Integration for SAP Governance, Risk and Compliance Access Control Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Integration for SAP GRC Access Control extends the IBM® Security Verify Identity SAP NetWeaver Adapter.

In addition to the provisioning capabilities of the SAP NetWeaver Adapter, this integration sends access requests to SAP GRC Access Control for Separation of Duties (SoD) checks. The SAP GRC Access Control result allows a decision to be made on whether to provision the account. The provisioning step can be performed by either the SAP NetWeaver Adapter or by SAP GRC Access Control. The integration contains components that enable IBM Security Verify Identity to integrate with SAP GRC Access Control 5.3, 10.0, and 10.1.

This integration can also invoke the SAP GRC Access Control Risk Analysis web service on role assignments during an access request. It also enables rejected accounts and role assignments to be removed from the access request that was sent to the SAP NetWeaver Adapter.

The integration and configuration steps apply to SAP GRC Access Control 10.0 and 10.1.

Architecture of the integration

The integration uses two profiles. The first profile contains SAP NetWeaver Adapter account and service attributes only. This profile does not enable a connection with SAP GRC Access Control. The second profile contains an extended set of account and service attributes for interaction between SAP GRC Access Control (Version 5.3, 10.0, and 10.1) and SAP NetWeaver.

This interaction enables IBM Security Verify Identity to coordinate the account compliance checking process in SAP GRC Access Control with the SAP NetWeaver account provisioning process. This profile effectively enables a single account provisioning request to perform two tasks:

1. Submission of an access request to SAP GRC Access Control from IBM Security Verify Identity.
2. Submission of an account provisioning request to SAP NetWeaver from IBM Security Verify Identity, depending whether an approval or rejection is granted for the IBM Security Verify Identity request.

The relationships between components of the adapter are shown in Figure 1 on page 1.

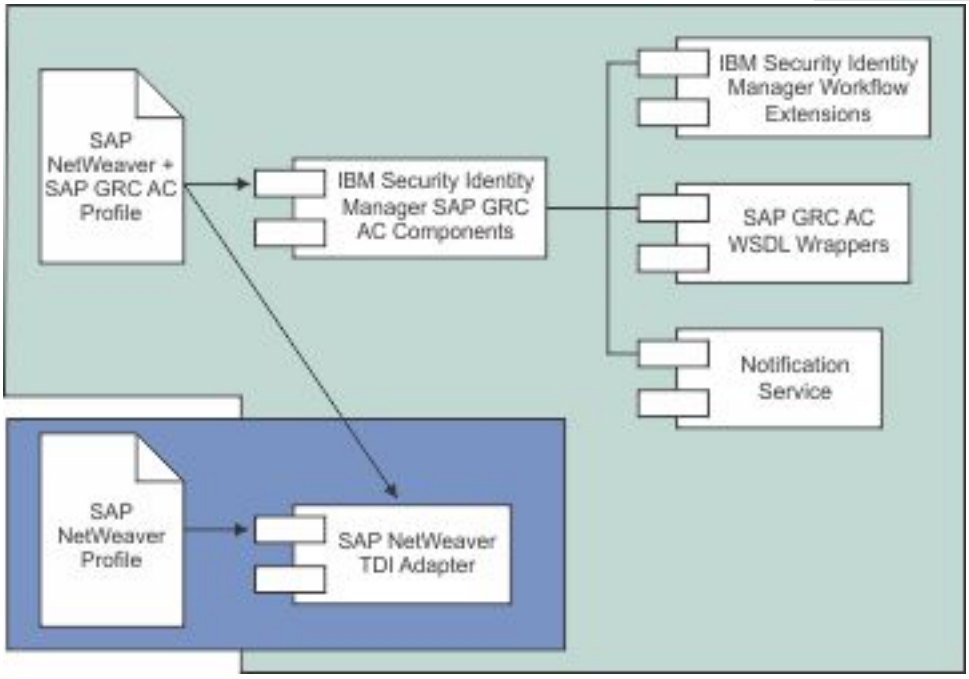


Figure 1. IBM Security Identity Manager SAP NetWeaver Adapter with Integration for SAP GRC Access Control components and relationships

A high level of control is obtained over the provisioning process by configuring IBM Security Verify Identity workflow extensions for SAP GRC Access Control. The IBM Security Verify Identity workflow extensions allow *Add*, *Modify*, *Suspend*, *Restore*, and *Delete* requests to be sent to SAP GRC Access Control. SoD compliance checks are then performed in SAP GRC Access Control before provisioning the account in SAP NetWeaver. The risk analysis and remediation features of SAP GRC Access Control Compliant Provisioning can be used to:

- Modify the request
- Submit an approval
- Submit a rejection
- Cancel the request

In IBM Security Verify Identity workflow, there are two possible modes to configure each type of request. These modes are referred to as **Non-blocking** mode and **Blocking** mode.

In **Non-blocking** mode, SAP GRC Access Control takes control of account provisioning on the target system. Following submission of an access request to SAP GRC Access Control, IBM Security Verify Identity workflow continues execution and does not wait for the result of the request in SAP GRC Access Control. This mode passes the responsibility of provisioning the account in SAP NetWeaver to SAP GRC Access Control.

In **Blocking** mode, IBM Security Verify Identity workflow blocks (or wait/pause) following submission of an access request to SAP GRC Access Control. The workflow continues to block until the result of the request is received from SAP GRC Access Control. A dedicated Notification Service deployed in WebSphere® is responsible for

- Periodically querying SAP GRC Access Control
- Relaying results of completed requests to IBM Security Verify Identity
- Unblocking the relevant IBM Security Verify Identity workflows.

The IBM Security Verify Identity workflow becomes the central point of coordination and auditing for account provisioning. IBM Security Verify Identity determines whether an account is provisioned in SAP NetWeaver, depending on pre-conditions such as whether the request was approved or rejected in SAP GRC Access Control.

Related concepts

Supported configurations
The integration requires the interaction of several components.

Supported configurations

The integration requires the interaction of several components.

The fundamental components of the integration are:

- An IBM Security Verify Identity Server
- A Tivoli® Directory Integrator server
- An IBM Security Verify Identity SAP NetWeaver Adapter
- The Integration for SAP GRC Access Control 5.3, 10.0 and 10.1

Related concepts

Architecture of the integration
The integration uses two profiles. The first profile contains SAP NetWeaver Adapter account and service attributes only. This profile does not enable a connection with SAP GRC Access Control. The second profile contains an extended set of account and service attributes for interaction between SAP GRC Access Control (Version 5.3, 10.0, and 10.1) and SAP NetWeaver.

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Note: There is a separate instruction for installing, upgrading or uninstalling adapters from the IBM Security Verify Governance Identity Manager virtual appliance.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Load attribute mapping.
8. Set account defaults.
9. Create an adapter service/target.
10. Install the adapter language package.
11. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a full installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
    a. Configure 1-way authentication.

b. Configure 2-way authentication.

3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter..

Table 1 on page 4 identifies hardware, software, and authorization prerequisites to install the Integration for SAP GRC Access Control.

Table 1. Prerequisites to install the integration

Prerequisite	Description
Operating System	The Integration for SAP GRC Access Control can be used on any operating system that is supported by Identity server.
Network Connectivity	TCP/IP network
System Administrator Authority	The person who completes the Integration for SAP GRC Access Control installation procedure must have system administrator authority.

Table 1. Prerequisites to install the integration (continued)	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Dispatcher	See the SAP NetWever adapter release notes for the supported versions.
IBM Websphere Application Server*	WebSphere Application Server 7.0 FixPack 19 (7.0.0.19)
SAP NetWeaver AS ABAP with SAP Basis Component	See the SAP NetWever adapter release notes for the supported versions.
SAP JCo	3.0.8
SAP GRC Access Control	5.3, 10.0 FP08, and 10.1

* The minimum WebSphere Application Server FixPacks listed are required to satisfy web service dependencies that the integration has in WebSphere.

Software downloads

Download the software through your account at the IBM Passport Advantage® website.

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Governance Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 2. Required information to install the integration

Required information	Description
Administrator account on the managed resource for SAP GRC Access Control 5.3	An administrator account on the managed resource that has the necessary administrative privileges for SAP GRC. The administrator account must have the following assigned role in UME: • AEADMIN
Administrator account on the managed resource for SAP GRC Access Control 10.0 and 10.1	An administrator account on the managed resource that has the necessary administrative privileges for SAP GRC 10.0 and 10.1. The administrator account must have at least the following assigned roles: • SAP_GRC_NWBC • SAP_GRAC_* See the GRC 10.0 and 10.1 Post-installation and Security guides for further information.
SAP GRC 10.0 and 10.1 Web Service Endpoint creation	Endpoint bindings must be created in the transaction SOAMANAGER under Service Administration – Single Service Configuration - Configurations, for at least the following SAP GRC 10.0 and 10.1 web services: • GRAC_AUDIT_LOGS_WS • GRAC_LOOKUP_WS • GRAC_REQUEST_DETAILS_WS • GRAC_REQUEST_STATUS_WS • GRAC_RISK_ANALYSIS_WITH_NO_WS • GRAC_USER_ACCES_WS After the endpoint binding has been created, the "Calculated Access URL" for the web service is found under the "Transport Settings" tab. This URL is defined on the service form. The service form in the SAP GRC Access Control integration and `SAPNotify.props` make use of these URLs to locate the relevant SAP GRC Access Control 10.0 and 10.1 web service.

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the *Dispatcher Installation and Configuration Guide*.

Related concepts

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions
You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the *Dispatcher Installation and Configuration Guide*.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions
You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing the adapter profile

An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Before you begin

- The Identity server is installed and running.
- You have root or administrator authority on the Identity server.
- The file to be imported must be a Java™ archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.The JAR file for the IBM Security Identity Governance and Intelligence is located in the `IGI-profile` folder of the installation package.

About this task

Target definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

Procedure

1. On the Appliance Dashboard, select Verify Governance Identity Manager Administration Console from the **Quick Links** widget.

   The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**.

The Target Administration console is displayed.

3. From the navigation tree, select **Manage Target Types**.

   The **Manage Target Types** page is displayed.

4. On the **Manage Target Types** page, click **Import**.

   The **Import Target Type** page is displayed.

5. On the **Import Target Type** page, complete these steps:

   a) In the **Target Definition File** field, click **Browse** to locate the <*Adapter*>`Profile.jar` file. For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the AD`ProfileJAR` file.

   b) Click **OK**.

      A message indicates that you successfully imported a target type.

6. Click **Close**.

What to do next

- The import occurs asynchronously, which means it might take some time for the target type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Target Types** page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. On the Appliance Dashboard, select **Manage System Settings** > **Maintenance** > **Log Retrieval and Configuration** > **Identity** > **trace log**, then click **View**.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions
You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.

   ```
   [conversion].<target_attribute>.<IGI_attribute> =
   [<target_attribute_value1>=<IGI_attribute_value1>;...;
   <target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

   ```
   [conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
   [conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
   [dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
   ```

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

   For more information, see *Mapping attributes for a connector* in the IBM Security Verify Governance Identity Manager product documentation.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions
You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Creating an adapter service/target

After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Before you begin

Complete “Importing the adapter profile” on page 8.

About this task

You must create an administrative user account for the adapter on the managed resource. Provide the account information when you create a target. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

Use the target form to provide information for the target. The actual target form fields might vary depending on whether the service form is customized. The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. On the Appliance Dashboard, select Verify Governance Identity ManagerAdministration Console from the **Quick Links** widget.

   The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**.

   The Target Administration console is displayed.
3. From the navigation tree, click **Manage Targets**.

The **Select a Target** page is displayed.

4. On the **Select a Target** page, click **Create**.

   The **Create a Target** wizard is displayed.

5. On the **Select the Type of Target** page, select a target type and click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

6. On **General Information** page, specify the values for the target instance.

   The content of the **General Information** page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.

7. On the **Users and Groups** page, which is displayed only for LDAP targets, complete the required fields.
8. On the **Authentication** page, which does not display for every target type, complete the required fields.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes and click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based targets.

10. On the **Status and Information** page, view information about the adapter and managed resource and click **Next** or **Finish**.

    The adapter must be running to obtain the information.

11. On the **Application Information** page, type a name and description for the application, and then click **Finish**.
12. Optional: Click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the target instance for a specific target type.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions
You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile

An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Service/Target form details

Complete the service/target form fields.

See #unique_18 in the *Directory Integrator-based Adapter for SAP NetWeaver Adapter Installation and Configuration Guide*. The `SapGRCNWProfile.jar` profile contains an additional SAP GRC **Service Attributes** tab. It contains the set of the following attributes.

Enable GRC Workflow Extensions
Optional attribute. Flag to indicate whether workflow extensions are configured for either SAP GRC Access Control 5.3, 10.0 and 10.1. The value of this flag is only used by the "Check GRC Version" workflow extension. It has no effect otherwise.

Disable SYS line
Select this check box if you want to disable the system line in the assignment list of the SAP GRC approval screen.

GRC Version
Optional attribute. The version of SAP GRC Access Control the service is configured against. This attribute can be used in the workflow to determine the path to take if these conditions exist:

- A combination of different SAP GRC Access Control versions exists in the environment.
- The environment is supported by a single Identity server instance.

The value of this flag is only used by the "Check GRC Version" workflow extension. It has no effect otherwise.

GRC Admin Id
The SAP GRC Access Control user name with privileges to invoke SAP GRC web services and submit Access Control requests. A value is required if the authentication and security services are enabled on the SAP NetWeaver Application server on which Access Control is deployed.

GRC Password
Password of the SAP GRC Access Control Admin ID.

Access Control Request URL
The URL address of the Access Control Submit Request web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from Identity server.

For example, the URL for SAP GRC 5.3 might be specified as `http://remotehost:port/SAPGRC_AC_IDM_SUBMITREQUEST/Config1?style=document`

The URL for SAP GRC 10.0 and 10.1 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_user_acces_ws/clientnumber/grac_user_acces_ws/binding?sap-client=clientnumber`

Access Control Look Up URL
The URL address of the Access Control Look Up Request web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from Identity server.

For example, the URL for SAP GRC Access Control 10.0 and 10.1 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_lookup_ws/clientnumber/grac_lookup_ws/binding?sap-client=clientnumber`

Access Control Risk Analysis URL

The URL address of the Access Control Risk Analysis Request with Request ID web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from Identity server.

For example, the URL for SAP GRC Access Control 10.0 and 10.1 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_risk_analysis_with_no_ws/clientnumber/grac_risk_analysis_with_no_ws/binding?sap-client=clientnumber`

Access Control Request Details URL

The attribute for Update Account Attribute Request. The URL address of the Access Control Request Details web service. The format is `http://remotehost:port/web-service-name` where:

- The *remotehost* is the SAP GRC Access Control host.
- The *port* is the port number on which SAP NetWeaver ABAP application server listens.
- The *web-service-name* is the web service exposed by SAP GRC Access Control that receives requests from Identity server.

For example, the URL for SAP GRC Access Control 10.0 and 10.1 might be specified as `http://remotehost:port/sap/bc/srt/rfc/sap/grac_request_details_ws/clientnumber/grac_request_details_ws/binding?sap-client=clientnumber`

System Identifier

The system identifier is the SAP connector name defined in Access Control to enable provisioning directly to the target SAP ABAP server from SAP GRC Access Control. This system identifier is also supplied to SAP GRC Access Control on a request submission in the account role data.

Detail Logging

Optional attribute. Flag to enable SAP GRC request debugging trace output. For SAP GRC Access Control 5.3, this option writes a log file called `grcextension.log` to the location specified by the Java system property **`user.home`**. For SAP GRC Access Control 10.0 and 10.1, this option enables the trace log file for the workflow extension component.

Note: The logging level must be set to DEBUG_MIN.

Related concepts

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Installing and configuring the workflow extensions

You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Installing and configuring the workflow extensions

You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

There are slightly different procedures to follow depending on which target system you want to support.

Support SAP GRC Access Control 10.0 and 10.1 only

1. “Installing SAP GRC Access Control 10.0 and 10.1 workflow extensions” on page 16
2. “SAP GRC Access Control 10.0 and 10.1 workflow extension configuration” on page 16
3. “Log file locations for workflow extensions” on page 26
4. “Installing and configuring the notification component for SAP GRC Access Control version 10.0 or 10.1” on page 23

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Installing SAP GRC Access Control 10.0 and 10.1 workflow extensions

Use the Workflow extension page to add custom workflow extensions to the IBM Security Verify Identity virtual appliance.

Procedure

SAP GRC Access Control 10.0 and 10.1 workflow extension configuration

SAP GRC Access Control 10.0 and 10.1 workflow extensions support these different SAP GRC operations: Access Request, Risk Analysis, and Update Account Attributes.

Use these steps to configure these workflow extensions using the Add operation as an example:

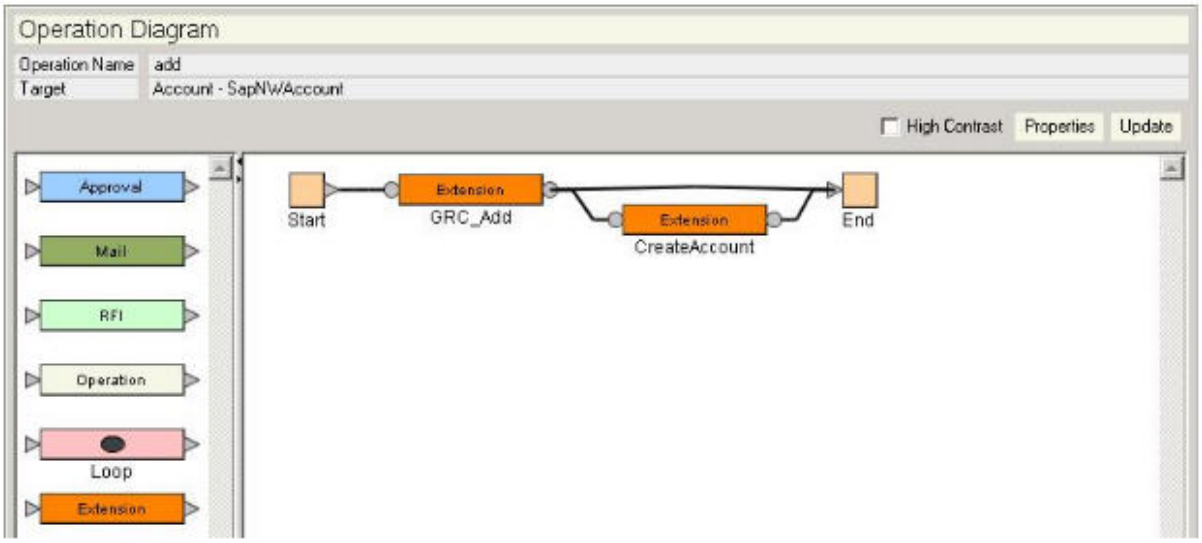
- “Configuring Access Request workflow extension (Blocking requests)” on page 16
- “Configuring Risk Analysis workflow extension” on page 19
- “Configuring Update Account Attributes workflow extension” on page 22

Configuring Access Request workflow extension (Blocking requests)

In Blocking mode, the IBM Security Verify Identity workflow blocks, waits, or pause after the submission of an access request to SAP GRC Access Control.

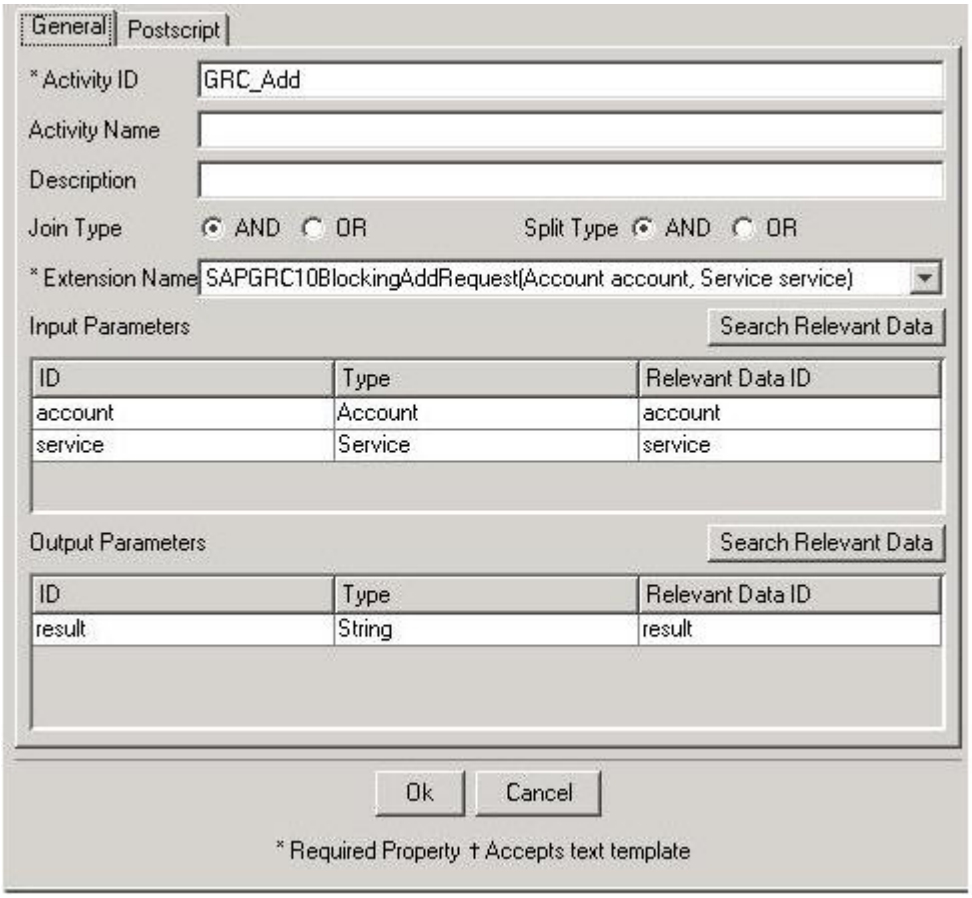
Procedure

1. Log on to IBM Security Verify Identity.
   a) Select **Configure System** > **Manager Operations**.
   b) For the **Operation Level**, select **Entity level**.
   c) Select **Account** as the **Entity type**.
   d) Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click **Add** to create an add operation if it does not exist.
   The operation diagram is displayed. Provide the same changes as shown in the following screen capture.

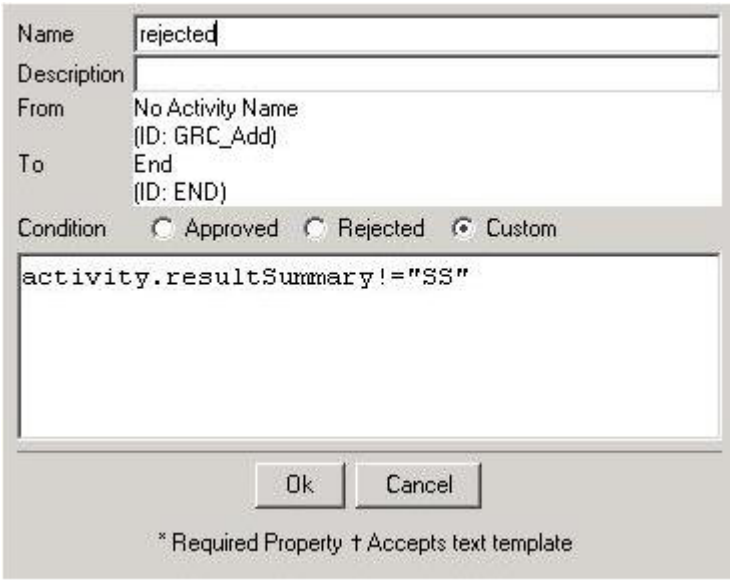


3. Remove the transition line from the **Start** node to the **CREATEACCOUNT** extension node.
4. Add an extension node between **Start** and **CREATEACCOUNT**.

5. Double-click the new **Extension** node. A pop-up window displays all the extensions registered by using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRC10BlockingAddRequest** and fill in the **Activity ID** with **GRC_ADD**. Set the **Activity Name** to **GRC ADD**.
7. Select **OR** for the **Split Type**.



   a) For `account`, click **Search Relevant Data** to specify `account` as the **Relevant Data ID** value.
   b) For `service`, click **Search Relevant Data** to specify `service` as the **Relevant Data ID** value.
   c) Under **Output Parameters**, enter `result` in the ID field. Ensure that **Type** is set to **String** and leave **Default Value** blank.
   d) Click **Ok**.
   e) Select **Search Relevant Data** to specify `result` as a value for **Relevant Data ID** and click **Ok**.
8. Click **Ok** and attach the transitions to the newly added extension.
9. Click **Properties**.
10. Click **Add** next to Relevant Data.
11. Create a result **Relevant Data**. Specify result in the **ID** field.
12. Ensure that the **Type** is String and leave **Default Value** as blank.
13. Click **Ok** to finish.
14. Double-click the transition that connects the newly added extension to the **CREATEACCOUNT** extension node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **Ok** to close the transition properties window.
15. Double-click the transition that connects the newly added extension to the **END** node and key in the condition `activity.resultSummary!="SS"`. Name the transition "rejected". Click **Ok** to close the transition properties window.



16. Click **Update** and then click **Ok** to close the **Operations** window.
17. Repeat Steps 2 to 15 for delete, modify, suspend, and restore operations.

Configuring Access Request workflow extension (Non-blocking requests)

In Non-blocking mode, SAP GRC Access Control takes control of account provisioning on the target system

Procedure

1. Log on to IBM Security Verify Identity.
   a) Select **Configure System** > **Manager Operations**.
   b) For the **Operation Level**, select **Entity level**.
   c) Select **Account** as the **Entity type**.
   d) Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click the **Add** button to create an add operation if it doesn't exist.
3. Remove the transition line from the **Start** node to the **CREATEACCOUNT** extension node.
4. Add an extension node between **Start** and **CREATEACCOUNT**.
5. Double-click the new **Extension** node.

   A pop-up window displays all the extensions that are registered by using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRC10NonBlockingAddRequest** and fill in the **Activity ID** with **GRC_ADD**. Set the **Activity Name** to **GRC ADD**.
7. Select **OR** for the **Split Type**.
   a) For `account`, click **Search Relevant Data** to specify `account` as the **Relevant Data ID** value.
   b) For `service`, click **Search Relevant Data** to specify `service` as the **Relevant Data ID** value.
   c) Under **Output Parameters**, enter `result` in the ID field. Ensure that **Type** is set to **String** and leave **Default Value** blank.
   d) Click **Ok**.
   e) Select **Search Relevant Data** to specify `result` as a value for **Relevant Data ID** and click **Ok**.
8. Click **Ok** and attach the transitions to the newly added extension.
9. Click **Properties**.

10. Click **Add** next to Relevant Data.
11. Create a **result** Relevant Data. Specify result in the **ID** field. Ensure that the **Type** is String and leave **Default Value** blank. Click **Ok** to finish.
12. Double-click the transition that connects the newly added extension to the **End** node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **Ok** to close the transition properties window.
13. Click **Update** and then click **Ok** to close the **Operations** window.
14. Repeat Steps 2 to 13 for delete, modify, suspend, and restore operations.

    Note: When configuring the properties of the newly added extension nodes (see Step 6) for these operations, the following values can be used:

Table 3. SAP GRC Access Control Workflow Extension Options

Blocking Operations	**ActivityID**	**Extension Name**
ADD	GRC_ADD	SAPGRCBlockingAddRequest
DELETE	GRC_DELETE	SAPGRCBlockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRCBlockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRCBlockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRCBlockingSuspendRequest
Non-Blocking Operations	**ActivityID**	**Extension Name**
ADD	GRC_ADD	SAPGRCNonblockingAddRequest
DELETE	GRC_DELETE	SAPGRCNonblockingDeleteRequest
MODIFY	GRC_MODIFY	SAPGRCNonblockingModifyRequest
RESTORE	GRC_RESTORE	SAPGRCNonblockingRestoreRequest
SUSPEND	GRC_SUSPEND	SAPGRCNonblockingSuspendRequest

Configuring Risk Analysis workflow extension

This workflow extension allows IBM Security Verify Identity to send a risk analysis request for a specific access request ID to SAP GRC Access Control 10.0 and 10.1.

About this task

The risk analysis result is recorded by IBM Security Verify Identity workflow as a string output parameter named“riskDetail”. Risk results returned from SAP GRC Access Control are indicated by a ‘#’ character. Each risk consists of a number of name-value pairs. These name-value pairs are separated by a ‘|’ character. The risk name and its value are separated by a ‘:’ character. If the value is multi-valued, then the set of values is enclosed by ‘[ ]' characters, and each value in the set is separated by a ‘,' character.

An example of the riskDetail returned to IBM Security Verify Identity workflow looks like:

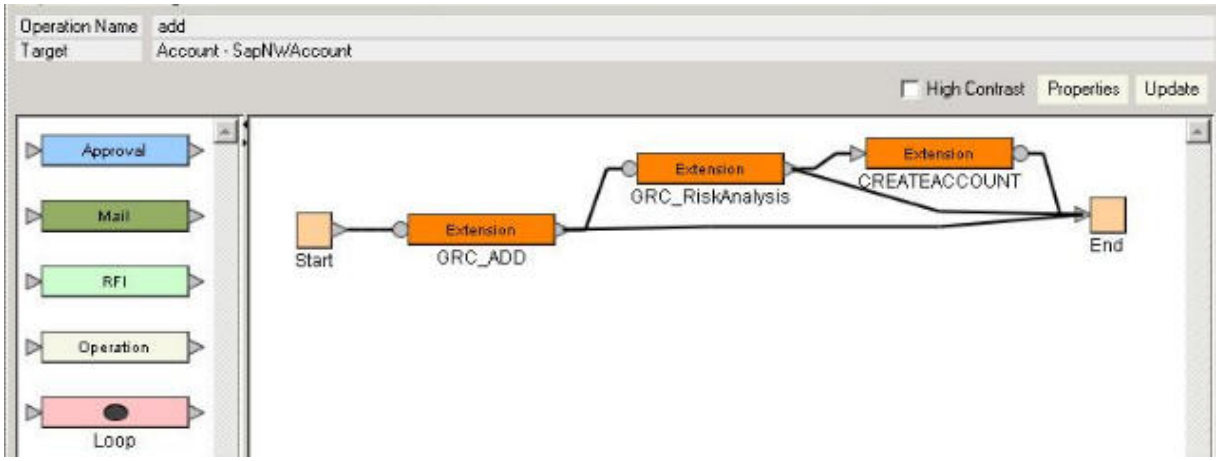
```
#Risk Number:1|Risk Id:B009|Risk Description:Basis Table Maintenance & System
Administration|Risk Level:High|System Name:GC7CLNT001|User Id:AC102509|Role
List:[SAP_XI_ADMINISTRATOR_ABAP, SAP_XI_CONFIGURATOR,
SAP_XI_BPE_ADMINISTRATOR_ABAP, SAP_XI_ADMINISTRATOR]|Action List:[SXMB_ADM,
SM30, SM12, SXMB_ADM_BPE, SM59]|
```

If necessary, the output parameter can be parsed in IBM Security Verify Identity workflow to catch risk violations that have been detected by SAP GRC Access Control 10.0 and 10.1. Detail on how to parse the riskDetail output parameter is out-of-scope of this guide.

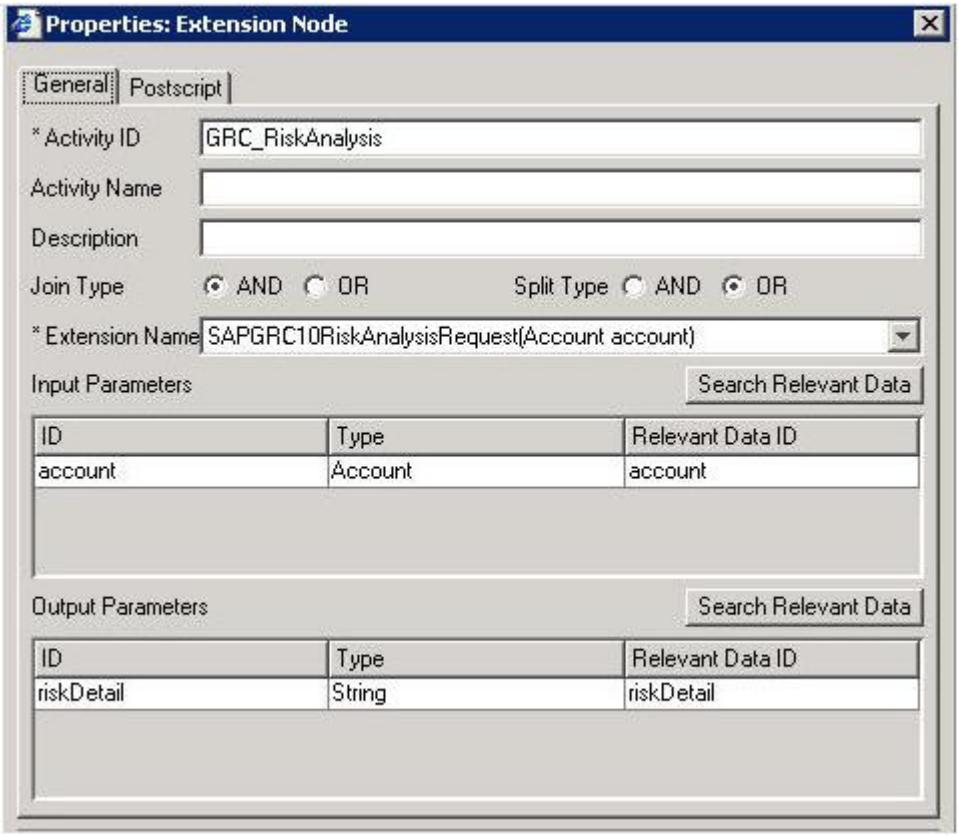
Define Risk Analysis workflow extensions for the existing SAP GRC NetWeaver account type.

Procedure

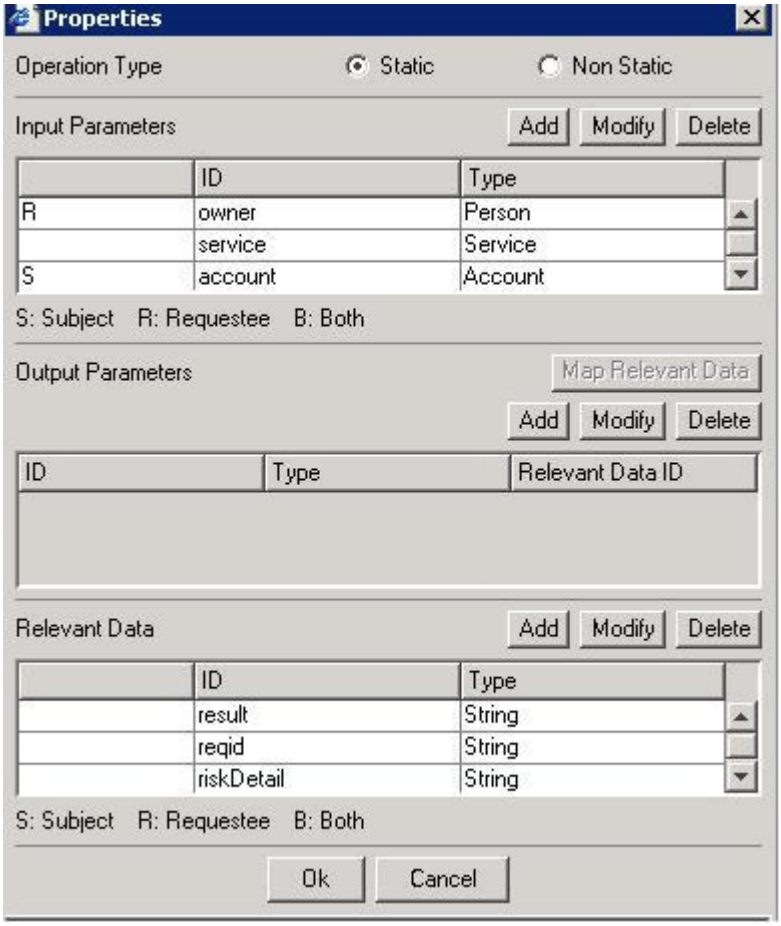
1. Log on to IBM Security Verify Identity.
   a) Select **Configure System > Manager Operations**.
   b) For the **Operation Level**, select **Entity level**.
   c) Select **Account** as the **Entity type**.
   d) Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.
2. Click the **Add** button to create an add operation if it does not already exist.
   The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



3. Remove the transition line from the **GRC_ADD** extension node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **GRC_ADD** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node.
   A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Select the **Extension Name** as **SAPGRC10RiskAnalysisRequest** and fill in the **Activity ID** with **GRC_RiskAnalysis**. Set the **Activity Name** to **GRC RiskAnalysis**.
7. Select **OR** for the **Split Type**.
   a) For `account`, click **Search Relevant Data** to specify `account` as the **Relevant Data ID** value.
   b) For `service`, click **Search Relevant Data** to specify `service` as the **Relevant Data ID** value.
   c) Under **Output Parameters**, enter `result` in the ID field. Ensure that **Type** is set to **String** and leave **Default Value** blank.
   d) Click **Ok**.
   e) Select **Search Relevant Data** to specify `result` as a value for **Relevant Data ID** and click **Ok**.
8. Click **OK** and attach the transitions to the newly-added extension.



9. Click the **Properties** button.
10. Click the **Add** button next to Relevant Data.
11. Create a new **reqid** Relevant Data. Enter **reqid** in the **ID** field.
    Ensure that the **Type** is String and leave **Default Value** as blank. Click **OK** to finish.



12. Create a new **riskDetail** Relevant Data. Enter **riskDetail** in the **ID** field.

    Ensure that the **Type** is String and leave **Default Value** as blank. Click **OK** to finish.
13. Double-click on the transition connecting the newly-added extension to the **CREATEACCOUNT** extension node and key in the condition `activity.resultSummary=="SS"`. Name the transition "approved". Click **OK** to close the transition properties window.
14. Double-click on the transition connecting the newly-added extension to the **END** node and key in the condition `activity.resultSummary!="SS"`. Name the transition "rejected". Click **OK** to close the transition properties window.
15. Click **Update** and then click **OK** to close the Operations window.
16. Repeat Steps 2 to 14 above for another operation when risk analysis is applicable.

Configuring Update Account Attributes workflow extension

This workflow extension compares the list of roles on an approved request that is returned by SAP GRC Access Control 10.0 with the list of roles that are requested by IBM Security Verify Identity.

About this task

If the status of a role is not “approved”, then the role is assumed to have been rejected in SAP GRC AC 10.0. The extension then removes the rejected roles from the request in IBM Security Verify Identity. The same behavior applies to rejection of account assignments. This workflow extension should be executed before the account is provisioned in SAP NetWeaver.

Define Update Account Attribute workflow extensions for the existing SAP GRC NetWeaver account type.

Procedure

1. Log on to IBM Security Verify Identity.

a) Select **Configure System > Manager Operations**.

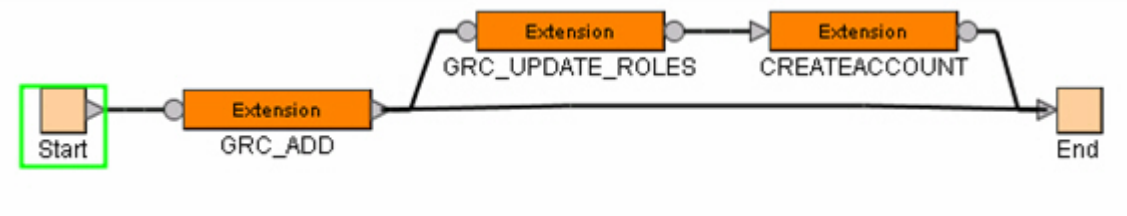
b) For the **Operation Level**, select **Entity level**.

c) Select **Account** as the **Entity type**.

d) Select **SAP GRC NetWeaver Account** as the type of account to be configured with the SAP GRC Access Control workflow extension.

2. Click the **Add** button to create an add operation if it doesn't already exist.

   The operation diagram is displayed. Provided the same changes as those shown in the following screen capture.



3. Remove the transition line from the **GRC_ADD** extension node to the **CREATEACCOUNT** extension node.
4. Add a new extension node between **GRC_ADD** and **CREATEACCOUNT**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using `workflowextensions.xml`.
6. Set the **ActivityId** to **GRC_UPDATE_ACCOUNT** and **ExtensionName** as **SAPGRC10UpdateAccountAttributesExtension(Account account, Service service)**.
7. Click **Ok** to save and close the popup window.

   a) For `account`, click **Search Relevant Data** to specify `account` as the **Relevant Data ID** value.

   b) For `service`, click **Search Relevant Data** to specify `service` as the **Relevant Data ID** value.

   c) Under **Output Parameters**, enter `result` in the ID field. Ensure that **Type** is set to **String** and leave **Default Value** blank.

   d) Click **Ok**.

   e) Select **Search Relevant Data** to specify `result` as a value for **Relevant Data ID** and click **Ok**.
8. Connect the **GRC_UPDATE_ACCOUNT** extension node to the **End** node with a transition line.

   Enter the following condition:

```
activity.resultSummary!="SS"
```

9. Click **Update** and then click **Ok** to close the Operations window.
10. Repeat steps 2 to 7 above for another operation when update account attributes is applicable.

Installing and configuring the notification component for SAP GRC Access Control version 10.0 or 10.1

Install the notification component for SAP GRC Access Control version 10.0 and 10.1.

Procedure

1. If the `SAPGRC10Workflow.jar` file does not exist for SAP GRC Access Control 10.0 or 10.1, copy it from the installation package `\workflow\grc10\SAPGRC10Workflow.jar` to the directory:

   WEBSPHERE_HOME`\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\ITIM.ear\app_web.war\WEB-INF\lib`

   If the `\WEB-INF\lib` directory does not exist, create one.

2. Copy the `jaas_login_was.conf`, `runNotifierWAS7.[bat|sh]`, and `SAPNotify.props` files from the installation packages `workflow\grc10\notifier` to a directory on the IBM Security Verify Identity server.

   Use the `runNotifierWAS7.sh` file for UNIX systems or the `runNotifierWAS7.bat` file for Windows systems.

3. Edit the **runNotifierWAS7** script and update the following variables to match your environment:

APP_SRV_HOME	The location of the IBM Security Verify Identity server, including the profile name. For example: `c:\Program Files\IBM\WebSphere\AppServer\profiles\server1`
JAVA_HOME	The location of the root directory of a JAVA installation. For example, `c:\Program Files\IBM\WebSphere\AppServer\java`
ITIM_HOME	The location on the IBM Security Verify Identity installation, not the ITIM deployed ear. For example: `c:\Program Files\IBM\itim`
APP_SRV_CELL	Name of the WebSphere cell that the IBM Security Verify Identity application is deployed on. This attribute is required to find the `SAPGRC10Workflow.jar` file.
WFE_HOME	The location of the `SAPGRC10Workflow.jar` file.

4. Edit the `SAPNotify.props` file and provide the correct value for each of the attributes.

GRCNotifyURL	This attribute is the URL to the SAP GRC Access Control 10.0 and 10.1 Audit Logs Web Service. For example, the URL could resemble: `http://`*`remotehost`*`:`*`port`*`/sap/bc/srt/rfc/sap/grac_audit_logs_ws/`*`client_number`*`/grac_audit_logs_ws/binding?sap-client=`*`client_number`*
GRCUserName	An administration or user ID used to access the SAP GRC Access Control system.
GRCPassword	The password for the Administrator user name.
itim.user	An IBM Security Verify Identity user with administration privileges.
itim.pswd	The password for the IBM Security Verify Identity user.
itim.home	Path to the IBM Security Verify Identity server directory. For example, the path might be: `C:/Program Files/IBM/itim`
apps.context.factory	This attribute is the context to get access to the IBM Security Verify Identity server. Use the default value `com.ibm.itim.apps.impl.websphere.WebSpherePlatformContextFactory`, unless otherwise instructed by an IBM representative.
`isim.authentication.factory.classname`	This attribute is the authentication factory class name. For IBM Security Verify Identity 6.0. Use the default value `com.ibm.tivoli.auth.ISIM6AuthenticationFactory` ,unless otherwise instructed by an IBM representative.
isim.jaas.logincontextname	This attribute is the JAAS login context name. The default value is used if no value is defined. For IBM Security Verify Identity 6.0, the default value is `WSLogin`.
enrole.appServer.realm	This attribute is the application server realm name. The default value is defined in the *`ISIM_HOME`*`\data\ enrole.properties` file.
encryption.password	This attribute is the keystore password. It is for IBM Security Verify Identity 6.0 only. The default value is defined in *`ISIM_HOME`*`\data\enrole.properties`.

5. Encrypt the passwords in the **SAPNotify.props** file of the SAP NetWeaver Adapter. Add **{protect}** before the property name in the file as follows:

```
{protect}<Property Name>=<Property Value>
```

For example, **{protect}GRCPassword=Passw0rd**.

After running the notifier, the property value in the **SAPNotifier.props** file changes as follows:

```
{protect}<Property Name>={encr}<Encrypted Property Value>
```

For example, **{protect}GRCPassword={encr}VsBnPSfYoqpSUidp1v36FkxlPvOSCGxfgvpD**.

Note: To change the value of a property, delete the encrypted string along with **{encr}** and write the new property value in clear text format after **=**.

6. Validate the configuration by running **runNotifierWAS7** from the command line. The following two lines are displayed on the command line:

```
Starting Notifier
......
Stopping Notifier
```

The notification service updates all relevant workflows in IBM Security Verify Identity to either "APPROVED_SUCCESS" or "APPROVED_REJECTED" if:

- There is a request in SAP GRC that was closed, either "Approved," "Rejected," or "Cancelled".
- The request has a matching SAP GRC Access Control request ID for an IBM Security Verify Identity workflow currently in the PENDING state.

7. Edit the `logging.properties` file in the JAVA_HOME lib directory to enable more or less logging.

For example, *WAS_HOME*`\java\jre\lib\logging.properties`

This log file contains the jlog configuration. By adding the following line the logging level can be increased:

```
com.ibm.tivoli.sapgrc10.level=ALL
```

The console handler might also need to be increased to allow for the output of all logging:

```
java.util.logging.ConsoleHandler.level=ALL
```

8. Logging might be disabled. This disablement might be required when running the notifier as a scheduled task. To turn logging off, set the following values:

```
java.util.loging.ConsoleHandler.level=NONE
com.ibm.tivoli.sapgrc10.level=NONE
```

9. If security is enabled on WebSphere, import the WebSphere key into the IBM Security Verify Identity keystore.

The IBM Security Verify Identity keystore file and its password are defined in the *ISIM_HOME*`\data\enrole.properties` file, look for the **enrole.encryption.keystore** and **enrole.encryption.password**:

a. Navigate to the *WAS_HOME*`\bin` directory.
b. Launch the `ikeyman.bat` file from `C:\Program Files\IBM\WebSphere\AppServer\bin`.
c. Select **Key Data File** > **Open**.
d. Select Key database type **PKCS12** and then browse to the keystore file in *WAS_HOME*`\config\cells\iqint17aNode01Cell\nodes\iqint17aNode01\key.p12`
e. Enter the keystore password `WebAS`.
f. Select **Export** to export the key to a temp directory `C:\temp\default.p12`.
g. Enter password `WebAS`.
h. Select **Key Data File** > **Open**.
i. Select Key database type **JCEKS** and then browse to the IBM Security Verify Identity keystore.
j. Enter the keystore password.

k. Select **Import** to import the key from `C:\temp\default.p12` into the IBM Security Verify Identity keystore and save it.

10. After confirming that the configuration is correct, place the **runNotifierWAS7** script into a scheduled task so that it runs on a regular basis.

    On Windows systems, use the Windows scheduler to schedule the task. On Linux® or UNIX systems, use the **crontab** command. Contact your system administrator to set up these tasks.

Log file locations for workflow extensions

The log file locations for SAP GRC Access Control are different for version 10.0 and 10.1. You must enable logging for SAP GRC Access Control 10.0 and 10.1.

SAP GRC Access Control 10.0 and 10.1

The logging for the workflow extensions is in the IBM Security Verify Identity `trace.log` file.

To enable logging for the extensions, modify the settings in the `enRoleLogging.properties` file in the *ISIM_HOME*`\data\` directory to:

```
logger.trace.com.ibm.tivoli.sapgrc10.wfe.SapGRC10ApplicationExtension.level=DEBUG_MAX
logger.trace.com.ibm.itim.workflowextensions.AccountExtensions.level=DEBUG_MAX
```

Reconciliation configuration for the SAP NetWeaver adapter with SAP GRC Access Control

Because of limitations in the SAP GRC Access Control reconciliation capability, the adapter uses the SAP ABAP server as an account repository for reconciliation process.

As result, all attributes that are specific to SAP GRC Access Control will be lost during reconciliation because the SAP AS ABAP server will not recognize them. To avoid losing values of SAP GRC Access Control-specific attributes, the reconciliation operation must exclude all of the SAP GRC Access Control-specific attributes listed in Table 5 on page 43.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing and configuring the workflow extensions

You can install and configure the SAP GRC Access Control workflow extensions, which are used as workflow objects within the IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Chapter 4. Upgrading

You can upgrade the Integration for SAP GRC Access Control to support SAP GRC Access Control 5.3, 10.0 or 10.1.

Upgrade to support SAP GRC Access Control 10.0 and 10.1

To upgrade the integration to support SAP GRC Access Control 10.0 or 10.1, you must do several tasks.

Follow these steps:

- "Profile import" on page 29
- "SAP NetWeaver GRC service creation" on page 29
- "Installing the SAP GRC Access Control 10.0 and 10.1 workflow extension" on page 29
- "SAP GRC Access Control 10.0 and 10.1 workflow extension configuration" on page 30

Profile import

Obtain the `SapGRCNWProfile.jar` profile from the installation package and import the profile into IBM Security Verify Identity.

SAP NetWeaver GRC service creation

After the `SapGRCNWProfile.jar` is imported into IBM Security Verify Identity successfully, update the attributes under the **SAP GRC Service Attributes** tab on the service form.

See "Creating an adapter service/target" on page 11 for details on how to create a service and how to define those attributes on the SAP GRC Service Attributes tab.

To support the different versions of SAP GRC Access Control with the same profile, the * which indicates mandatory account attributes has been removed from the account form because these attributes are not necessarily required for SAP GRC Access Control 10.0 and 10.1 support. Refer to Table 5 for a full reference of supported account attributes.

Installing the SAP GRC Access Control 10.0 and 10.1 workflow extension

Follow these steps to install the SAP GRC Access Control 10.0 and 10.1 workflow extension.

Procedure

1. Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to add a workflow extension.

   For more information, see "Installing SAP GRC Access Control 10.0 and 10.1 workflow extensions" on page 16.
2. Copy `workflow\grc10\SAPGRC10Workflow.jar` from the installation package to the appropriate directory: *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`

   If the directory does not exist, create one.
3. Restart the IBM Security Verify Identity application from the WebSphere console, or restart the WebSphere server itself.

   After a successful restart, continue with configuration.

SAP GRC Access Control 10.0 and 10.1 workflow extension configuration

The SAP GRC Access Control 10.0 and 10.1 workflow extensions support Access Request, Risk Analysis, and Update Account Attributes features by configuring the IBM Security Verify Identity workflow extension.

For more information, see "SAP GRC Access Control 10.0 and 10.1 workflow extension configuration" on page 16.

Upgrade to support SAP GRC Access Control 5.3

To upgrade the adapter to support SAP GRC Access Control 5.3, you must do several tasks.

Follow these steps:

Profile import

Obtain the `SapGRCNWProfile.jar` profile from the installation package and import the profile into IBM Security Verify Identity.

SAP NetWeaver GRC service creation

After the `SapGRCNWProfile.jar` is imported into IBM Security Verify Identity successfully, update the attributes under the **SAP GRC Service Attributes** tab on the service form.

See "Creating an adapter service/target" on page 11 for details on how to create a service and how to define those attributes on the SAP GRC Service Attributes tab.

To support the different versions of SAP GRC AC with the same profile, the * which used to indicate mandatory account attributes has been removed from the account form as these attributes are not necessarily required for SAP GRC Access Control 10.0 support. Refer to Table 5 for a full reference of supported account attributes.

Installing SAP GRC Access Control 5.3 workflow extension

The workflow extension JAR file for SAP GRC Access Control 5.3 is renamed. You must perform two actions, if the SAP GRC Access Control 5.3 notification component is already configured before you install and configure the new component.

Procedure

1. Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to remove all SAP GRC Access Control 5.3 extensions
2. Delete the `SAPGRCWorkflow.jar` file from the appropriate directory where it is installed: *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`
3. Install the new SAP GRC Access Control 5.3 workflow extension.
   a) Edit the `workflowextensions.xml` file under the *ITIM_HOME*`/data` directory to add a workflow extension. See Installing 5.3 workflow extension for details.
   b) Copy `workflow\grc53\SAPGRC53Workflow.jar` file from the installation package to the appropriate directory: *WEBSPHERE_HOME*`\AppServer\profiles\`*SERVER_NAME*`\installedApps\`*NODE_NAME*`\ITIM.ear\app_web.war\WEB-INF\lib`

      If the directory does not exist, create one.

c) Restart the IBM Security Verify Identity application from the WebSphere console, or restart the WebSphere server itself. After a successful restart, continue with configuration.

SAP GRC Access Control 5.3 workflow extension configuration

The SAP GRC Access Control 5.3 workflow extensions support only the Access Request feature by configuring the IBM Security Verify Identity workflow extension.

For more information, see "SAP GRC Access Control 10.0 and 10.1 workflow extension configuration" on page 16.

Installing and configuring SAP GRC Access Control 5.3 notification component

The workflow extension JAR file for SAP GRC Access Control 5.3 is renamed. You must take two actions, if the SAP GRC Access Control 5.3 notification component is already configured before you install and configure the new component.

Procedure

1. Delete the SAPGRCWorkflow.jar file from the appropriate directory where it is installed:
   WEBSPHERE_HOME\AppServer\profiles*SERVER_NAME*\installedApps*NODE_NAME*\ITIM.ear\app_web.war\WEB-INF\lib
2. Delete the runNotifierWAS7 script.

   See "Installing and configuring the notification component for SAP GRC Access Control version 10.0 or 10.1" on page 23.

Chapter 5. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you use the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Error messages and problem solving

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Error messages	Problem descriptions
Workflow Activity Status Failed CTGIMA407E A configured workflow activity expected to receive 1 parameters, but 0 parameters were received for <workflow_name> workflow that was processing the <activity_name> activity.	If no further information is supplied in IBM Security Verify Identity request details, enable the 'Detail Logging' option on the SAP GRC Service Attributes tab then inspect the IBM Security Verify Identity trace.log file for the root cause. Possible reasons include; incorrect SAP GRC Access Control username/password, SAP GRC Access Control user is unauthorized, Access Control Submit Request URL is incorrect, IBM Security Verify Identity workflow is incorrectly configured, or SAP GRC Access Control rejected the request due to invalid data supplied on the request.
GRC Request failed : This is the message received from SAP GRC V10: ' msgNo= , msgType= , msgStatement= . '	Incorrect URL for the relevant SAP GRC Access Control 10.0 and 10.1 web services have been specified so no error message was returned by the SAP GRC Access Control web service call. Revise the SAP GRC Service Attributes Tab on the service form to correct the relevant URL.
Risk Analysis returns ERROR when no risk results are found. GRC Request failed : This is the message received from SAP GRC V10: ' msgNo=4 , msgType=ERROR , msgStatement=Invalid input or no data found for given input data. . '	This message is returned by the SAP GRC Access Control 10.0 and 10.1 risk analysis web service when no risk results are found. It receives no special handling by the IBM Security Verify Identity Adapter for SAP GRC Access Control 10.0 and 10.1. For more information on the problem see SAP Note “1692553 - Risk Analysis web service output is wrong when no risks”.
GRC Request failed. This is the message received from SAP GRC V10: ' msgNo=4 , msgType=ERROR , msgStatement=Invalid Item Name. . '	Indicates invalid configuration of either the SAP GRC Access Control connector (System Identifier) referenced on the IBM Security Verify Identity service form, or one or more of the roles specified on the request have not been imported correctly into IBM Security Verify Identity 10.0 and 10.1.
Activity status terminated.	Inspect IBM Security Verify Identity *trace.log*. Potential cause is IBM Security Verify Identity workflow misconfiguration such as missing relevant data.
Notification Failed SEVERE: File Not Found Exception during Connection: [java.io.FileNotFoundException: SAPNotify.props (The system cannot find the file specified.)]	`SAPNotify.props` file is missing. The `SAPNotify.props` file needs to be existed in the same location where the notifier script is being executed.
Notification Failed SEVERE: File Not Found Exception during Connection: [java.io.FileNotFoundException: \data\enRole.properties (The system cannot find the path specified.)]	Cannot locate the `enRole.properties` file. Define itim.home in the `SAPNotify.props` file. For example `itim.home=C:/Program Files/IBM/itim`

Error messages	Problem descriptions
Notification Failed SEVERE: A value for the property itim.user was not found in SAPNotify.props	The user name to login to the Identity Manager server is missing. Define itim_user in the `SAPNotify.props` file.
Notification Failed SEVERE: A value for the property itim.pswd was not found in SAPNotify.props	The password for the Identity Manager user is missing. Define itim_pswd in the `SAPNotify.props` file
Notification Failed SEVERE: A value for the property GRCUserName was not found in SAPNotify.props	The user name to login to SAP GRC Access Control system is missing. Define GRCUserName in the `SAPNotify.props` file.
Notification Failed SEVERE: A value for the property GRCPassword was not found in SAPNotify.props	The password for the SAP GRC Access Control user is missing. Define GRCPassword in the `SAPNotify.props` file.
Notification Failed SEVERE: A value for the property GRCStatusURL was not found in SAPNotify.props	The SAP GRC Access Control 10 Audit Logs Web Service URL is missing. Define the correct URL for the audit logs web service in the `SAPNotify.props` file. For example: `http://sapgrc10:8000/sap/bc/srt/ rfc/sap/grac_audit_logs_ws/001/grac_audit_logs_ws/binding?sap-client=001`
Notification Failed SEVERE: Exception occurred during request lookup [(500) SRT: Unexpected failure in SOAP processing occurred: ("No Web service configuration for this access path: "/sap/bc/srt/rfc/sap/grac_audit_log_ws/001/grac_aud"")]	Incorrect web service URL has been defined in the `SAPNotify.props` file. Verify the URL for the GRCNotifyURL property.
Notification Failed SEVERE: WSWS3938E: The message is enclos ebServicesFault faultCode: HTTP faultString: (401) Unauthorized faultActor: http://10.150.22.7:8000 faultDetail: null: WSWS3192E: Error: return code: (401) Unauthorized	Incorrect SAP GRC Access Control user password has been defined in the `SAPNotify.props` file. Verify the GRCPassword property.
Notification Failed SEVERE: Login Exception during Connection: [com.ibm.itim.apps.ITIMFailedLoginException: The information used to login is not correct.] com.ibm.itim.apps.ITIMFailedLoginException: The information used to login is not correct.	Incorrect Identity Manager user password has been defined in the `SAPNotify.props` file. Verify the itim.pswd property.
GRC Request failed : This message is received from SAP GRC V10: '`msgNo=4 , msgType=ERROR , msgStatement=Invalid request initiation system..`'	An incorrect value has been supplied for the System Identifier on the GRC Service Attributes. Revise the value and correct the System Identifier to match the name of the relevant SAP connector in GRC 10.0 and 10.1.

Error messages	Problem descriptions
GRC Request failed : `msgNo= , msgType= , msgStatement=Primary email address on the Communications tab is not in the correct format.`	The email address on the Communications tab needs to be input using a particular syntax. For more information about this format consult the “Special Attributes” section in the *SAP NetWeaver Adapter Installation and Configuration Guide*. The GRC 10.0 and 10.1 integration inserts the standard email address into the user information **email address** field as required by the GRAC_USER_ACCES_WS web service.

Chapter 6. Uninstalling

To uninstall the integration, you must remove the SAP GRC Access Control workflow extensions from IBM Security Verify Identity.

Procedure

1. Log on to IBM Security Verify Identity, navigate to **Configure System** > **Manage Operations**. Remove the SAP GRC Access Control workflow extension configuration for the add, delete, modify, restore, and suspend operations for the SAP GRC NetWeaver Account type.
2. Delete SAPGRC53Workflow.jar or SAPGRC10Workflow.jar from the following directory *WEBSPHERE_HOME*\AppServer\profiles*SERVER_NAME*\installedApps*NODE_NAME*\ITIM.ear\app_web.war\WEB-INF\lib
3. Remove the following SAP GRC Access Control workflow activity from the *ITIM_HOME*\data\workflowextensions.xml file.
   - If using SAP GRC Access Control 5.3:

     ```
     SAPGRCNonblockingAddRequest
     SAPGRCBlockingAddRequest
     SAPGRCNonblockingModifyRequest
     SAPGRCBlockingModifyRequest
     SAPGRCNonblockingDeleteRequest
     SAPGRCBlockingDeleteRequest
     SAPGRCNonblockingSuspendRequest
     SAPGRCBlockingSuspendRequest
     SAPGRCNonblockingRestoreRequest
     SAPGRCBlockingRestoreRequest
     ```

   - If using SAP GRC Access Control 10.0 or 10.1:

     ```
     SAPGRC10NonblockingAddRequest
     SAPGRC10BlockingAddRequest
     SAPGRC10NonblockingModifyRequest
     SAPGRC10BlockingModifyRequest
     SAPGRC10NonblockingDeleteRequest
     SAPGRC10BlockingDeleteRequest
     SAPGRC10NonblockingSuspendRequest
     SAPGRC10BlockingSuspendRequest
     SAPGRC10NonblockingRestoreRequest
     SAPGRC10BlockingRestoreRequest
     SAPGRC10RiskAnalysisRequest
     SAPGRC10UpdateAccountAttributesExtension
     checkGRCVersion
     ```

4. Restart WebSphere Application Server.
5. To remove the SAP GRC Access Control workflow notification component:
   a) Log on to IBM Security Verify Identity server.
   b) Remove the following notification configuration files from *ITIM_HOME*\bin or the directory where it was installed.
      - jaas_login_was.conf
      - runNotifierWAS7.bat or runNotifierWAS7.sh
      - SAPNotify.props

Chapter 7. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes and object classes

After the GRC profile is installed, the integration supports a standard set of attributes from the NetWeaver adapter in addition to attributes required for SAP GRC Access Control.

The following table lists the standard attributes supported for SAP GRC Access Control, in addition to the SAP NetWeaver attributes that are listed in the *Adapter for SAP NetWeaver Installation and Configuration Guide*.

The following table shows the SAP GRC Access Control attributes used by requests sent to the SAP GRC Access Control 5.3, 10.0 and 10.1. The set of attributes between SAP GRC Access Control versions is different as indicated in Table 3.

The list of SAP GRC Access Control service form attributes can be found in Table 4 on page 41.

Table 4. Supported SAP GRC AC service attributes

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for SAP GRC Access Control 5.3 Request	Required for SAP GRC Access Control 10.0 and 10.1 Request
Enable GRC Workflow Extensions	ersapgrcenabled	Optional attribute. Indicates whether SAP GRC Access Control workflow extensions have been configured	String	Yes	Yes

Table 4. Supported SAP GRC AC service attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for SAP GRC Access Control 5.3 Request	Required for SAP GRC Access Control 10.0 and 10.1 Request
GRC Version	ersapgrcversion	Optional attribute. The version of SAP GRC Access Control the service has been configured against. Used when there is a combination of different version of SAP GRC Access Control needs to be supported in the a single server instance.	String	Yes	Yes
GRC Admin Id	ersapgrcsubmitrequestuid	User ID of the SAP GRC Access Control Administrator	String	Yes	Yes
GRC Password	ersapgrcabappwd	Password of the SAP GRC Access Control Administrator	String	Yes	Yes
System Identifier	ersapgrcsystemid	System identifier	String	Yes	Yes
Access Control Request URL	ersapgrcsubmitrequesturl	The URL address of the Access Control Submit Request Web service	String	Yes	Yes
Access Control Look Up URL	ersapgrclookupurl	The URL address of the Access Control Look Up Request web service	String	No	Yes
Access Control Risk Analysis URL	ersapgrcriskanalysisurl	The URL address of the Access Control Risk Analysis Request web service	String	No	Yes, If using Risk Analysis workflow extension

Table 4. Supported SAP GRC AC service attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for SAP GRC Access Control 5.3 Request	Required for SAP GRC Access Control 10.0 and 10.1 Request
Access Control Request Detail URL	ersapgrcrequestdetailsurl	The URL address of the Request Detail web service	String	No	Yes, If using Update Account Attribute workflow extension
Detail Logging	ersapgrcdebug	Flag to enable GRC request debugging trace output	String	No	No

Note: A GRC request contains values of several attributes that are supplied from the SAP NetWeaver account form tabs such as Given name, Surname, Email address, and Role. The list of SAP GRC and NetWeaver account form attribute values that are forwarded onto a GRC request is found in Table 5 on page 43.

Table 5. Supported SAP GRC/NetWeaver account attributes

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 and 10.1 Request
Priority	ersapgrcpriority	Request Priority. The value must match the identifier of a configured AC priority.	String	Yes	Yes
Location	ersapgrclocation	The work location of the user to be provisioned.	String	No	No
Employee Type	ersapgrcemployeetype	Type of employee. This attribute value must match configuration in AC.	String	No	No

Table 5. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 and 10.1 Request
Requestor ID	ersapgrcrequesteruid	User name of the requester.	String	Yes	If Requestor ID is not defined, SAP GRC Access Control 10.0 and 10.1 will default it to the SAP GRC Access Control Admin ID defined on the service form as the requestor.
Requestor First Name	ersapgrcrequesterfirstname	Given name of the requester.	String	Yes	No
Requestor Last Name	ersapgrcrequesterlastname	Surname of the requester.	String	Yes	No
Requestor Email	ersapgrcrequesteremail	The email address of the requester.	String	Yes	Yes
Requestor Telephone	ersapgrcrequestertelephone	Telephone number of the requester.	String	No	No
Manager ID	ersapgrcmanageruid	User name of the employees manager. This attribute value must match the user ID of a user in the AC authentication data source.	String	Yes	If Manager is configured as one of the approver in GRC 10.0 and 10.1, this attribute is required.

Table 5. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 and 10.1 Request
Manager First Name	ersapgrcmanagerfirstname	Given name of the employees manager.	String	No	No
Manager Last Name	ersapgrcmanagerlastname	Surname of the employees manager.	String	No	No
Manager Email	ersapgrcmanageremail	Email address of the employees manager.	String	No	No
Manager Telephone	ersapgrcmanagertelephone	Telephone number of the employees manager.	String	No	No
Locale	ersapgrclocale	Locale of the employee. For example, EN, DE, US.	String	No	No
Request Reason	ersapgrcrequestreason	The reason for the AC request.	String	Yes	Yes
Organization Unit	ersapgrcorgunit	Organization Unit	String	No	No
Business Process	ersapgrcbusprocess	Business Process. This attribute value must match the configuration in AC.	String	Yes	Yes
Functional Area	ersapgrcfunctionalarea	Functional Area	String	No	No
Personnel Area	ersapgrcpersonnelarea	Personnel Area	String	No	No
Employee Job	ersapgrcemployeejob	Job of Employee	String	No	No
Employee Position	ersapgrcemployeeposition	Position of Employee	String	No	No
Request Due Date	ersapgrcrequestduedate	Due Date of the request	Date	No	No
Request Item Comments	ersapgrcreqitemcomment	Comments on the request item	String	No	No

Table 5. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 and 10.1 Request
Custom Fields	ersapgrccustomfields	Custom fields that are configured in AC. This attribute is a multi-valued attribute that must be supplied in the format: `"<custom field name>|<custom field value>"` It must match a configured custom field in AC.	Key/Value Pair String	No	No
Given Name	ersapnwgivenname	Given name of the user.	String	Yes	Yes
Surname	ersapnwsurname	Surname of the user.	String	Yes	Yes
Email Address	ersapnwemailaddress	The value of the "primary email address" given in the Communication tab. For more information about the format for providing email addresses, see the email section under Special Attributes.	String	Yes	Yes

Table 5. Supported SAP GRC/NetWeaver account attributes (continued)

IBM Security Verify Identity Name	Attribute Name	Description	Data Type	Required for GRC 5.3 Request	Required for GRC 10.0 and 10.1 Request
Company	ersapnwcompany	Represents the identifier of a company configured in AC. The value must match a “Company ID” configured in AC role attributes. This value is set as the value for company in both the AC request and all requested roles for the request.	String	No	No
Department	ersapnwdepartment	Represents the department of the user to be provisioned.	String	No	No
Function	ersapnwfunction	Represents the department of the user to be provisioned. The value must match a “Functional Area” configured in AC role attributes.	String	No	No

Table 5. Supported SAP GRC/NetWeaver account attributes (continued)					
IBM Security Verify Identity Name	**Attribute Name**	**Description**	**Data Type**	**Required for GRC 5.3 Request**	**Required for GRC 10.0 and 10.1 Request**
Role	ersapnwagrname	Multi-valued attribute that contains the proposed group of roles to be provisioned for the account. The request uses the values supplied for system ID, company, role name, start date, and end date in the role data. CUA client names are not used as the system ID in the role data.	Custom Data Type	Yes	Yes
CUA Systems	ersapnwcuasystem	Connector name for CUA clients.	String	No	Yes

There are constraints imposed by SAP GRC AC for a successful request submission, such as attribute values that match pre-configured values in SAP GRC AC. The attributes that have values that must match values in SAP GRC AC are listed in Table 6 on page 48.

Table 6. Attributes with required data in SAP GRC AC 10.0 and 10.1	
Attribute Name	**Details**
Role	All roles that exist on an SAP GRC AC request are inspected. Therefore all roles that exist in the target SAP NetWeaver system must also exist in SAP GRC AC 10.0 and 10.1.
CUA Systems	The value must match the connector name of a configured SAP Client.
Priority	The value must match the identifier of a configured AC priority. If the priority codes in SAP GRC AC are different from the supported defaults `006=HIGH, 007=LOW, 008=MEDIUM` then the **`ersapgrcpriority`** form element on the account form must be edited to match the configured priorities. To customize the adapter profile, see the *IBM Security Verify Identity SAP NetWeaver Adapter Installation and Configuration Guide*.
Employee Type	This attribute value must match configuration in AC.
System Identifier	The attribute value must match the name of a connector that is configured in SAP GRC AC 10.0 and 10.1.
Manager ID	This attribute value must match the user ID of a user in the AC authentication data source.
Function	The value must match a "Functional Area" configured in AC.

Table 6. Attributes with required data in SAP GRC AC 10.0 and 10.1 (continued)	
Attribute Name	**Details**
Business Process	This attribute value must match the business process configuration in AC.

Index

S

T

U

V

W