based interface which has numerous navigational and workflow differences? This also entails administrating a web application server for Reporter/Viewer. Audit SP2 supports either Tomcat or Websphere - If Tomcat is chosen it is installed automatically, however you must install Websphere prior to installing Reporter/Viewer if this is your web server choice.
5. Is your organization ready to evaluate a probable hardware upgrade for the Audit policy manager and event viewer servers? New Audit SP2 components will probably require faster hardware and additional disk space that you have currently allocated. See the README file for a full list of system requirements. In addition you should allocate an additional server for EEM (see number 7).
6. Is your organization ready to manage another database? The PMDB moves from an embedded Microsoft Access instance to Oracle 10g or Microsoft SQL 2000 / 2005.

7. Do you already have an EEM server set up? EEM is the CA Embedded Entitlements Manager and provides general authentication and authorization functionality for Audit SP2 as well as other CA products. It is highly recommended that you install EEM on a dedicated server. EEM was formerly known as Embedded Identity and Access Management toolkit or eIAM.

Platform and database

If you decide to upgrade, you'll need to decide on which server platform and database to upgrade to: Solaris 10 and Oracle 10g or Windows Server 2000 / 2003 and Microsoft SQL 2000 / 2005. Note that Security Command Center (SCC) SP2 supports only Microsoft SQL 2000.

For the latest product announcements including vulnerabilities, see the product home pages for both Audit and Security Command Center on either http://supportconnect.ca.com http://supportconnect.ca.com or http://support.ca.com.

Note: Please heed the announcement concerning the Ingres vulnerability that affects EEM at http://supportconnectw.ca.com/public/eiam/etrusteiam_supp.asp.

For more details, see the following:

- R8 SP2 README
- R8 SP2 Implementation Guide, Chapter 4: Planning Your SIM Implementation.
- R8 SP2 Implementation Guide, Chapter 15: Upgrading from a Previous Release.
- R8 SP2 Implementation Guide, Chapter 8: Installing Policy Manager.

Upgrade scenarios

The upgrade scenarios outlined in this section assume that you employ the two-server architecture outlined in the Background section, although it is certainly possible to combine or separate the product components in different ways.

Scenario 1: Upgrade existing Audit Windows Servers to new Solaris Servers.

1. Provision new Solaris 10 servers and an Oracle Database. For ease of conversion you should plan to swap the names and IP addresses of the new servers with those of the existing servers once the upgrade is complete.
2. Shut down the Audit Server components running on the Windows servers, including the Audit database and associated collectors.
3. Take the old servers offline and give the new servers the identity of the old server.
4. Install Audit SP2 on the Solaris servers.
5. Give the old Windows PM server a new IP address and hostname and then migrate the Windows PMDB to Solaris. See the "How to Migrate a Windows PMDB to Solaris" section for more information
6. Start the Audit Services on the new Solaris Servers.
7. Your SP1 Audit clients and infrastructure should continue to work. You can upgrade Audit Clients to SP2 on a deliberate timetable.

Scenario 2: Upgrade existing Audit Windows servers in place.

1. Shut down the Audit Server components running on the Windows servers, including the Audit database and associated collectors. Events should be queued at their sources and flow again once the upgrade is finished and the collector is restarted.
2. Take Ghost backups of your server machines. They can be used to restore the current environments in case any issues arise during the upgrade process as there is no other way to revert back to your pre-SP2 environment.
3. Install an instance of MS SQL on the Policy Manager machine, if it is not already present.
4. Run the Audit SP2 installation on the Policy Manager, which will allow you to automatically convert the existing Access PMDB to MS SQL.

5. Run the Audit SP2 installation on the DT server (Collector, Report and Viewer, etc.)
6. Once both upgrades are finished, restart the services.
7. Your SP1 Audit clients and infrastructure should continue to work. You can upgrade Audit Clients to SP2 on a deliberate timetable.

Scenario 2a: Upgrade existing Audit Windows servers to new more powerful Windows servers

1. In an isolated test environment, create cloned versions of your Windows servers on your new hardware. This can be done using backup and restore tools or complete machine image tools.

   Alternatively, you can install the copy of Audit currently running in your production environment on the clone machine, and then copy the production version of the MS Access PMDB to your clone machine (c:\Program Files\CA\eTrustAudit\database\policy_db.mdb) and export the related MS Access PMDB password registry keys value found in HKLM\SOFTWARE\ComputerAssociates\eTrust Audit\Policy Manager\Database. (Import the registry file on the test machine.)
2. Proceed to upgrade your test environment as in scenario 2 with the exception that you may perform step 2 at your discretion.
3. Audit SP2 is now available to test.
4. When you feel you are ready to move SP2 into production, repeat scenario 2a skipping the test, take the old servers offline, and move the new test environment servers into the production network.

Scenario 2b: Upgrade existing Audit Windows servers to new more powerful Windows servers.

1. Provision new Windows servers (preferably Windows 2003 and MS SQL 2005). For ease of conversion you should plan to swap the names and IP addresses of the new servers with those of the existing servers once the upgrades are complete.
2. Shutdown the Audit Server components running on the Windows servers, including the Audit database and associated collectors.
3. Take the old servers offline and give the new servers the identity of the old servers.
4. Install Audit SP2 on the new Windows servers.
5. Give the old Windows PM server a new IP address and hostname and then bring it online. Run the PMDBMigrate process in order to migrate SP1 policies to the new SP PMDB. (see Chapter 8 of the Implementation Guide)

6. Start the Audit Services on the new servers.
7. Your SP1 Audit clients will continue to work and infrastructure should continue to work. You can upgrade Audit Clients to SP2 on a deliberate timetable.

How to Migrate a Windows PMDB to Solaris

1. Copy the migration directory located under Solaris/Shared from the SP2 install package to an area or removable media that you can access in subsequent steps.
2. Login in to your old Windows Audit Policy Server.
3. Verify that policy_db.mdb exists. Its default location is c:\Program Files\CA\eTrust Audit\database.
4. Copy the migration directory from the location used in step 1 to a location such as: c:\catemp
5. Create a New Data Source using the Oracle ODBC driver:
    a. Install the Oracle windows client on this machine; use the custom install in order to also install the Oracle ODBC driver.
    b. Go to Start->Programs->Administrative Tools->Data Sources(ODBC).
    c. Click the System DSN tab.
    d. Click Add (the Oracle ODBC driver should be listed).
    e. Choose the Oracle driver and click Finish.
    f. Enter a Data Source Name (for example "eAuditR8sp2pmdb").
    g. Enter a description such as "eTrust Audit r8 Sp2 policy Manager Database".
    h. Enter the TNS Service Name of the Policy Manager Database, which was specified during the Solaris Audit SP2 install.
    i. Enter the User ID defined during the Solaris Audit SP2 install.
    j. Click on Test Connection.
    k. Enter password and click OK.
    l. Click OK to save the DSN settings.
6. Launch the PMDBMigrate.exe utility by double clicking on PMDBMigrate.exe that you copied in Step 4.
7. Supply the DSN name for the new Oracle DB with username and password.
    a. Enter Data Source Name: "eAuditR8sp2pmdb".
    b. Enter User Name: "eauditpm".
    c. Enter Password.

d. Click Next.

e. Click Finish.

8. Pre-SP2 policies and nodes should now be migrated to the new Oracle PMDB.

   Note: Information and errors are logged by default to c:\Documents and Settings\{username}\local settings\temp\PMDBMigrate.log).

9. Verify the migration by logging in with a "maker" role to URL: https://<policy_manager_host_name>:5250/spin/auditadmin. You should use the IAM account 'EiamAdmin' and the password given during setup when accessing the interface for the first time to confirm the migration.

   Note: If you haven't already created a "maker" role see the section in the Implementation Guide entitled "Start the Audit Administrator".