Data drives your business, and a seamless flow of information across your enterprise can give your business the edge it needs to stay competitive. The more that data flows, however, the more open it is to improper access — and not just from hackers outside of your company, but also from within the organization, whether intentional or inadvertent. To adhere to legal and organizational requirements, as well as industry standards, you need to be able to immediately identify who accessed what, when it was accessed, and where it was accessed; and you need to be able to deal with any potential data security violations.

To address these needs, SAP included Read Access Logging (RAL) functionality in SAP NetWeaver Application Server (AS) ABAP 7.40. RAL is a new security functionality that allows customers to log and monitor user access to sensitive or classified data.

Before you can take advantage of these benefits, however, you’ll need to configure RAL.

Note: The current version of RAL supports Web Dynpro ABAP, web services, and RFC calls. Support for ABAP Dynpro is planned for a future release.

Configuring Read Access Logging
The configuration begins in the RAL Manager (transaction SRALMANAGER), which offers two tab strips: an Administration tab for configuration and a Monitor tab to view the logging results. To perform the configuration steps, choose the Administration tab.

Note that to perform the steps, you must be assigned the relevant authorization objects as part of the required authorization template roles. See the “Read Access Logging Authorization Roles and Objects” sidebar on the next page for an overview of the template roles and authorization objects provided for RAL.

Step 1: Define the Logging Purpose
Each RAL configuration requires a logging purpose, which groups the log events you want to record by use case and reason for recording. For example, the purpose could be a financial audit for logging various types of access to bank account details, or it could be to ensure privacy by logging access to different kinds of personal data, such as religious affiliation.

To define a logging purpose, click Logging Purposes in the Administration tab. Then click Create and specify an ID, a name, and a description for the new logging purpose (see Figure 1 on the next page). Note that, once created, you cannot change the logging purpose ID.

Step 2: Define a Log Domain
Next, you need to define a log domain, which will later be assigned to each field that will be recorded by the log. Log domains define the semantic meaning of the data elements that will be captured during the log recording, so an auditor can understand the recorded data when viewing the log results. Using log domains allows you to create descriptions of semantically
identical or related fields that may have different technical representations when captured — a financial account is often present in more than one user interface (UI), web service, or other interface, for example, and may be referenced by an internal or external ID, appear as text or an integer, or be formatted differently.

To create a log domain, click Log Domains in the Administration tab. Then click Create and, in the resulting dialog box, specify a name, a software component, and, optionally, a description (see Figure 2). The software component functions much like a namespace; it refers to a business area and serves as a grouping element for different, related log domains. An HR audit, for instance, would likely involve logging many different types of HR data. So you might create an additional log domain for personal data, such as address and birthday, and another for social security number. For each log domain created for the audit, you would specify the same software component (for example, human capital management; HCM).

Together, the logging purpose and log domains function as a structure that will make the log results easier to collect and digest. Once these two elements have been defined, the next step is to configure the recording function so that you can specify the fields to be logged when you create the actual logging configuration.

**Step 3: Configure a Recording**

To log information presented in a UI, the fields that are of interest must be collected into a recording. The recording function is based on the particular UI technology, or “channel,” through which the data access will occur. To specify the fields to record, click Recordings in the Administration tab. To activate an old recording, simply search for it and select it. To create a new recording, click Create and select the channel (for example, Web Dynpro). Then specify a name and add an optional description for the recording (see Figure 3).

Once you’ve created a recording, when you launch the UI that you want to track, a new context menu entry, Recorded Field, will be available. To add a field in the UI to the recording, you simply right-click on the field to launch the context menu and select Recorded Field. The field is then added to the recording and will be available to be selected and assigned log domains in the next step, when you perform the actual log configuration.

**Step 4: Create the Log Configuration**

With the logging purpose, log domains, and field recording in place, you are ready to create the log configuration, which specifies the read

---

**Read Access Logging Authorization Roles and Objects**

Read Access Logging (RAL) follows the SAP NetWeaver authorization concept, in which authorizations are assigned to users based on roles. For working with RAL, SAP delivers the following template authorization roles:

- **SAP_BC_RAL_ADMIN_BIZ** for business-related administration of RAL
- **SAP_BC_RAL_ADMIN_TEC** for technical administration of RAL
- **SAP_BC_RAL_ANALYZER** for access to events logged by RAL
- **SAP_BC_RAL_CONFIGURATOR** for log configuration of RAL
- **SAP_BC_RAL_SUPPORTER** for RAL support activities

The RAL template authorization roles include authorization objects that allow user/security administrators to set up segregation of duties and authorizations to configure and access RAL. These objects are:

- **S_RAL_BLKL** for the user exclusion list
- **S_RAL_CFG** for configuration of data to be logged
- **S_RAL_CLIS** for enabling/disabling RAL
- **S_RAL_ELOG** for the error and action logs
- **S_RAL_LDOM** for log domains
- **S_RAL_LOG** for read access log data
- **S_RAL_PDAT** for performance trace data
- **S_RAL_PURP** for logging purposes
- **S_RAL_REC** for configuration of recordings
- **S_RAL_TADM** for technical administration tasks

---

**FIGURE 1** On this screen, users can define the logging purpose ID, name, and description.
accesses that will be logged in the channel or UI technology that was selected in the previous step for the recording.

To create a new configuration, click Configuration in the Administration tab. Search for the relevant recording and assign it to this new configuration by selecting it and clicking Create. The fields contained in the recording will appear as parameters in the configuration settings (see Figure 4). Select the fields you want to include in the log configuration and assign log domains to them. You can also assign conditions.

**Step 5: Enable the Logging**

Once the log configuration is complete — and transported if necessary (see the “Centralizing Your RAL Configuration Using Transports” sidebar on the next page) — you are then ready to enable RAL. RAL includes an enable/disable function that gives you the option to set, per client, whether logging is active.

RAL is disabled by default. While you can create configurations for logging with RAL disabled, for the configured logging to execute, you must explicitly enable it for each client in which you want logging to occur. To enable RAL, choose Enabling in Client in the Administration tab, click Edit, and select the Enable Read Access Logging in Client checkbox. To disable logging, deselect the checkbox. It might make sense to temporarily disable RAL when it’s not needed to avoid cluttering the log results with unnecessary information.

Once RAL has been enabled, access to data via the configured channels will be recorded.

**Note:** If you would like to exclude logging the activities of specific users, such as technical users who run expected, scheduled background jobs, you can do so with the user exclusion list. Simply click User Exclusion List in the Administration tab, and then Edit and Add User.
Viewing Log Results
RAL provides a monitor function so administrators can look up the data access events recorded by the log configuration. Choose Read Access Log in the Monitor tab of the SRALMANAGER transaction, and simply search for the log entries you want to evaluate (see Figure 5).

You can search for log events by channel, time, user, and other parameters. You can quickly and easily change the search parameters using the drop-down menus below each search field. Select a log entry to view the information recorded based on the configuration. Under the Details tab, you will see the information logged for the event selected. If you choose the Access Environment tab, you can also look at the technical details of a log entry, such as the service call that triggered the entry.

The RAL Error Log and Action Log
In addition to the events recorded by the log configuration, RAL keeps an error log and an action log, accessed via transaction SRAL_ADMIN to help with error handling and troubleshooting. The error log contains failure messages reported by the framework itself (for example, errors involving communication issues), while the action log tracks all changes to the configuration of the framework (for example, changes made to configurations, the user exclusion list, and enabling or disabling of logging).

To view these logs, go to transaction SRAL_ADMIN and choose the relevant log. Specify the time range, for example, as selection criteria, and the log will list all the errors (for the error log) or changes (for the action log) that occurred during the selected range, including which user produced the error or made the change, and when and where it occurred. See the “Archiving Recorded Logging Data” sidebar for information about archiving the error and action logs.

Centralizing Your RAL Configuration Using Transports
The Read Access Logging functionality includes a transport manager that allows you to centrally configure RAL and then transport the configuration settings — such as logging purposes, log domains, channel configurations, the user exclusion list, and the logging parameters.

To create a transport, open transaction SRAL_TRANS, select the type of data to transport, and click Execute. Then select the objects to transport, click the create transport request icon, and specify the transport details.

Archiving Recorded Logging Data
Read Access Logging is integrated into the standard archiving infrastructure of SAP NetWeaver, so that you can easily configure archiving and retention periods for all logged data according to your requirements using transaction SARA with the appropriate archiving object.

For the logs recorded by your RAL configuration, you can use transaction SARA with archiving object SRAL. In this case, the archiving rules are based on the logging purpose assigned to the configuration. To archive the error and action logs associated with the configuration, you can use transaction SARA with archiving object SRAL_ELOG.

Conclusion
Your data is the backbone of your business, and ensuring its integrity is crucial. RAL allows you to record all types of access — including read and change access — to your business-critical data to ensure that you can get a detailed overview about who accessed which data and when.

RAL is a part of SAP NetWeaver AS ABAP 7.40 and will be available in release 7.31 soon. In addition, SAP is planning to do more than just provide new functionality for the latest releases. Downports to lower releases are planned, and in the meantime, SAP offers a focused-business solution (FBS) — a fully standardized, pre-built logging solution available from SAP Custom Development that customers can implement in their own environments, including on release levels down to 7.00, ensuring that they have the tools they need to watch over data with confidence.

FIGURE 5 A view of recorded events in the RAL monitor