IBM Tivoli Composite Application Manager Agent for SAP Applications
Version 7.1.1.2

Installation and Configuration Guide

SC27-5672-02

IBM Tivoli Composite Application Manager Agent for SAP Applications
Version 7.1.1.2

Installation and Configuration Guide

SC27-5672-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 51.

This edition applies to version 7.1.1 Fix Pack 2 of IBM Tivoli Composite Application Manager Agent for SAP Applications (product number 5725-I45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview of the SAP agent

The IBM® Tivoli® Composite Application Manager Agent for SAP Applications provides you with the capability to monitor your SAP system. You can also use the agent to take basic actions with the SAP system. IBM Tivoli Monitoring is the base software for the SAP agent. The SAP agent offers a central point of management for gathering the information you need to detect problems early, and to take steps to prevent them from recurring. It enables effective systems management across SAP releases, applications, and components; and the underlying databases, operating systems, and external interfaces.

IBM Tivoli Monitoring overview

IBM Tivoli Monitoring helps you to monitor the availability and performance of all the systems in your enterprise from one or several designated workstations. It also provides useful historical data that you can use to track trends and to troubleshoot system problems.

You can use IBM Tivoli Monitoring to achieve the following tasks:

- Monitor for alerts on the systems that you are managing by using predefined situations or custom situations.
- Establish your own performance thresholds.
- Trace the causes leading to an alert.
- Gather comprehensive data about system conditions.
- Use policies to take actions, schedule work, and automate manual tasks.

The Tivoli Enterprise Portal is the interface for IBM Tivoli Monitoring products. You can use the consolidated view of your environment as seen in the Tivoli Enterprise Portal to monitor and resolve performance issues throughout the enterprise.

See the publications listed in “Prerequisite publications” on page 49 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

Features of the monitoring agent

By using this agent, you can enable effective systems management across SAP releases, applications, and components; and the underlying databases, operating systems, and external interfaces. You can easily collect and analyze the following components and procedures to learn about your SAP enterprise:

- Operating system and the associated local area network (LAN)
- Databases that are used by SAP, for example, Oracle and DB2®.
- SAP memory and buffer performance
- Layout and configuration of SAP system components
- Layout and configuration of SAP application instances and databases
- Batch processing, including batch data create sessions
- Monitoring the imported transport history
- Performance monitoring reported by SAP service, transaction, user, application, subapplication, or program
- IBM Tivoli Monitoring generated alerts from our best practice monitoring situations and SAP CCMS alerts from the systems that are running SAP solutions
- Transport system activity that might affect the integrity of your development, test, and production systems
- Monitoring the system by using syslog and ABAP memory dumps

- Monitoring inbound and outbound queues for RFC calls in SAP
- Monitoring services that are defined in SAP and the message server
- Monitoring SAP instances that are selected by the user
- Solution Manager monitoring that includes information about the following alerts:
  - Early Watch
  - System Monitoring
  - Historical
  - Business Process Monitoring

  Note: Business Process monitoring alerts are generated in the satellite systems that are connected to Solution Manager.
- Monitoring the system landscape (server and database) as defined in Solution Manager
- PI/XI monitoring that includes the following information:
  - XML messages, business process engine, synchronous/asynchronous communication in PI/XI
  - Job overview and details, workflow details

New in this release

For version 7.1.1 Fix Pack 2 of the SAP agent, the following enhancements were made since version 7.1.1.1:

- The SAP agent version 7.1.1 Fix Pack 2 uses the NetWeaver RFC SDK V7.20 library that results in better performance and faster data collection.
- Changes related to system requirements. See the information about system requirements in Software product compatibility reports website (http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html)
- Added new MAI Alert fetching mechanism that is based on fetching MAI Alerts without configuring email notification settings and without BAdi implementation.
- New attribute groups:
  - ABAP Dump Count
  - License Information
  - Output Requests Status Count
- Modified attribute groups:
  - ICM Monitor
  - ICM Monitor Services
- New workspace:
  - License Information workspace
- Modified workspaces:
  - ABAP Dumps workspace
  - Output Requests workspace
  - ICM Monitor workspace
  - ICM Monitor Service workspace
- New views:
  - Output Requests Status Count
  - ABAP Dumps Count
- New situations:
  - R3_License_Expiry_Crit
  - R3_License_Expiry_Warn

Components of the IBM Tivoli Monitoring environment

After you install and set up the SAP agent, you have an environment that contains the client, server, and monitoring agent implementation for IBM Tivoli Monitoring.

This IBM Tivoli Monitoring environment contains the following components:

Tivoli Enterprise Portal client
The portal has a user interface based on Java™ for viewing and monitoring your enterprise.

Tivoli Enterprise Portal Server
The portal server is placed between the client and the Tivoli Enterprise Monitoring Server and enables retrieval, manipulation, and analysis of data from the monitoring agents. The Tivoli Enterprise Portal Server is the central repository for all user data.

Tivoli Enterprise Monitoring Server
The monitoring server acts as a collection and control point for alerts received from the monitoring agents, and collects their performance and availability data. TheTivoli Enterprise Monitoring Server is also a repository for historical data.

Tivoli Enterprise Monitoring Agent: SAP agent (one or more instances of the monitoring agent).
The agent instances communicate with the systems or subsystems that you want to monitor. This monitoring agent collects and distributes data to a Tivoli Enterprise Portal Server.

Tivoli Enterprise Monitoring Agent: SAP agent, installed on a remote system
This monitoring agent collects and distributes data to a Tivoli Enterprise Portal Server.

IBM Tivoli Enterprise Console
The Tivoli Enterprise Console® is an optional component that acts as a central collection point for events from various sources, including events from other Tivoli software applications, Tivoli partner applications, custom applications, network management platforms, and relational database systems. You can view these events through the Tivoli Enterprise Portal (by using the event viewer), and you can forward events from IBM Tivoli Monitoring situations to the Tivoli Enterprise Console component.

IBM Tivoli Netcool/OMNIbus
Tivoli Netcool/OMNIbus is an optional component and an alternative to the Tivoli Enterprise Console. The Netcool/OMNIbus software is a service level management (SLM) system that delivers real-time, centralized monitoring of complex networks and IT domains. The Tivoli Netcool/OMNIbus components work together to collect and manage network event information.

IBM Tivoli Common Reporting
Tivoli Common Reporting is a separately installable feature available to users of Tivoli software that provides a consistent approach to generating and customizing reports. Some individual products provide reports that are designed for use with Tivoli Common Reporting and have a consistent look and feel.

IBM Tivoli Application Dependency Discovery Manager (TADDM)
TADDM delivers automated discovery and configuration tracking capabilities to build application maps that provide real-time visibility into application complexity.

IBM Tivoli Business Service Manager
The Tivoli Business Service Manager component delivers real-time information to help you respond to alerts effectively based on business requirements. Optionally, you can use this component to meet service-level agreements (SLAs). Use the Tivoli Business Service Manager tools to help build a service model that you can integrate with IBM Tivoli Netcool/OMNIbus alerts or optionally integrate with data from an SQL data source. Optional components provide access to data from other IBM Tivoli applications such as IBM Tivoli Monitoring and IBM Tivoli Application Dependency Discovery Manager.

Agent Management Services

You can use IBM Tivoli Monitoring Agent Management Services to manage the SAP agent.

Agent Management Services is available for the following IBM Tivoli Monitoring OS agents: Windows, Linux, and UNIX. The services are designed to keep the SAP agent available, and to provide information about the status of the product to the Tivoli Enterprise Portal. For more information about Agent management Services, see "Agent Management Services" in the *IBM Tivoli Monitoring Administrator's Guide*.

User interface options

Installation of the base software and other integrated applications provides the following interfaces that you can use to work with your resources and data:

Tivoli Enterprise Portal browser client interface
The browser interface is automatically installed with Tivoli Enterprise Portal. To start Tivoli Enterprise Portal in your Internet browser, enter the URL for a specific Tivoli Enterprise Portal browser client installed on your Web server.

Tivoli Enterprise Portal desktop client interface
The desktop interface is a Java-based graphical user interface (GUI) on a Windows or Linux workstation.

IBM Tivoli Enterprise Console
Event synchronization component for synchronizing the status of situation events that are forwarded to the event server. When the status of an event is updated because of IBM Tivoli Enterprise Console® rules or operator actions, the update is sent to the monitoring server, and the updated status is reflected in both the Situation Event Console and the Tivoli Enterprise Console event viewer.

Manage Tivoli Enterprise Monitoring Services window
The window for the Manage Tivoli Monitoring Services utility is used for configuring the agent and starting Tivoli services that are not already designated to start automatically.

IBM Tivoli Monitoring command line
IBM Tivoli Monitoring commands are run from the command line. These commands are primarily used in the UNIX environment. They can be used for installing, configuring, starting, and stopping the agent.

IBM Tivoli Application Dependency Discovery Manager
The Discovery Management Console is the IBM Tivoli Application Dependency Discovery Manager client user interface for managing discoveries.

Tivoli Business Service Manager
The Tivoli Business Service Manager console provides a graphical user interface (GUI) that you can use to logically link services and business requirements within the service model. The service model provides an operator with a second-by-second view of how an enterprise is performing at any specific moment in time or how the enterprise performed over a specific time period.

Chapter 2. Agent installation and configuration

Agent installation and configuration requires the use of the IBM Tivoli Monitoring Installation and Setup Guide and agent-specific installation and configuration information.

To install and configure the SAP agent, use the "Installing monitoring agents" procedures in the *IBM Tivoli Monitoring Installation and Setup Guide* with the agent-specific installation and configuration information.

If you are installing silently by using a response file, see "Performing a silent installation of IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

With the self-describing agent capability, new or updated IBM Tivoli Monitoring agents that use IBM Tivoli Monitoring V6.2.3 or later can become operational after installation without completing additional product support installation steps. To take advantage of this capability, see "Enabling self-describing agent capability at the hub monitoring server" in the *IBM Tivoli Monitoring Installation and Setup Guide*. Also, see "Self-describing monitoring agents" in the *IBM Tivoli Monitoring Administrator's Guide*.

Requirements

Before installing and configuring the agent, make sure your environment meets the requirements for the IBM Tivoli Composite Application Manager Agent for SAP Applications.

For the most current information about system requirements, see the Software product compatibility reports website (http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html). Search for the ITCAM for Applications product.

Prerequisites checking

The prerequisite checker utility verifies whether all the prerequisites that are required for the agent installation are met. The prerequisite checker creates a log file that contains a report of all the prerequisites checks when the prerequisite checker was run.

For the SAP agent, the prerequisite checker verifies the following requirements:

- Memory
- Disk
- Operating systems

For detailed information about installation prerequisites, see the Software product compatibility reports website (http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html).

You can run the prerequisite checker in stand-alone mode or remotely. For more information about the prerequisite checker, see "Prerequisite Checking for IBM Tivoli Monitoring Agents" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Verifying the prerequisites for data collection

Verify the following prerequisites for data collection:

- "Oracle historical statistics information" on page 6
- "Oracle data collection" on page 6
- "OS Collector" on page 6

- "Setting the SAP system time zone"

Oracle historical statistics information

The COLLECTOR_FOR_PERFORMANCE batch job provides information on Oracle historical statistics.

The SAP agent relies on the COLLECTOR_FOR_PERFORMANCE batch job to report Oracle historical statistics. Use transaction SM37 to verify that the COLLECTOR_FOR_PERFORMANCE batch job is set up as described in the mySAP installation documentation and SAP Note 16083. The actual job name might be different on your system.

Oracle data collection

Data collection problems might occur when the SAP program, RSDB_TDB, which collects the Oracle statistics, does not work correctly. Too many data rows are stored in MONI. Collection might stop or run sluggishly on busy systems. See SAP Notes: 591801, 713211.

To correct this problem, perform the following steps:

1. Have your SAP Administrator implement these SAP notes.
2. Run the specified program, RSORAUD0, with the recommended cleanup options.
3. Update the Oracle statistics manually through transaction DB02.

After implementing these steps, the number of rows being returned to the agent is correct, the volume of data in MONI does not increase, and agent data collection periods are normal.

OS Collector

The SAP agent relies on the saposcol program provided by SAP to collect operating system and file system metrics. Have your SAP Administrator enable this service on all computers hosting SAP application servers.

Setting the SAP system time zone

The SAP agent depends on SAP statistics collection working correctly on the SAP systems that it monitors. On SAP 7.0 systems, you must set the SAP system time zone to match the time zone for the operating system so that SAP statistics are collected with the correct time stamps. You must make this change for the SAP agent to successfully collect data. See SAP Note 926290 for more information about this issue.

Language pack installation

The steps for installing language packs depend on which operating system and mode of installation you are using.

To install a language pack for the agent support files on the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Monitoring Agent, and the Tivoli Enterprise Portal Server, make sure that you installed the product in the English language. Then use the steps for the operating system or mode of installation you are using:

- "Installing language packs on AIX or UNIX systems"
- "Installing language packs on Windows systems" on page 7
- "Installing language packs on Windows, UNIX, or Linux systems silently" on page 8

Installing language packs on AIX or UNIX systems

You can install the language packs on an AIX® or UNIX system.

Before you begin

First, make sure that you installed the product in the English language.

Procedure

1. Enter the following command to create a temporary directory on the computer: `mkdir dir_name`. Make sure that the full path of the directory does not contain any spaces.
2. Mount the language pack CD to the temporary directory that you created.
3. Enter the following command to start the installation program: `cd dir_name lpinstaller.sh -c install_dir` where *install_dir* is where you installed IBM Tivoli Monitoring. Typically, the directory name is `/opt/IBM/ITM` for AIX and UNIX systems.
4. Select the language of the installer and click **OK**.
5. In the Introduction panel, click **Next**.
6. Click **Add/Update** and click **Next**.
7. Select the folder where the National Language Support package (`NLSPackage`) files are located. Typically, the `NLSPackage` files are located in the `nlspackage` folder where the installer executable file is located.
8. Select the language support for the agent of your choice and click **Next**. To make multiple selections, press Ctrl and select the language that you want.
9. Select the languages that you want to install and click **Next**.
10. Examine the installation summary page and click **Next** to begin installation.
11. After installation completes, click **Finish** to exit the installer.
12. Restart the Tivoli Enterprise Portal Tivoli Enterprise Portal Server, and Eclipse Help Server if any of these components are installed.

Installing language packs on Windows systems

You can install the language packs on a Windows system.

Before you begin

First, make sure that you installed the product in the English language.

Procedure

1. On the language pack CD, double-click the `lpinstaller.bat` file to start the installation program.
2. Select the language of the installer and click **OK**.
3. In the Introduction panel, click **Next**
4. Click **Add/Update** and click **Next**.
5. Select the folder where the National Language Support package (`NLSPackage`) files are located. Typically, the NLSPackage files are located in the `nlspackage` folder where the installer executable file is located.
6. Select the language support for the agent of your choice and click **Next**. To make multiple selections, press Ctrl and select the language that you want.
7. Select the languages that you want to install and click **Next**.
8. Examine the installation summary page and click **Next** to begin installation.
9. After installation completes, click **Finish** to exit the installer.
10. Restart the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Eclipse Help Server if any of these components are installed.

Installing language packs on Windows, UNIX, or Linux systems silently

You can use the silent-mode installation method to install the language packs. In silent mode, the installation process obtains the installation settings from a predefined response file. It does not prompt you for any information.

Before you begin

First, make sure that you installed the product in the English language.

Procedure

1. Copy and paste the `ITM_Agent_LP_silent.rsp` response file template as shown in "Response file example."
2. Change the following parameter settings:

   NLS_PACKAGE_FOLDER
   Folder where the National Language Support package (NLSPackage) files are located. Typically, the NLSPackage files are in the `nlspackage` folder, for example, `NLS_PACKAGE_FOLDER = //tmp//LP//nlspackage`.

   PROD_SELECTION_PKG
   Name of the language pack to install. Several product components can be included in one language package. You might want to install only some of the available components in a language pack.

   BASE_AGENT_FOUND_PKG_LIST
   Agent for which you are installing language support. This value is usually the same as *PROD_SELECTION_PKG*.

   LANG_SELECTION_LIST
   Language you want to install.
3. Enter the command to install the language pack with a response file (silent installation):
   - For Windows systems:
     `lpinstaller.bat -f path_to_response_file`
   - For UNIX or Linux systems:
     `lpinstaller.sh -c candle_home -f path_to_response_file`

     where *candle_home* is the IBM Tivoli Monitoring base directory.

Response file example

```
#     IBM Tivoli Monitoring Agent Language Pack Silent Installation Operation
#
#This is a sample response file for silent installation mode for the IBM Tivoli
#Monitoring Common Language Pack Installer.
#.
#This file uses the IBM Tivoli Monitoring Common Agent Language Pack with the
#install package as an example.
#Note:
#This response file is for the INSTALLATION of language packs only.
#This file does not support UNINSTALLATION of language packs in silent mode.
#-------------------------------------------------------------------------------
#-------------------------------------------------------------------------------
#To successfully complete a silent installation of the the example of Common Agent
#localization pack, complete the following steps:
#
#1.Copy ITM_Agent_LP_silent.rsp to the directory where lpinstaller.bat or
#lpinstaller.sh is located (IBM Tivoli Monitoring Agent Language Pack build
#location).
#
#2.Modify the response file so that it is customized correctly and completely for
```

```
#your site.
#  Complete all steps listed in the response file.
#
#3.After customizing the response file, invoke the silent installation using the
#following command:
#For Windows:
#    lpinstaller.bat -f <path_to_response_file>
#For UNIX and Linux:
#    lpinstaller.sh -c <candle_home> -f <path_to_response_file>
#Note:<candle_home> is the IBM Tivoli Monitoring base directory.
#-------------------------------------------------------------------------------
#-------------------------------------------------------------------------------
#Force silent install mode.
#-------------------------------------------------------------------------------
INSTALLER_UI=silent
#-------------------------------------------------------------------------------
#Run add and update actions.
#-------------------------------------------------------------------------------
CHOSEN_INSTALL_SET=ADDUPD_SET
#-------------------------------------------------------------------------------
#NLS Package Folder, where the NLS Packages exist.
#For Windows:
#   Use the backslash-backslash(\\) as a file separator (for example,
#C:\\zosgmv\\LCD7-3583-01\\nlspackage).
#For UNIX and Linux:
#   Use the slash-slash (//) as a file separator (for example,
#//installtivoli//lpsilenttest//nlspackage).
#-------------------------------------------------------------------------------
#NLS_PACKAGE_FOLDER=C:\\zosgmv\\LCD7-3583-01\\nlspackage
NLS_PACKAGE_FOLDER=//tmp//LP//nlspackage
#-------------------------------------------------------------------------------
#List the packages to process; both variables are required.
#Each variable requires that full paths are specified.
#Separate multiple entries with a semicolon (;).
#For Windows:
#           Use the backslash-backslash(\\) as a file separator.
#For Unix and Linux:
#           Use the slash-slash (//) as a file separator.
#-------------------------------------------------------------------------------
#PROD_SELECTION_PKG=C:\\zosgmv\\LCD7-3583-01\\nlspackage\\KIP_NLS.nlspkg
#BASE_AGENT_FOUND_PKG_LIST=C:\\zosgmv\\LCD7-3583-01\\nlspackage\\KIP_NLS.nlspkg
PROD_SELECTION_PKG=//tmp//LP//nlspackage//kex_nls.nlspkg;//tmp//LP//nlspackage//
koq_nls.nlspkg
BASE_AGENT_FOUND_PKG_LIST=//tmp//LP//nlspackage//kex_nls.nlspkg;//
tmp//LP//nlspackage//koq_nls.nlspkg
#-------------------------------------------------------------------------------
#List the languages to process.
#Separate multiple entries with semicolons.
#-------------------------------------------------------------------------------
LANG_SELECTION_LIST=pt_BR;fr;de;it;ja;ko;zh_CN;es;zh_TW
```

Image extraction tool

The Image extraction tool extracts only the required files from an installation image and then creates a separate image for you. It extracts images that are specific to platforms and operating systems.

Use the **tacmd exportBundles** command to export one or more silent installation deployment bundles to the specified export directory for use with software distribution products. You must run the **exportBundles** command locally on a server and specify a populated agent depot or agent installation image as input.

Note: A bundle is the combination of an agent silent installation image and any necessary prerequisites and configuration information required to silently install an agent on a remote system. An agent depot is a directory on the monitoring server from which you deploy agents and maintenance packages to remote systems across your environment.

If the current OS user has the correct permissions, it is not necessary to run the **login** command before you run the **exportBundles** command.

Extracting an image

You complete specific steps to extract an image by using the Image extraction tool.

Before you begin

For a description of the Image extraction tool, see "Image extraction tool" on page 9.

Procedure

1. Extract the `.gz` file and extract the `.tar` file from the SAP Agent version 7.1.1 Fix Pack 2 installer.
2. Open the `CANDLE_HOME` folder and run the following command:
   - **C:\IBM\ITM\BIN> tacmd exportBundles -o LOCAL -t sa -e c:\temp1 -i c:\set_up\unix -p li6263**

     An image is created on the LINUX li6263 platform only.
   - **C:\IBM\ITM\BIN> tacmd exportBundles -i c:\set_up\unix -e c:\temp -o LOCAL -t sa -os LINUX**

     An image is created on the LINUX operating system. This command is available on all LINUX platforms.
   - **C:\IBM\ITM\BIN> tacmd exportBundles -i c:\set_up\unix -e c:\temp -o LOCAL -t sa -os HP**

     An image is created on Hewlett Packard operating systems and platforms.
   - **C:\IBM\ITM\BIN> tacmd exportBundles -i c:\set_up\WINDOWS\Deploy -e c:\temp -o LOCAL -t sa -os WINDOWS**

     An image is created for Windows operating systems. This command is available on all Windows platforms.

     Note: The following options are available:
     - **o** – Output Format {LOCAL/SPD/SPB}
     - **-t** – Product code
     - **-e** – Extraction Folder
     - **-I** – Image Path
     - **-p** – Platform
     - **-os** – Operating System.
3. Copy the platform-specific image folder to the test system and run it through a silent installation.

Installation and configuration of the SAP agent

Agent-specific information includes the following procedures:

Basic Installation:

- "Importing the Advanced Business Application Programming (ABAP) transport on the SAP system" on page 11
- "Prerequisite verification" on page 13
- "Using SAP transport and defining the user" on page 13

- "Local installation" on page 15
- "Remote installation" on page 16

Configuration:
- "Configuring the SAP agent locally" on page 19
- "Configuring the SAP agent remotely" on page 22
- "Product upgrade configuration" on page 25

Remember: You install and configure only one SAP agent for each mySAP system, not one agent per application server.

Important: In case of distributed SAP systems, it is mandatory to configure the SAP agent to host where the message server or ABAP SAP Central Services (ASCS) is configured for both the modes (Logon Group mode and Application Server mode).

Be sure to plan your monitoring. For example, determine which situations to use and which CCMS trees to monitor. Obtain information about requirements from your SAP Administrator. The SAP agent is a powerful tool that, when configured correctly, can effectively monitor your SAP environment. The key is careful planning. Your monitoring team and SAP Administrators must carefully plan the areas to monitor. You must also periodically review and update your plan as circumstances warrant. Follow these guidelines when you are developing a monitoring plan:
- Select the key SAP applications, transactions, programs, and processes that you want to monitor.
- Select specific attributes that represent the most critical aspects of your environment.
- Document thresholds and cycle times for each monitoring attribute.
- Use historical data collection to trend and predict potential issues.
- Prioritize areas that you want to monitor. Too much data can cloud analysis and hinder preventive diagnosis.
- Review implementation, integration, and business process documentation.
- Review past problem areas, outages, and performance degradations.
- Consider the entire enterprise and all of the applications, components, services, computers, and infrastructure that enable the critical business operations.
- Gather input from as many people as possible. Ensure that the plan addresses the business requirements.

Importing the Advanced Business Application Programming (ABAP) transport on the SAP system

You can install one SAP agent for each SAP system.

Procedure

1. Verify the prerequisites for import.
2. Install the SAP transport and define the user with which the agent connects to the SAP system.
3. Verify the prerequisites for data collection.

MAI Alert related prerequisites for importing the ABAP transport

You must verify the MAI Alert related prerequisites before you import the ABAP transport.

Configuration settings in the `transport.prop` file

When you use the new MAI Alert fetching mechanism that includes fetching MAI Alerts without configuring email notification settings and without BAdi implementation, then you must modify the following configuration setting in the `transport.prop` file.

Add the SPLEVEL=X line, where X is the support pack (SP) level of the Solution Manager system.

For example, if the System ID is S10 and the support pack level is 13, then add SPLEVEL=13.

Important: For the SAP system with SP level 10, or later, the value of the Technical Name (MEA) attribute is not populated on the Tivoli Enterprise Portal when the MAI Alerts are fetched without configuring email notification in the SAP Solution Manager and without BAdi implementation. The value of the Technical Name (MEA) attribute is populated on the Tivoli Enterprise Portal when the MAI Alerts are fetched by configuring email notification in the SAP Solution Manager and BAdi implementation.

Determination of old and new mechanism for fetching MAI Alerts based on the Solution Manager Support Pack (SP) Level

Old MAI Alert fetching mechanism
This mechanism is based on configuring email notification settings and the /IBMMON/ITM_IMPL_ALRTINBX BAdi implementation with the IF_ALERT_DYN_COFIGURATION interface to collect MAI Alerts and send them to the SAP Agent.

New MAI Alert fetching mechanism
This mechanism is based on fetching MAI Alerts without configuring email notification settings and without the /IBMMON/ITM_IMPL_ALRTINBX BAdi implementation with the IF_ALERT_DYN_COFIGURATION interface.

You can use the following table to understand the usage of the `transport.prop` file and its dependency on the configuration of email notification settings.

Table 1. Usage of transport.prop file and its dependencies

SAP system SP Level	transport.prop settings		Configuration of email notification settings	MAI Alert mechanism to be used
	MAI_ CONFIGURED	Solution Manager SP level		
Any	No or file does not exist	Not Applicable	Configured or not configured	The SLM subnode does not appear instead the SOL subnode appears.
SP 6 through 9	Yes	Mentioned	Configured	Old mechanism
SP 6 through 9	Yes	Not mentioned	Configured	Old mechanism
SP 6 through 9	Yes	Not mentioned	Not configured	Old mechanism does not work because the configuration of email notification settings is mandatory.
SP 6 through 9	Yes	Mentioned	Not configured	Old mechanism does not work because the configuration of email notification settings is mandatory.
SP 10, or later	Yes	Mentioned	Configured	New mechanism
SP 10, or later	Yes	Mentioned	Not configured	New mechanism
SP 10, or later	Yes	Not mentioned	Configured	Old mechanism
SP 10, or later	Yes	Not mentioned	Not configured	Old mechanism does not work because the configuration of email notification settings is mandatory.

Prerequisite verification

You must verify the prerequisites before you import the transport request.

When you import the ABAP (Advanced Business Application Programming) transport to the SAP system, you must ensure that the DDIC user is set up on the client where you install the SAP transport.

R3trans Version 01.07.04 or later is required for a successful import of the product transport request because of Dynpro and Export and Import table incompatibility. The basic operation of the agent is not affected by the Dynpro or Export and Import incompatibility issues; only the SAP configuration windows are affected.

You can set up the SAP Solution Manager V7.1 or later to monitor with the Monitoring and Alert Infrastructure (MAI) configuration enabled. However, you must ensure that you import the SAP agent V7.1.1 transport on the client where the Monitoring and Alert Infrastructure (MAI) configuration is available. To view the features that is displayed in the PI subnode, you must ensure that you import the SAP agent V7.1.1 transport on the client where the PI configuration is available.

To view the data in the workspaces under SLM subnode, you must complete the MAI configurations for PI and Solution Manager. You must also configure business process monitoring so that you can view data in the Business Process Monitoring workspace. To view the data for MAI Alert Inbox workspace, make the following configurations:

- In Solution Manager 7.1, under the System Monitoring, activate the third-party component, and add **Implementation: BADI Definition for Alert Reactions** and third part connector.
- Set the scope filter to **All Alerts and Metrics**.
- Ensure that Implementation state is **Active**.

For more information, see the following Online Service System (OSS) Notes, including a list of required SAP service pack levels:

- OSS Note 454321
- OSS Note 330267
- OSS Note 743155

Using SAP transport and defining the user

The SAP agent provides a set of ABAP (Advanced Business Application Programming) routines to support data collection in the SAP system. This ABAP code is delivered as a SAP transport that must be installed on each SAP system that is to be monitored. Your SAP Administrator installs the transport.

About this task

The authorization profile **ZITM_610AUTH** and authorization role **ZITM_610AUT** are valid until the 6.1 release only. From release 6.2 onwards, the **/IBMMON/AUTH** authorization profile is used.

Note: To protect against unauthorized use, the ABAP code that is installed in the SAP system is not visible from within the SAP system. In addition, this code cannot be modified or generated. Support for this code must be obtained through IBM Software Support.

In addition to installing ABAP code, the transport also installs translated language text elements to provide NLS support for SAP transport text elements.

Important: If you need to import the transport on the SAP system, you must not start the SAP agent instance that is configured to monitor the SAP system. Also, before you delete the transport from the SAP system, you must stop the SAP agent instance that is configured to monitor the SAP system.

Use this procedure to install the SAP transport into the SAP system.

Procedure

1. Go to the /ABAP directory on the product CD.
2. To install the single ITM file, select one of the following file import options:
   - If the SAP system, where you want to install the single IBM Tivoli Monitoring file, is a Solution Manager 7.1 Service Pack 6 level and has MAI configured, you must create the file-transport.prop file in the user/sap/SID SAP work directory, and add MAI_CONFIGURED = YES entry in that file. This entry creates a MAI_CONFIGURED = YES entry in the /IBMMON/ITM_CNFG database.

     Note: Before you import the single IBM Tivoli Monitoring transport file, you must create the file-transport.prop file and add MAI_CONFIGURED = YES entry. You must not edit the entry in the /IBMMON/ITM_CNFG database.
   - For all other SAP systems that have basis version equal to 7.0 or later and Solution Manager V7.1 without MAI configuration, you must directly import the single IBM Tivoli Monitoring transport file.
3. Copy the following transport files into the SAP environment from the /ABAP directory or /ABAP/BADI directory of the SAP agent CD or image:
   - K711_00xxxU.ITM and R711_00xxxU.ITM

     These files are Unicode versions of the transport. They contain the SAP agent ABAP code and Unicode support for text strings for Latin code pages and double-byte code pages.
   - K711_00xxx_DELETE.ITM and R711_00xxx_DELETE.ITM

     These transport files remove the ABAP code. The DELETE transport does not need to be imported, unless you stop using the product entirely and want to remove the transports from their SAP systems. See "Uninstalling the Advanced Business Application Programming (ABAP) transport from the SAP system" on page 44
4. Copy your transport files to the SAP Transport System data directory as follows, and do not change the transport file name:

   Unicode transport

   a. Copy the K711_00xxxU.ITM file to the cofiles directory
   b. Copy the R711_00xxxU.ITM file to the data directory.
5. Run the following command:

   ```
   tp addtobuffer ITMK711_00xxxU SID
   pf=\usr\sap\trans\bin\PROFILE_NAME
   ```

   Where:

   SID Target SAP system ID

   PROFILE_NAME
   Name of the tp profile file. Make sure that the current tp parameter file is specified when importing the agent transport files from the command line. The tp parameter file is typically named TP_DOMAIN_*SID*.PFL. This file name is case sensitive on UNIX systems.

   nnn Number for the target client where the agent is to run and in which the user ID, IBMMON_AGENT, and authorization profile, /IBMMON/AUTH, are defined.

   If you are using Central User Administration (CUA), see "Using Central User Administration (CUA)" on page 33. Alternately, you can use the SAP STMS transaction to import the ITMK711_00xxx.ITM and ITMK711_00xxxU.ITM transport requests. Ensure that the **Import Transport Request Again** and the **Overwrite Objects in Unconfirmed Repairs** options are checked on the **Import Options** tab of the Import Transport Request window.

Results

Depending on your SAP release level, when running the **tp import** command, you might receive return code 4, which does not indicate a problem, and is an expected result from the **import** command.

Local installation

You can install the SAP agent on the IBM Tivoli Monitoring system.

Procedure

To install the SAP agent on the IBM Tivoli Monitoring system, complete the agent installation steps in the "Installing monitoring agents" section of the *IBM Tivoli Monitoring Installation and Setup Guide*.

What to do next

After you install the SAP agent, you must download the SAP NetWeaver RFC SDK V7.20 library. All the files related to the NetWeaver RFC SDK V7.20 library are available for download from the SAP website.

Downloading the NetWeaver RFC SDK V7.20 library

Download the NetWeaver RFC SDK V7.20 library after you finish installing the SAP agent.

Procedure

1. Log in to SAP Marketplace by using the following URL:
   http://service.sap.com
2. Click **SAP Support Portal**.
3. Enter your Service Marketplace user name and password.
4. Click **Software Downloads** and expand the **Support Packages and Patches** link.
5. Click **Browse our Download Catalog**, and then click **Additional Components**.
6. Click **SAP NetWeaver RFC SDK**, and then click **SAP NetWeaver RFC SDK 7.20**.
7. Select the operating system where you have the SAP agent.
8. Download the `*.SAR` file on your computer.
9. To extract the `SAP Netweaver RFC SDK *.SAR` file by using the SAPCAR utility that is provided by SAP, run the following command:
   sapcar -xvf <SAP NetWeaver RFC SDK File Name>.SAR

   Note: You can download the SAPCAR utility from the SAP website.
10. Navigate to the `lib` folder inside the extracted folder.

What to do next

Copy the NetWeaver RFC SDK V7.20 library in to the SAP agent setup.

Copying the NetWeaver RFC SDK V7.20 library in SAP agent setup

The NetWeaver RFC SDK V7.20 library contains files that you must manually copy in the SAP agent setup location.

Procedure

1. Navigate to the directory where you downloaded the NetWeaver RFC SDK V7.20 library.
2. Copy the files to the SAP agent setup location.
   - For Windows 32-bit and 64-bit operating systems you must copy the following files:
     - icuin34.dll
     - libicudecnumber.dll

- libsapucum.dll
- icudt34.dll
- icuuc34.dll
- sapnwrfc.dll
- For Windows 32-bit operating system, you must copy the files to `%CANDLE_HOME%\TMAITM6` location.
- For Windows 64-bit operating system, you must copy the files to `%CANDLE_HOME%\TMAITM6_x64` location.

- For operating systems other than Windows, you must copy the files to the **$CANDLE_HOME\<intrp>/sa/lib** location, where <intrp> is the operating system code (aix526, li6263, sol606). You must copy the following files:
  - libsapnwrfc.so
  - ibicudecnumber.so
  - ibicuuc34.a
  - libicui18n34.a
  - libicudata34.a
  - libsapucum.so

What to do next

Verify the version of the NetWeaver RFC SDK V7.20 library that you have downloaded.

Verifying the NetWeaver RFC SDK V7.20 library

You must verify the version of the files after you copy the extracted files.

Procedure

- For Windows operating system:
  1. Right-click `sapnwrfc.dll` and click **Properties**.
  2. Click the **Version** tab.
  3. In the **Product Version** section, ensure that you have the following version: **720, patch 514, changelist 1448293**
- For operating systems other than Windows:
  1. Go to the `lib` folder in the extracted `*.SAR` file.
  2. Run the following command: **strings libsapnwrfc.so | grep SAPFileVersion**
  3. You must see the following message: `[root@IBMSAP2V6 lib]# strings libsapnwrfc.so | grep SAPFileVersion GetSAPFileVersion #[%]SAPFileVersion: 7200, 514, 22, 6206 .GetSAPFileVersion`

  Note: The message shows that this library has the version 720 patch 514.

Remote installation

You can install the SAP agent remotely from the Tivoli Enterprise Portal or from the command line.

Prerequisite:

If you deploy the SAP agent to a UNIX or Linux computer, you must ensure that the korn (ksh) shell is installed on that computer.

Note: Only the ksh shell is supported for running the installation and runtime scripts.

See the *IBM Tivoli Monitoring Installation and Setup Guide* for procedural information. See the following sections for agent-specific parameters:

- "Remote deployment from the Tivoli Enterprise Portal"
- "Deploying the monitoring agent by using the tacmd command" on page 18

Deploying the monitoring agent remotely in a Windows environment

You can deploy the SAP agent remotely in a Windows environment.

Procedure

1. Download the SAP RFC library for the platform to the location where you plan to deploy the SAP agent remotely.
2. Depending on your architecture and environment, copy the RFC library into one of the following paths:
   - `%CANDLE_HOME%/TMAITM6` for a 32-bit agent on a 32-bit Windows computer.
   - `%CANDLE_HOME%/TMAITM6_x64` for a 64-bit agent on a 64-bit Windows computer.
3. Deploy the agent either through the Tivoli Enterprise Portal or by using the **tacmd** command. To deploy the SAP agent on the Windows 2008 Enterprise Edition 64 bit platform, use IBM Tivoli Monitoring V6.2.2 Fix Pack 8.

Deploying the monitoring agent remotely in a non-Windows environment

You can deploy the SAP agent remotely in a non-Windows environment.

Procedure

1. Download the SAP RFC library for the platform to the location where you plan to deploy the SAP agent remotely.
2. Find the `sa<interp>.jar` file specifically for the computer where you plan to deploy the SAP agent.
3. Compress the NetWeaver RFC SDK V7.20 library (`lib*`) into the `sa<interp>.jar` file in the `<interp>/sa/lib` subfolder.
4. Complete the addbundles procedure.
5. Deploy the agent either through the Tivoli Enterprise Portal or by using the **tacmd** command.

Related reference:

"Remote deployment from the Tivoli Enterprise Portal"

"Deploying the monitoring agent by using the tacmd command" on page 18

Remote deployment from the Tivoli Enterprise Portal

For the **mySAP Properties** tab, complete the properties in Table 1. For information about these properties, see the descriptions of the values in step 2 here: "Configuring the SAP agent locally" on page 19.

Table 2. Properties for remote deployment mySAP Properties tab in the portal

Properties	**Values described in Configuring the SAP agent locally, Step 2: "Configuring the SAP agent locally" on page 19**
mySAP System ID	System identifier
mySAP Hostname (Primary)	Host name Primary
mySAP Hostname (Alternate 1)	Host name Alternate 1
mySAP Hostname (Alternate 2)	Host name Alternate 2
mySAP System Number (Primary)	System number Primary
mySAP System Number (Alternate 1)	System number Alternate 1
mySAP System Number (Alternate 2)	System number Alternate 2
mySAP Client Number	Client number

Table 2. Properties for remote deployment mySAP Properties tab in the portal (continued)

Properties	Values described in Configuring the SAP agent locally, Step 2: "Configuring the SAP agent locally" on page 19
mySAP User ID	User ID
mySAP User Password	Password or Password File
mySAP Language Code	Language

Use the following settings for the **Agent** tab "Run as" information:

Use local system account
(Windows only) Select this setting.

Allow service to interact with desktop
(Windows only) Leave this check box clear.

User Name
(UNIX only and optional) If you do not use the default User ID and password (the ID that is selected when you configure the OS agent), you can override them by using this field.

Group Name
(UNIX only and optional) If you do not use the default group name (the name that is selected when you configure the OS agent), you can override it by using this field.

Deploying the monitoring agent by using the tacmd command

See the *IBM Tivoli Monitoring Command Reference* for the complete **tacmd addSystem** command.

Use the **-t |--type TYPE** parameter to specify the SAP agent that you are configuring: SA

Use the values in Table 3 for the **-p | --properties** parameter to configure the SAP agent. For information about these values, see the descriptions of the values in Step 2 in: "Configuring the SAP agent locally" on page 19.

Table 3. Required values for remote deployment properties parameter

Values in properties parameter	Values described in Configuring the SAP agent, Step 2: "Configuring the SAP agent locally" on page 19
INSTANCE	System identifier
sap_conn.sap_conn_mode	Connection Mode
sap_appsrvmode.sap_hostname	Host name Primary
sap_appsrvmode.sap_systemno	System number Primary
sap_logon.sap_clientno	Client number
sap_logon.sap_userid	User ID
sap_logon.sap_password	Password
sap_logon.sap_language	Language

You can also use the optional values in Table 2. For information about these values, see the descriptions of the values in Step 2 in: "Configuring the SAP agent locally" on page 19.

Table 4. Optional values for remote deployment properties parameter

Values in properties parameter (optional)	Values described in Configuring the SAP agent, Step 2: "Configuring the SAP agent locally" on page 19
sap_appsrvmode.sap_hostname2	Host name Alternate 1
sap_appsrvmode.sap_hostname3	Host name Alternate 2

Table 4. Optional values for remote deployment properties parameter (continued)

Values in properties parameter (optional)	Values described in Configuring the SAP agent, Step 2: "Configuring the SAP agent locally"
sap_appsrvmode.sap_systemno2	System number Alternate 1
sap_appsrvmode.sap_systemno3	System number Alternate 2

See the following example of using the Application Server Mode

```
tacmd addSystem -t sa -n ps7488:LZ -p
INSTANCE=RDX
sap_conn.sap_conn_mode=appsrvmode sap_appsrvmode
sap_hostname=10.77.97.156
sap_appsrvmode.sap_systemno=20
sap_logon.sap_clientno=111
sap_logon.sap_userid=rdx_usr
sap_logon.sap_password=XXXXXXXX
sap_logon.sap_language=EN
```

Configuring the SAP agent locally

To monitor an SAP system, the SAP agent must connect to an application server in the system to be monitored so the agent can access the Advanced Business Application Programming (ABAP) code provided with the product. The specification of these connection parameters is the configuration process.

About this task

This section describes the basic configuration steps for the SAP agent on both Windows and UNIX systems. If you want to use remote management (install the SAP agent on a computer that is different from the SAP application server), see "Advanced installation and configuration of the SAP agent" on page 28.

You must choose between the Application Server Mode or the Logon Group Mode when you configure the SAP agent in the configuration window.

To configure a new instance of the SAP agent by using the Application Server Mode, perform the following steps:

Procedure

1. Do one of the following depending on your operating system:
   - For Windows systems:
     a. From the Manage Tivoli Enterprise Monitoring Services window, double-click **IBM Tivoli Composite Application Manager Agent for SAP Applications Template**
     b. Use the information in Step 2 to complete the agent-specific parameters.
   - For UNIX systems, do one of the following procedures:
     Use the GUI:
     a. In the Manage Tivoli Enterprise Monitoring Services window, select **SAP agent**.
     b. Select **Actions** > **Configure** to display the Configured SAP agents window.
     c. Select the **Create new configuration** check box.
     d. Enter a 3-character identifier.
     e. Click **Configure**.
     f. Use the information in Step 2 to complete the agent-specific parameters.
   - or
     Use the command line:

a. Run the **itmcmd config** command:

```
itmcmd config -A -o system_identifier sa
```

system_identifier
Unique three-character SAP system identifier, for example, QA1. This identifier is the same as the system identifier described later in this topic.

sa Product code for the SAP agent

The following example command configures the SAP agent for a system named "QA1":

```
itmcmd config -A -o QA1 sa
```

This example command configures the SAP agent for a system named "QA1." You can have multiple configurations for the agent, one for each SAP system ID (SID). Each configuration must be created separately by running the **itmcmd config** command.

b. Complete the parameters for configuring IBM Tivoli Monitoring.

c. Use the information in Step 2 to complete the line prompts for the agent-specific parameters.

For additional information about the **itmcmd config** command, see the *IBM Tivoli Monitoring Administrator's Guide.* You must configure only one instance of the agent per SAP system. You do not need one instance per application server.

2. Use the following values to configure the SAP agent. Depending on the configuration mode selected by the user, the input parameters vary.

Application Server Mode:
Obtain these values from your SAP Administrator.

System identifier
3-character SAP system identifier (SID).

More than one instance of the SAP agent might run on this computer, so you want to supply a name to uniquely identify this agent instance. The name you supply is shown in the **Task/Subsystem** column of the Manage Tivoli Enterprise Monitoring Services window. It is also shown in the agent name in the Navigator tree of the Tivoli Enterprise Portal.

You can use the SID for the SAP system that you want this agent to monitor. However, in some cases where you might want to supply a different identifier. For example, if you plan to run two instances of the agent to monitor two different SAP systems with the same SID, you can supply a different identifier to ensure uniqueness. The identifier is used only as a label.

Host name

Primary
Host name of the SAP application server to which this agent is to connect. If your SAP servers communicate over a private LAN, the computers that host the servers have two or more network cards. For the host name, enter a name by which the application server can be reached from external systems, such as through the SAPGUI logon. Do not use the private LAN host name. The default is the host name on which the agent is installed.

Use an application server, such as the central instance, that is highly available in the SAP system.

Alternate 1
(optional) Second choice for the host name if the Primary host is unavailable.

Alternate 2
(optional) Third choice for the host name if both the Primary and Alternate 1 hosts are unavailable.

System number
Two-digit SAP system or instance number used for connecting to an SAP host server, defaults to 00.

Primary
System number for the primary host name.

Alternate 1
(optional) System number for the host name that is the first alternate.

Alternate 2
(optional) System number for the host name that is the second alternate.

Logon group Mode:
Obtain these values from your SAP Administrator.

Logon Group: Name of the SAP Server Logon group.

Message Server Hostname: Host name of the SAP message server.

Message Service: Name of the service where the SAP Message server is located.

Note: For example, you might use the sapmsTV1 Message service name, or the 3601 full message service port number.
You must include service names in the following operating system services files:

- On UNIX systems: `/etc/services`
- On Windows systems: `\windows\system32\drivers\etc\services`

Route String: Contains the SAP router string. Specify the SAP router string if you want access to the SAP server with a SAP router.
For example, the `/H/host/H/` router string must be in the following format:
`/H/beagle/H/brittany/H/`
or
`/H/amsaix11.tivlab.raleigh.ibm.com/W/tivoli/H/amsaix25`

Common parameters
The following parameters are common to both configuration modes:

Client number
SAP client number for the RFC logon to SAP, defaults to 000. If the predefined IBM Tivoli Monitoring user generated by ABAP is used, enter the client number that was specified in the transport import. This number is the same as the *nnn* client number under the Profile Name here: "Using SAP transport and defining the user" on page 13.

User ID
SAP user ID for the RFC logon to SAP, defaults to IBMMON_AGENT, which is the predefined user ID created during the import.

Password
Use one of these two options:

Password
SAP password for the user ID that you specified, for example, you enter a user-defined ID and password.

A default password, for example, `ITMMYSAP` for an IBMMON_AGENT user.

Language
Language code that indicates the language that the agent is to use when it connects to the SAP system. The language specified here determines the language in which you see SAP information, such as alert messages, syslog messages, and job log messages.

All SAP systems are delivered in English and German. If you require a different language, confirm with your SAP Administrator that the language is installed on the SAP system. Specifying an unsupported language prevents the agent from connecting to the SAP system.

The following languages and codes are supported:

- CS - Czech
- EN - English
- FR - French
- DE - German
- HU - Hungarian
- IT - Italian
- ES - Spanish
- JA - Japanese
- KO - Korean
- PL - Polish
- PT - Portuguese
- RU - Russian
- ZH - Chinese
- ZF - Traditional Chinese

RFC Trace

RFC trace setting for the SAPTRACE variable. When you select this check box, you activate RFC tracing and the default is no RFC tracing. For the command line, 0 = No trace and 1 = Do trace. Because RFC tracing generates extensive diagnostic information, use RFC tracing with the guidance of IBM Software Support.

View RFC Trace

If you are using the GUI, click **OK** to save the configuration values in the system registry.

3. If you are using the GUI, click **OK** to save the SAPROUTESTRING configuration value that you define in the system registry. SAPROUTESTRING is a route string that describes a connection required between two hosts using one or more SAProuters. Each of these SAProuters then checks the Route Permission Table to see whether the connection between the predecessor and successor is allowed, and if the connection is allowed, the SAProuter sets it up.
4. If you want to create another instance of the SAP agent, repeat Steps 1 - 3. Use a unique System Identifier for each SAP agent instance that you create.

Configuring the SAP agent remotely

You configure the SAP agent remotely by using either the **tacmd** command or the **configureSystem** command.

Procedure

1. To configure the SAP agent remotely by using the **configureSystem** command, enter the information for the property that you are changing. For information about the configuration settings, see Table 2 in “Deploying the monitoring agent by using the tacmd command” on page 18.
2. Open the Tivoli Enterprise Portal.
3. Navigate to the system where the agent that you want to configure is located.
4. Select the agent.
5. Right-click the agent and click **Configuration**.
6. Modify the parameters.
7. Click **OK** to save the changes.

   The following examples show the **ConfigureSystem** command:

Remote reconfiguration for the Application server mode

```
./tacmd configureSystem -m P10-ps8805:fvssun11-1:mySAP -p INSTANCE=P10
sap_conn.sap_conn_mode=appsrvmode
sap_appsrvmode.sap_hostname=ps8805sap_appsrvmode.sap_systemno=00
sap_logon.sap_clientno=200
sap_logon.sap_userid=IBMMON_AGENT
sap_logon.sap_password=ITMMYSAPsap_logon.sap_language=EN
```

Remote reconfiguration for the Logon Group mode

```
./tacmd configuresystem -m PS5-ibmsap3v1:fvssun11-1:mySAP -p INSTANCE=PS5
sap_conn.sap_conn_mode=loggrpmode sap_loggrpmode.sap_logongroup=LG1
sap_loggrpmode.sap_msgserver=ibmsap3v1 sap_loggrpmode.sap_msgservice=3600
sap_logon.sap_userid=IBMMON_AGENT sap_logon.sap_password=ITMMYSAP
sap_logon.sap_clientno=100
sap_logon.sap_language=EN
```

Upgrading the SAP agent from a previous installation

You can upgrade from a previous installation of IBM Tivoli Composite Application Manager Agent for SAP Applications in an IBM Tivoli Monitoring environment.

Procedure

1. Upgrade the IBM Tivoli Monitoring installation to one of the minimum supported versions. For more information about the minimum supported versions, see the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. Upgrade the IBM Tivoli Composite Application Manager Agent for SAP Applications installation to version 7.1.1 Fix Pack 2.
3. Import the IBM Tivoli Composite Application Manager Agent for SAP Applications version 7.1.1 Fix Pack 2 Advanced Business Application Programming (ABAP) transport to the SAP system. For more information about importing this transport, see "Importing the Advanced Business Application Programming (ABAP) transport on the SAP system" on page 11.
4. Start IBM Tivoli Composite Application Manager Agent for SAP Applications. For more information about starting IBM Tivoli Composite Application Manager Agent for SAP Applications, see "Starting or stopping the SAP agent" on page 27.

Upgrading the SAP agent in Windows

You can upgrade the SAP agent from a previous installation locally on Windows monitoring servers. As you complete the upgrade procedure, the SAP agent is stopped.

Procedure

1. To start the installation, in the `\WINDOWS` subdirectory, double-click the `setup.exe` file. For distributed products, use the `agent product` CD and for z/OS® products, use the `data files` CD.
2. In the Welcome window, click **Next**.
3. In the Install Prerequisites window, read the prerequisites and the information about the SAP agent, and click **Next**.
4. After you accept the license agreement, to select the agent that you want to install, expand the **Tivoli Enterprise Monitoring Agent-TEMA** node. A list of monitoring agents to install on the monitoring server is shown.
5. In the Select Features window, select the **IBM Tivoli Composite Application Manager Agent for SAP** check box and the **32/64 bit Agent Compatibility Package** check box. Then, click **Next**.

   Note: The **32/64 bit Agent Compatibility Package** check box is enabled only for a Windows 64-bit operating system.
6. In the Start Copying Files window, read the list of actions that must be completed. To start the installation, click **Next**.

7. To continue the installation, click **YES**. The upgrade procedure starts.
8. Ignore the feature installation error and to proceed with the installation, click **OK**.
9. In the Setup Type window, click **Next**.
10. Enter the following configuration details for the SAP agent in the Configuration Defaults for Connecting to a TEMS dialog box.
    a. Enter the host name or the IP address of the Tivoli Enterprise Monitoring Server, for example, `IBMSAP2V15` and click **OK**.
    b. Select one of the following SAP connection modes: Application Server Mode or Logon Group Mode. For more information about the SAP connection modes, see "Configuring the SAP agent locally" on page 19
    c. Enter the configuration parameters and values for the connection mode that you selected and click **OK**. For more information about these configuration parameters, see "Environment variables in script files" on page 34.
    d. Enter the mySAP system information. For example, enter `10.77.85.100` as the SAP host name and `04` as the System number.
    e. Use the Test Connection feature to verify that you can connect to the SAP system successfully. For more information about this feature, see "Test Connection feature" on page 45.
    f. Click **OK**.
11. Click **Finish**.

Upgrading the SAP agent on UNIX or Linux

You can upgrade the SAP agent on UNIX or Linux monitoring servers. The SAP agent is stopped during the upgrade process.

Procedure

1. Run the **`./install.sh`** command by using the following installation media:
   - Use the agent product CD for the distributed agent products.
   - Use the data files CD for the z/OS agent products.
2. Press **Enter** to accept the `/opt/IBM/ITM` default directory as the IBM Tivoli Monitoring home directory, or type the full path to the installation directory that you used for the previous installation.
3. Select one of the following options, for example, type `1` to install the products locally, or type `2` to install the products remotely.
   1) Install the products to the local host.
   2) Install the products to the depot for remote deployment.
   3) Install Tivoli Enterprise Monitoring Server support for remote seeding.
   4) Exit the installation.

   Important: The **Install the products to the depot for remote deployment** option requires the Tivoli Enterprise Monitoring Server.
4. Read through the agreement, and type `1` to accept the agreement or type `2` to reject the agreement.
5. To install the additional components, type `1`. For example, to select the **IBM Tivoli Monitoring components for this operating system** component from the following list of options, type `1`:
   1) IBM Tivoli Monitoring components for this operating system
   2) Tivoli Enterprise Portal Browser Client support
   3) Tivoli Enterprise Portal Server support
   4) Tivoli Enterprise Monitoring Server support
   5) Other operating systems
6. To confirm your selection, type `1`.

7. To upgrade the SAP agent, and to select the **all of the above** option from the following list of options, type 3:
   1) IBM Tivoli Composite Application Manager Agent for SAP V07.11.00.00
   2) Tivoli Enterprise Services User Interface Extensions V06.23.03.00
   3) all of the above
8. Type 1 to confirm your selection.
9. Complete one of the following steps:
   - To add an additional component, for example, Tivoli Enterprise Portal Server support or Tivoli Enterprise Monitoring Server support, type 1.
   - To proceed with the installation, type 2.
10. To refresh the TEMS server, in the Manage TEMS Mode window, in the **View** menu, click **Refresh**. After you upgrade the SAP agent successfully, you must refresh the Tivoli Enterprise Monitoring Server configuration to check for the upgraded version of the SAP agent.

Upgrading the SAP agent remotely

You can upgrade the SAP agent remotely by using the command line.

Procedure

1. Complete the addbundles procedure. For more information about the **tacmd addbundles** command, see the *IBM Tivoli Universal Agent API and Command Programming Reference Guide*.
2. Use the **updateagent** command as shown in the following example:

   ```
   tacmd updateagent -t SA -n Primary:IBMSAP1-V20:NT -v 071100000
   ```

   This command has the following syntax: managed-os [{-v|--version} version] [{-f|--force}] where:

   -t type Specifies the type of agent to update.

   -n node managed-os
   Identifies the node on the computer where the agent that you want to update resides.

   -v version
   Specifies the version of the agent to which you want to upgrade.

   You must use the following format to specify the version of the agent: vvrrmmfff where *vv = version number*, *rr = release number*, *mm = modification*, and *fff = fix pack*.
3. To check the status of the upgrade, use the **getDeployStatus** command, as shown in the following example:

   ```
   tacmd getDeployStaus –c  UPDATE
   or
   tacmd getDeployStatus –g
   ```

Product upgrade configuration

Use manual updates if you upgrade from a previous version of the SAP agent.

Perform manual updates in the following cases:

- If you are using a password file created with the ksapwd utility.
- If you are using Take Action command wrapper scripts, such as **ksar3** or **ksanfy**, or copies of these scripts.

Password file changes

Version 6.2 of the SAP agent uses a new password encryption algorithm that is different from the one used in prior releases. This new algorithm is used when encrypting new clear-text passwords and when decrypting all encrypted passwords.

If the agent encounters an encrypted password that was encrypted with the old algorithm, the agent decrypts the password to an incorrect clear-text string and uses that password in an RFC OPEN call. The SAP system rejects the logon request because of an invalid password. If you make repeated attempts to log on with the incorrect password, the SAP system locks that user ID.

Encrypted passwords exist in upgraded installations in the following areas:

- Agent configuration files: Registry on Windows or localhost_sa_SID.cfg files on UNIX systems
- Password files created with the ksapwd utility
- Take Action command wrapper scripts such as **ksar3** and **ksanfy**

During the upgrade process, the SAP agent upgrade converts encrypted passwords that exist in the agent configuration files. This conversion occurs for all configured agents on both Windows and UNIX systems. You do not need to perform any actions to correct these passwords.

Encrypted passwords that are stored in `ksapwd` files are not converted during the upgrade process. You might be using a `password` file for the agent itself or for Take Action command utility scripts. If so, you must rerun the ksapwd utility after the upgrade to generate a new encrypted password in your password file. Failure to upgrade your password files can result in locked user IDs on your SAP system.

Encrypted passwords that are hard-coded in wrapper scripts are not converted during the upgrade process. See "Take Action command script changes" for more information about these files.

Take Action command script changes

The Take Action command scripts are updated to include environment variables that access and reference new encryption libraries and paths. Also, UNSET statements pass default values from the runtime agent to the Take Action command scripts.

The Take Action command scripts include the following scripts:

- For the ksar3exe program, **ksar3** on UNIX systems and **ksar3.bat** on Windows systems
- For the ksar3nfy program, **ks3nfy** on UNIX systems and **ksanfy.bat** on Windows systems

On non-windows systems, the following SAP agent environment variables are updated in the shell scripts for Take Action and SAPOffice Mail utilities:

- *ARCHITECTURE*: The value for the ARCHITECTURE variable is updated from **tmaitm6** to **TAMITM6**.
- *ICCRTE_DIR*: In previous versions of the SAP agent, the value for the *ICCRTE_DIR* variable was taken from **/usr/local/ibm/gsk7**. However, in SAP Agent 7.1, this value is taken from `//gsKit.config`.

The following tracing exports are included to generate the logs:

```
### set RAS1 tracing
export CTIRA_LOG_PATH=|CANDLEHOME|/logs
export KBB_VARPREFIX='%'
export KBB_RAS1_LOG='%(CTIRA_LOG_PATH)/aquarius_sa_
%(SAPSYSTEMNAME)_%(syspgm)_%(sysutcstart)-.log
INVENTORY=%(CTIRA_LOG_PATH)/aquarius_sa_%
(SAPSYSTEMNAME)_%(syspgm).inv COUNT=03
LIMIT=5 PRESERVE=1 MAXFILES=9'
export KBB_RAS1='ERROR'
```

Note: In this example, the variables are used in Take Action, SAP Office and Password Encryption/Decryption shell scripts for exporting the *LD_LIBRARY_PATH*, *LIBPATH*, *SHLIB_PATH*, and *ICCRTE_DIR* to the respective utilities binaries.

```
export LD_LIBRARY_PATH=|CANDLEHOME|/|BINARCH|/sa/lib:|CANDLEHOME|
/|ARCHITECTURE|/lib:|ICCRTE_DIR|/lib
export LIBPATH=|CANDLEHOME|7|BINARCH|/sa/lib:|CANDLEHOME|
/|ARCHITECTURE|/lib:|ICCRTE_DIR|/lib
```

```
export SHLIB_PATH=|CANDLEHOME|/|BINARCH|/sa/lib:|CANDLEHOME|
/|ARCHITECTURE|/lib:|ICCRTE_DIR|/lib:/lib:/usr/lib
export ICCRTE_DIR=|ICCRTE_DIR|
export KEYFILE_DIR=|CANDLEHOME|/keyfiles
```

During the upgrade process, the default wrapper scripts, ksar3 and ksanfy, are updated for all of the environment variable and UNSET statement changes. If you are using the default wrapper scripts, the only changes you must make are for updated password values if you included these values in the wrapper scripts.

If you made copies of the default wrapper scripts, your copies are not updated during the upgrade process. You must make all the updates manually. Compare the updated 6.2 wrapper scripts with your scripts to determine the changes that you need to make.

If you included encrypted passwords in the wrapper script files, you must update these encrypted passwords also to avoid locking your SAP system user ID. Use the ksapwd utility after upgrade to encrypt your password. If your wrapper script includes the encrypted password, then copy the new encrypted password into the wrapper script. If your wrapper script is using a password file, regenerate the password file with the ksapwd utility.

Starting or stopping the SAP agent

Depending on your operating system, to start or stop the SAP agent, you can use either the Windows or UNIX GUI or a command line.

You use the GUI in Windows or UNIX to start and stop the SAP agent. For UNIX operating systems, you can also use the command line.

When using the command line to start or stop the SAP agent, use the -o option to specify which SAP instance to control. For example:

```
itmcmd agent -o system_identifier start sa
```

or

```
itmcmd agent -o system_identifier stop sa
```

where:

system_identifier
Three-character SAP system ID for the SAP system.

For example, the following command starts a SAP system with the system ID of QA1:

```
itmcmd agent -o QA1 start sa
```

For more information about the **itmcmd agent** command, see the *IBM Tivoli Monitoring Command Reference*.

Verification of Solution Manager with MAI-Monitoring

To receive data for MAI Alerts, you must verify whether the Solution Manager V7.1 is configured correctly.

You can use Solution Manager V7.1 with MAI-Monitoring and Alerting Infrastructure to monitor the Managed Systems. Solution Manager V7.1 monitors itself and the satellite systems. Each satellite system has a plugin and a Diagnostic Agents. Diagnostics Agents fetch the data for Host or Operating System level. Each host can have multiple Diagnostic Agents for different Solution Managers monitoring the host. Following are the keywords that are used in Solution Manager MAI Monitoring:

- Metrics: Data from the satellite systems.

- Alerts: Notifications that are based on some crossovers of threshold values that can be configured.
- Incident: Alerts that are converted into tickets and assigned to any user.

Verifying the configuration of Solution Manager V7.1

To verify the configuration of Solution Manager V7.1 with MAI monitoring, you must verify the basic settings, global level settings, and template level settings.

Procedure

1. To verify the basic settings, enter the Transaction Code: `SOLMAN_SETUP` and click **Enter**. Ensure that all the LEDs are green in the following tabs:
   - Overview
   - Basic Configuration
   - Managed System Configuration

   Note: There are different categories of Managed Systems such as Technical Systems, Technical Scenarios, Host, Database, Instance, PI Domain, Technical Component, and Connection. You must configure these Managed Systems according to business requirements. The MAI Alerts are based on the Managed Systems that you configured.
2. Enter the Transaction code: `SE38` and click **Enter**.
3. Provide the program name as `RTCCTOOL` and run the report. Ensure that all the LEDs are green in the output.
4. To verify the global level settings, enter the Transaction code: `SOLMAN_WORKCENTER` and click **Enter**. Ensure that all the LEDs are green in the following tabs:
   - Overview
   - Configure Infrastructure
   - Pre-requisites
   - Configure
5. Verify whether the **Global Settings** for **Notification** status is **Active**.
6. To verify the template level settings, enter the Transaction Code: `SOLMAN_SETUP` and click **Enter**. In **Technical Settings**, in the **Auto-Notifications** list, ensure **Active** is selected.

   Note: For initial troubleshooting, ensure that email notifications are active.
7. For MAI system monitoring, verify the configuration of End-User Experience Monitoring (EEM) by using the following steps:
   a. Enter the Transaction code: `SE37` and press **Enter**.
   b. Enter **`AI_EEM_LIST_ALL_SCENARIOS`** in the **Function Module name** field and press F8. There must be an entry for End-User Experience Monitoring (EEM).

Advanced installation and configuration of the SAP agent

This following installation and configuration topics are described:

- "SAP RFC connections" on page 30
- "Test Connection feature" on page 45
- "Optional advanced configuration in SAP" on page 38
- "CEN CCMS reporting" on page 43
- "Uninstalling the Advanced Business Application Programming (ABAP) transport from the SAP system" on page 44

SAP function module

When the data volume is high on the SAP server, you might experience problems with certain workspaces causing a slow response time from the server. If the workspaces are not critical, you can disable the associated SAP function module.

By default, the SAP agent function modules are enabled. However, the following function modules are disabled by default:

- HTTP services under the SYS subnode (`/IBMMON/ITM_HTTP_SRVS`)
- XML messages under the PI/XI subnode (`/IBMMON/ITM_SXMB_MONI_NEW`)
- Sync/Async communication under the PI/XI subnode (`/IBMMON/ITM_SYN_ASYN_COMM`)
- qRFC inbound queue details under the Sys subnode (`/IBMMON/ITM_QIN_QDETAILS`)

When you disable the SAP function module, if you select a workspace, data is not displayed on the Tivoli Enterprise Portal. Therefore, you avoid any performance-related problems.

Related tasks:

"Enabling the SAP agent function module"
You can enable the SAP agent function module if you have disabled it previously to resolve performance problems.

"Disabling the SAP function module"
Some workspaces may cause a slow response from the SAP server and you can disable the SAP function module to improve the server performance.

Enabling the SAP agent function module

You can enable the SAP agent function module if you have disabled it previously to resolve performance problems.

Procedure

1. By using the SAP GUI, logon to the SAP system.
2. Run the `SE16` transaction code.
3. Enter `/IBMMON/ITM_CNFG` as the table name.
4. Select the row to delete and press **shift + F2** to delete the entry.
5. Click **Save**.

Disabling the SAP function module

Some workspaces may cause a slow response from the SAP server and you can disable the SAP function module to improve the server performance.

Procedure

1. By using the SAP GUI, logon to the SAP system.
2. Run the `SE16` transaction code.
3. Enter `/IBMMON/ITM_CNFG` as the table name.
4. To create a new entry, press **F5**.

5. In the **PARM NAME** field, enter the name of the SAP function module.
6. In the **VALUE CHAR** field, enter `No`.
7. Click **Save**.

Using remote management

The SAP agent completes its functions by using SAP Remote Function Calls (RFC).

About this task

The RFC architecture allows calls between network connected computers. That is, the SAP agent must not stay on the same physical computer as your SAP servers. It can remain on a remote computer. You might want to use remote management in the following cases:

- When SAP systems are under strict change control, minimize SAP system changes by not having the monitoring component on the SAP computers.
- Minimize resource usage (CPU, memory, disk) on the SAP computers. This minimal resource usage is useful if you use intensive historical data collection operations on the SAP agent or when SAP platforms have limited resources for additional operations.
- Monitor SAP systems on any operating system or hardware platform. For example, the SAP agent does not run natively on OS/400®, but you can manage your OS/400 SAP systems by using remote management.

To implement remote management, complete the following steps:

Procedure

1. Install the SAP agent on a computer or operating system supported by the agent, such as Windows 2003 Enterprise Edition.
2. Ensure that you have not set firewall limitations between this computer and the SAP application server to which you want to connect.
3. Configure the agent on this computer.
4. Complete the rest of the configuration section.

   Local management is appropriate in the following environments:
   - Environments that require other local IBM Tivoli Monitoring operating system and database agents on SAP systems
   - Environments with SAP systems that have sufficient resources for additional operations
   - Small environments with few SAP systems

SAP user IDs

This section provides information about SAP user IDs and permissions required by the SAP agent.

User IDs support the following purposes:

- "Basic agent monitoring" on page 31
- "Take Action commands and SAP permissions" on page 33
- "SAPGUI" on page 33
- "Using Central User Administration (CUA)" on page 33

SAP RFC connections

The SAP agent uses Remote Function Calls (RFC) connections for internal Centralized Computing Center Management (CCMS) polling and CCMS alert data collection. This behavior is specific to the SAP RFC architecture.

The SAP agent opens one dedicated RFC connection to the SAP system that is monitored by the agent. The SAP system then opens one internal connection per application server for data collection through function modules and programs. If CCMS alerts are collected by the agent, the SAP system opens one additional (system internal) RFC connection to each application server for this collection thread. When data collection starts, one RFC connection for the agent is opened. Then, up to twice the number of SAP application servers for additional internal system RFC connections are opened.

You must ensure that the instance that is monitoring can accommodate the additional RFC sessions, especially in large systems with 10 or more instances. When the anticipated RFC load for monitoring might adversely affect system performance and tolerances, adjust the SAP profile parameter. Contact your SAP Administrator and see the following SAP Notes:

- Terminal Sessions (default setting: 200) 22099
- communication/Gateway/Conversation Settings 887909 316877 384971

Basic agent monitoring

The SAP agent creates an IBMMON_AGENT in the SAP system when the agent transport is imported.

This user ID is IBMMON_AGENT with the default password ITMMYSAP. It is preconfigured to be System Type user-only and to use the /IBMMON/AUTH authorization profile. This profile, which is created at transport import time, contains the minimal set of permissions to run the agent Advanced Business Application Programming (ABAP) code. Also, this profile accepts a set of limited actions on your SAP system.

If this user ID name is unacceptable, for example, if it violates your installation naming conventions, you can create a different user ID. The user ID can be any allowable SAP user ID, but it requires the complete set of permissions in the /IBMMON/AUTH profile. The user ID requires System Type user-only access.

The default user ID provides sufficient authority only for the following purposes:

- Monitoring and data collection
- Closing Computing Center Management System (CCMS) alerts
- Enabling, disabling, and resetting gateway statistics
- Resetting Oracle database statistics

If you choose to limit the action capabilities of the agent, you can remove some of the action permissions such as closing CCMS alerts.

To access data on the Tivoli Enterprise Portal for specific sub nodes, ensure that you have appropriate authorizations. Table 1 lists the authorizations that are required to access the data from different sub nodes:

Table 5. The list of authorizations

Sub nodes	Authorization objects	Authorization description
General system authorizations that include the following sub nodes: • Ins • Sys	S_ADMI_FCD	To access the System
	S_BDS_DS -BC-SRV-KPR-BDS	To access the Document Set
	S_BTCH_JOB	To run operations on the background jobs
	S_CCM_RECV	For transferring the Central System Repository data
	S_C_FUNCT	To make C calls in the ABAP programs
	S_DATASET	To access files
	S_RFC	To check RFC access. The S_RFC authorization object contains the following two sub-authorizations: • RFC1: To provide the authorizations for the RFC1 function group. • SDIFRUNTIME: To provide the authorizations for the SDIFRUNTIME function group.
	S_RFCACL	For RFC User
	S_RZL_ADM	To access Computing Center Management System (CCMS): System Administration
	S_TCODE	To check Transaction Code at Transaction Start
	S_TOOLS_EX	To access Tools Performance Monitor
Authorizations for Solution manager that include the following sub nodes: • Lds • Sol	D_MD_DATA -DMD	To view Data Contents of Master Data
	D_SOLMANBU	To access a Session Type of the Solution Manager
	D_SOLM_ACT	To access a Solution in the Solution Manager
	D_SOL_VSBL	To view a Solution in the Solution Manager
	S_CTS_SADM	To view System-Specific Administration (Transport)
	S_TABU_RFC	To view Client Comparison and Copy: Data Export with RFC
Authorizations for PI that includes the PI sub node	S_XMB_MONI	To access XI Message Monitoring

Table 5. The list of authorizations (continued)

Sub nodes	Authorization objects	Authorization description
Authorizations for MAI that includes the Slm sub node	AI_DIAGE2E	To access Solution Diagnostics end-to-end analysis
	AI_LMDB_OB	To access Landscape Management Database (LMDB) Objects
	SM_MOAL_TC	To access Monitoring and Alerting
	SM_WC_VIEW	To access Work Center User Interface Elements
	S_RFC_ADM	To access Administration options for RFC Destination
	S_RS_AUTH	To access BI Analysis in Role
	SM_APPTYPE	To access Solution Manager App Type
	SM_APP_ID	To access applications provided in Work center

Take Action commands and SAP permissions

Take Action commands such as **Cancel Job**, **Delete Job**, **Start job**, and **Output Request** require additional SAP permissions.

The agent provides a set of Take Action commands that require additional SAP permissions. The default user ID does not have permission for these functions. The following Take Action commands are affected:

- **Cancel Job**
- **Delete Job**
- **Output Request**
- **Start Job**

If you want to allow the agent to take these actions, you must grant additional permissions to the agent user ID. Alternatively, you can provide a separate user ID with these limited permissions. You configure the user ID to use the SAP agent by using the `ksar3` and `ksapwd` capabilities.

For configuration information, see:

- "Automated functions" on page 34
- "SAP Office email" on page 34
- "SAP password encryption" on page 36

SAPGUI

Use the SAP agent to open a SAPGUI session directly in the SAP system from workspace views within the agent.

The SAPGUI logon parameters default to the Windows user ID.

If you want to allow users to access your SAP systems and take actions in them, you can provide additional user IDs for this purpose. Any user IDs that you add with permissions to open the GUI can be configured into the SAP agent by using the procedures described in "Using the sapshcut command" on page 36.

Using Central User Administration (CUA)

You use the CUA to monitor a SAP system.

Procedure

To use the predefined user ID and authorization role to monitor a SAP system set up with Central User Administration, complete one of the following steps:

- Install the transport into the Central User Administration parent logical system client.
- Manually create the user ID or role in the client where you want to install the transport. The user ID or role is in the client where the transport is installed (imported).
- Manually create the user ID or role in the Central User Administration parent logical system client. Then, distribute the user ID or role to the client where the agent runs.
- Manually create the user ID or role in the Central User Administration parent logical system client and run the agent in this client.

Automated functions

You use the `ksar3` and `ksar3exe` utilities to run automated functions.

The SAP agent provides the `ksar3exe` utility to run an action in a SAP system that you are monitoring. The SAP agent provides the `ksar3` script (batch or shell) as a wrapper for this utility. The script is used to set or override environment variables required by the utility, in particular, the SAP user ID and password. Always use the script in your automation functions such as Take Action commands, situation actions, and policy actions.

For more information about setting environment variables in these scripts, see "Environment variables in script files."

For detailed command syntax and examples, see the "ksar3" section and the "ksar3exe" section of the *ITCAM Agent for SAP Applications Troubleshooting Guide*.

SAP Office email

You use the `ksanfy` and `ksar3nfy` utilities to send SAP Office email.

The SAP agent provides the `ksar3nfy` utility to send mail items to SAP Office inboxes in a SAP system that you are monitoring. Then, you deliver information or instructions to administrative users. The SAP agent provides the `ksanfy` script (batch or shell) as a wrapper for this utility. The script is used to set or override environment variables required by the utility, in particular the mySAP user ID and password. Always use the script in your automation functions such as Take Action commands, situation actions, and policy actions.

For more information about setting environment variables in these scripts, see "Environment variables in script files."

For detailed command syntax and examples, see the "ksar3" section and the "ksar3nfy" section of the *ITCAM Agent for SAP Applications Troubleshooting Guide*.

Environment variables in script files

All required environment variables are passed to the `ksar3` and `ksanfy` scripts from the Tivoli Enterprise Portal.

Use the information in this section to modify your `ksar3` and `ksanfy` script files to override these variables. You can set the logon environment variables in Table 6 on page 35. For information about these variables, see the descriptions for the values in Step 2 in: "Configuring the SAP agent locally" on page 19.

Note: Do not modify the series of lines at the beginning of the script that use the **unset** command to set environment variables to empty values. Make changes after the section of the script that is marked as `DO NOT MODIFY THESE LINES`.

Table 6. Logon environment variables

Variables	Values described in Configuring the SAP agent, Step 2: "Configuring the SAP agent locally" on page 19
INSTANCE	System identifier
sap_conn.sap_conn_mode	Connection Mode
sap_loggrpmode.sap_logongroup	SAP Logon Group
sap_loggrpmode.sap_msgserver	Logon group SAP Message Server
sap_loggrpmode.sap_msgservice	Logon group SAP Message Service
sap_logon.sap_userid	User ID
sap_logon.sap_password	Password
sap_logon.sap_language	Language
sap_routestring	SAP Route String

See the following example for using the Logon Group Mode:

```
tacmd addSystem -t sa -n ibmsap2v16:LZ -p INSTANCE=PS5
 sap_loggrpmode.sap_logongroup=PSL
 sap_loggrpmode.sap_msgserver=IBMVSAP1
 sap_loggrpmode.sap_msgservice=3600
 sap_logon.sap_userid=IBMMON_AGENT
 sap_logon.sap_password=ITMMYSAP
 sap_logon.sap_clientno=100
 sap_loggrpmode.sap_routestring=
 sap_logon.sap_language=EN
```

SAPPASSWORD can have the following values:

Password
Plain text or encrypted password

FILE() Instructs the utility to read the encrypted password from the default `ksa.pwd` file in the current directory. To create this file, see "SAP password encryption" on page 36.

FILE(*file_name*)
Instructs the utility to read the encrypted password from the `file_name` file. `file_name` can be either a simple file name or a path and file name. To create this file, see "SAP password encryption" on page 36.

Use the **ksanfy** command to send SAP Office email to SAP users.

Note: The command is called **ksanfy.exe** on Windows systems and **ksanfy** on UNIX systems.

Before you send mail, you must set the environment variables shown in the following table in the `ksanfy.bat` file.

Table 7. Environment variables for the Application server mode and the Logon group mode

Mode	Environment variables
Application Server Mode	*set SAPHOST=*
	set SAPHOST2=
	set SAPHOST3=
	set SAPSYSTEMNUMBER=
	set SAPSYSTEMNUMBER2=
	set SAPSYSTEMNUMBER3=
	set SAPSYSTEMNAME=
	set SAPCLIENT=
	set SAPUSER=
	set SAPPASSWORD=
Logon Group Mode	*set SAPHOST=*
	set SAPSYSTEMNAME=
	set SAPCLIENT=
	set SAPUSER=
	set SAPPASSWORD=
	set SAPLOGONGROUP=
	set SAPMSGSERVER=
	set SAPMSGSERVICE=
	set SAPROUTESTRING=

Important: All parameters with a field name that includes the digit 2 or the digit 3 are **alternate1** and **alternate2** parameters. For example, SAPHOST, SAPSYSTEMNUMBER, SAPGATEWAY, and SAPGATEWAYSERVICE. All parameters with a filename that ends with the digit 2 or 3 are **primary** parameters.

If you do not provide **primary** parameters, you must provide **alternate1** or **alternate2** parameters.

For example, to send a mail to a user, use this syntax: ksanfy Recipient(User) Message(Message)

The following return code is shown in the log:

```
0000 - for Successful send Mail to SAP User
0012 - for Connection Failure with SAP Server
```

SAP password encryption

The SAP agent provides the ksar3pwd utility to enable you to encrypt a SAP password and save it in a file.

The SAP agent provides the ksapwd script (batch or shell) as a wrapper for this utility.

See the “ksapwd” section and the “ksar3pwd” section of the *ITCAM Agent for SAP Applications Troubleshooting Guide* for detailed command syntax and examples.

Using the sapshcut command

You use the **sapshcut** command to open the SAPGUI.

About this task

In most of the SAP agent workspace tables, you right-click on a table row and select **Launch**. A list of SAP transactions are shown that are relevant to the IBM Tivoli Monitoring workspace that you are viewing are shown.

When you select one of the Launch options, IBM Tivoli Monitoring starts the SAP command called **sapshcut** that in turn brings up the SAPGUI. IBM Tivoli Monitoring passes the appropriate parameters that start the selected SAP transaction on the SAP system that is being monitored.

For this feature to work, you must complete the following procedure:

Procedure

1. Install the SAPGUI on the computer where you are running the Tivoli Enterprise Portal desktop or browser. This computer must have a Windows operating system because the **sapshcut** command is available on Windows systems only. The SAP agent supports the Windows SAPGUI only, not the Java SAPGUI.
2. Add the directory that contains the **sapshcut.exe** command to your system or user path. The **sapshcut.exe** command is installed as part of the SAP client into the following directory: `C:\Program Files\SAP\FrontEnd\SAPgui`. To add additional directories to the system or user path on Windows systems, select **Control Panel** > **System** > **Advanced** > **Environment Variables**.
3. Restart the Tivoli Enterprise Portal desktop or browser after you modify the path.
4. Configure saplogon for any systems to which you want to connect. It is optional to reduce the number of SAPGUI prompts.
5. Make sure the saplogon description starts with the SID. It is optional to reduce the number of SAPGUI prompts.

   By default you are logged on to the SAPGUI as follows:

   - SAP system that is being monitored
   - SAP client that was specified for the SAP agent
   - Windows user ID

   You can override these default logon parameters (client and user) by setting them in the `sapshcut.bat` file. You can also set the password and other SAP environment variables in this file.

   You can override these default logon parameters (client and user) by setting them in the `sapshcut.bat` file. You can also set the password and other SAP environment variables in this file.

   You can create and run a Windows `sapshcut.bat` file as a front end to the `sapshcut` executable file. The `.bat` file must be named `sapshcut.bat`(or `sapshcut.cmd`) and must be located in your default path preceding the `sapshcut.exe` file.

   The following parameters are passed to the `sapshcut.bat` file when called from a predefined Launch definition:

   %1 keyword "-command"

   %2 transaction_name, for example: SM13

   %3 keyword "-system"

   %4 SAP_system_identifier, for example: TV1

   %5 keyword "-client"

   %6 client_number, for example: 100

   The following example shows a sample `sapshcut.cmd` file. In this example, you use a different user ID and password when **sapshcut** is run through the Application Launch for the SAP system TV1. All other SAP systems use the default logon parameters.

```
@echo off set sapshcut="C:\Program Files\SAP\FrontEnd\SAPgui\sapshcut.exe"
if "%4" == "TV1" (
   %sapshcut% %* -user=myid -password=mypwd
) else (
   %sapshcut% %*
)
```

Optional advanced configuration in SAP

You configure the SAP agent by using standard SAP or agent-provided SAP functions.

Use agent-provided transactions in SAP to customize a number of agent behaviors. After you run the/n/IBMMON/ITM_CONFIG transaction to access the main configuration menu in SAP, select one of the following configuration options:

- "Copy, back up, restore feature and transactions"
- "Copy, back up, and restore data by using transactions" on page 39
- "Command line utility tool" on page 40
- "Running the command line utility on a Windows environment" on page 40
- "Running the command line utility on a Non-Windows environment" on page 41
- "IBM Tivoli Monitoring generated alerts maintenance" on page 41
- "Default sample periods maintenance" on page 41
- "Log file name maintenance" on page 42
- "Managed groups maintenance" on page 42
- "Select monitor sets and monitors transaction" on page 42

Note: You must preface all /IBMMON/ITM* transactions with /n.

Configuration changes made in these transactions are used immediately by the SAP agent except for those changes made to maintain managed groups. When the managed group configuration changes, the changes are discovered by the SAP agent at the next heartbeat.

Use SAP standard functions to complete the following configuration: "Configure Dialog Step Response Threshold in the SAP system" on page 43

Copy, back up, restore feature and transactions

The Copy, back up, and restore feature is available to you after you log on to the SAP server and run the following transaction:/n/IBMMON/ITM_CONFIG.

Copy, backup, and restore operations allow you to backup, restore, and copy IBM Tivoli Monitoring configuration data.

Use this feature to select from the following functions and to save the IBM Tivoli Monitoring configuration data:

- **Copy**

  Use this feature to copy the IBM Tivoli Monitoring configuration settings from one SAP server to another SAP server. For example, you might want to copy the IBM Tivoli Monitoring configuration settings from agent **a1** to SAP server instance SAP2. This agent runs on system **m1** and is configured for SAP server instance SAP 1. All the IBM Tivoli Monitoring configuration settings, except the SAP server instance monitoring settings are copied to the target SAP system. You implement the copy feature by using either the command line utility or the SAP GUI.

- **Backup**

  You store agent specific configurations that you completed on the SAP server by taking a backup of the system. Use this feature to save IBM Tivoli Monitoring specific configuration settings on the SAP

system. You use the /IBMMON/ITM_CONFIG transaction to enter the settings. The backup file is stored in the work directory on the SAP server to the following path: /usr/sap//DVEBMGS/work.

- **Restore**

  Use this feature to restore IBM Tivoli Monitoring configuration data on the SAP server from the work directory. You restore the IBM Tivoli Monitoring configuration data on the same SAP server where you completed the backup procedure of this configuration data or another SAP server. You can restore IBM Tivoli Monitoring configuration data to specific SAP and IBM Tivoli Monitoring tables. Configuration files are stored with a date and time stamp so you can select the point to which you want to restore your files.

You can backup IBM Tivoli Monitoring configurations that you completed for the SAP agent version 6.20. Then, after you upgrade to the SAP agent version 7.1.1 Fix Pack 2, you apply these saved configurations to the SAP system.

However, you must complete the following procedure to import a separate ABAP transport to the SAP server before you upgrade the agent:

1. Import the IBM Tivoli Monitoring file from the \ABAP\UPGRADE directory in the Installer.
2. Run the **se38** transaction code.
3. Enter **ZITM_CONFIG_BACKUP** as the program name and run this program to create a backup file.

Agent-specific configurations include configuration settings in the /IBMMON/ITM_CONFIG transaction in SAP. You can complete the following configuration procedures:

- Sample the frequency for alerts.
- Enable specific alerts.
- Store log file names.
- Manage group definitions.
- Select monitor sets and monitors.
- Select SAP instances for monitoring purposes.

Related tasks:

"Copy, back up, and restore data by using transactions"
On the SAP user interface, you copy, back up, and restore data by using the /n/IBMMON/ITM_CONFIG transaction.

Copy, back up, and restore data by using transactions

On the SAP user interface, you copy, back up, and restore data by using the /n/IBMMON/ITM_CONFIG transaction.

Before you begin

Use the Copy, Backup, and Restore procedures to copy the IBM Tivoli Monitoring configuration settings from one SAP server to another SAP server. All the IBM Tivoli Monitoring configuration settings, except the SAP server instance monitoring settings are copied to the target SAP system.

Procedure

Complete the following procedures to copy, back up, and restore your data on SAP:

- **Copy**
  1. Enter the target SAP system ID and the existing file name as source system id__<filenam>date_time.

     The /IBMMON/ITM_COPY transaction creates an IBM Tivoli Monitoring configuration file in the work directory with the filename as SAP target SAP system id__<filename>_date_time.
  2. Click **Execute** to copy the IBM Tivoli Monitoring configuration data to the file.

3. To return to the previous IBM Tivoli Monitoring configuration screen, click **Back** or **Cancel**.
   Input parameters expected are **Target System id** and **filename** that has to be copied.

- **Backup**
  1. Log on to the SAP server and start the /IBMMON/ITM_CONFIG transaction.
  2. Select **Backup**.
  3. Enter the backup filename.
     The file name is stored as sys_id_<filename>_date_time.
  4. Click **Execute** to run the backup and to store the file on the Application Server.

     Note: The backup file is stored in the work directory of the application server.
  5. To return to the previous IBM Tivoli Monitoring configuration screen, click **Back** or **Cancel**.
- **Restore**
  1. Log on to the SAP server and start the /IBMMON/ITM_CONFIG transaction.
  2. Select **Restore**.
  3. Enter the filename to restore as sys_id_<filename>_date_time.
  4. Click **Execute** to restore IBM Tivoli Monitoring configuration data.
  5. To return to the previous IBM Tivoli Monitoring configuration screen, click **Back** or **Cancel**.

Command line utility tool

You use the command line utility tool to copy, backup, and restore IBM Tivoli Monitoring configuration data on the SAP server.

You run the command line utility tool on Windows and Non-Windows environment. See "Running the command line utility on a Windows environment" and "Running the command line utility on a Non-Windows environment" on page 41.

- **Copy**

  You run the **backup** command to copy the IBM Tivoli Monitoring configuration file from the agent directory SAP server instance sap1 to sap2. You enter the filename and sap1 as the source system from the sap1 agent directory. Then, the ABAP function is called that copies the IBM Tivoli Monitoring settings from this file to the IBM Tivoli Monitoring configuration file for Sap2. You select **Copy** from the sap1 agent directory utility tool and enter a filename and sap2 as the target SAP system.
- **Backup**

  After you run the command line utility tool, you select the **Backup** option. Then, you enter the filename and the SAP system ID. The tool calls the /IBMMON/ITM_BACKUP SAP function module. The function module reads the specific IBM Tivoli Monitoring configuration settings that are stored in tables and stores them with a row and column separator. Then, the command line utility tool reads the string and writes the data into a file. The filename that is generated has the following format: ID>_<filename>-<date&time>. This file is stored in the directory where the utility program is stored.
- **Restore**

  After you run the command line utility tool, you enter the filename to restore and the target SAP system where you want to restore the file. The command line utility tool reads the file from the agent directory and calls the /IBMMON/ITM_RESTORE SAP function module. Then, the tool passes the IBM Tivoli Monitoring configurations as a string. The SAP function module updates the specific IBM Tivoli Monitoring tables and restores the specific IBM Tivoli Monitoring configurations.

Running the command line utility on a Windows environment

You run the command line utility on a Windows environment to complete copy, backup, and restore procedures.

Procedure

1. Depending on your operating system, complete one of the following procedures:

- For a 32-bit operating system, run the **ksacopybackuprestore.exe** command from the following path: %candle_home%\ TMAITM6.
- For a 64-bit operating system, run the **ksacopybackuprestore.exe** command from the following path: %candle_home%\ TMAITM6x64.

2. To create a backup file, complete the following steps:
   a. Select **Backup** and enter the file name and source SAP system name.
   b. The backup file is created with the following format: SYS ID>_<filename>_<date&time>.
3. To restore the file, complete the following steps:
   a. Select **Restore** and enter the target SAP system name.
   b. Enter the filename.
4. To copy the file, complete the following steps:
   a. From the source agent, select **Backup** and create a backup file.
   b. Copy the backup file from the source agent directory to the target agent directory.
   c. From the source directory, run the command line utility tool and select **Copy**.
   d. Enter the file name and the target SAP system.

Related tasks:

"Running the command line utility on a Non-Windows environment"
You run the command line utility on a Non-Windows environment to complete copy, backup, and restore procedures.

Running the command line utility on a Non-Windows environment

You run the command line utility on a Non-Windows environment to complete copy, backup, and restore procedures.

Procedure

1. Run the **ksacopybackuprestore.sh** command from the following path: /candle_home/<arch>/sa/shell.
2. To create a backup file complete the following steps:
   a. Select **Backup** and enter the file name and source SAP system name.
   b. The backup file is created with the following format: SYS ID>_<filename>_<date&time>. The backup file is saved to this location: %candlehome% / arch /sa/bin.
3. To restore the file, complete the following steps:
   a. Select **Restore** and enter the target SAP system name.
   b. Enter the filename.
4. To copy the file, complete the following steps:
   a. From the source agent, select **Backup** and create a backup file.
   b. Copy the backup file from the source agent directory to the target agent directory.
   c. From the source directory, run the command line utility tool and select **Copy**.
   d. Enter the file name and the target SAP system.

IBM Tivoli Monitoring generated alerts maintenance

You can modify alerts that are generated by Tivoli Monitoring by changing their status and thresholds.

This transaction is used to enable or disable alerts generated by Tivoli Monitoring and to set warning and critical thresholds. All alerts generated by Tivoli Monitoring are shown with their current status and threshold values.

When you modify alert status and thresholds, the modified values are used at the next sample time.

Default sample periods maintenance

The default sample period provides information about real-time reporting for certain attribute groups.

Some attribute groups have an implicit date and time for each record in the group. For example, the R/3_Abap_Dumps attribute group reports the create time for the dump and the R/3_System_Log attribute group reports the create time for the log entry. These records have a date and time field. You can obtain a report for a short history of the table instead of just the most recent information. This time interval is the time span for data collection and is used as the real-time interval when collecting data. The /IBMMON/ITM_PERIOD transaction defines a default sample period (time span for real-time reporting) for each of these attribute groups. The sample period identifies the length of the data sample period that starts from the current time and works back in time.

Log file name maintenance

Specific log files that are matched only to instances are included in IBM Tivoli Monitoring reports with log file information.

This transaction is used to identify which log files to consider for inclusion in IBM Tivoli Monitoring reports that contain log file information. All log files with a name that matches the specified name patterns on the specified instances are included in the report at the next data collection interval.

Managed groups maintenance

The Managed Group names transaction monitors and processes specific transactions in the SAP system.

Use this transaction to maintain IBM Tivoli Monitoring Managed Group definitions. All Managed Group names are passed to the Tivoli Enterprise Portal and shown in the Managed System Selection Lists. At the time of data collection, only data that matches the Attribute selection conditions are sent to the SAP agent. This data is shown in reports or used for evaluation in situations and policies.

You use Managed Groups to monitor subsets of information in the SAP system. You focus only on the parts of the SAP system in which you are interested and you ignore other parts that do not concern you. For example, if you are only interested in the response time of transactions that are part of the Financial Application, you create a Managed Group named Financials. Then, you include only Financial transaction codes in it. Whenever the Financials Managed Group is processed by the Tivoli Enterprise Portal only information that contains the specified transaction codes is considered when showing a report, evaluating a situation, or evaluating a policy.

Note: Managed group names cannot contain double-byte characters.

Select monitor sets and monitors transaction

Use the select monitor sets and monitors transaction to edit the Centralized Computing Central Management (CCMS) alerts configuration. For example, you can turn off CCMS alert collection completely.

This transaction is used to select the CCMS monitors from which IBM Tivoli Monitoring retrieves alerts. By default, the Entire System monitor is selected the first time this window is shown. You can change the monitor set, the monitor, or both the monitor set and monitor, and then save the configuration. You can select a maximum of three monitors for which to collect CCMS alerts.

To turn off CCMS alert collection completely, clear the check boxes for all of the monitors and save this configuration.

The agent that is already running reads this configuration and collects the CCMS alerts for the monitors that you selected. However, any CCMS alerts that were already collected by the agent before changing the CCMS alerts configuration remain with the agent and IBM Tivoli Monitoring.

In addition to selecting monitors and monitors sets, this transaction specifies the number of occurrences of an alert type to retrieve. Also, it helps you to decide whether to automatically close the older occurrences of the alerts that are not retrieved.

Configure Dialog Step Response Threshold in the SAP system

You configure a Dialog Step Response Threshold for any transaction by running the SE16 transaction.

Procedure

1. In the **Table Name** field, type `/IBMMON/ITM_TRSH`, and then select **Table Contents (F7)** to access the table.
2. To view the current threshold settings, select **Execute (F8)**. The transaction names are shown under **WORKLOAD** column; the threshold values are shown under the **THRESHOLD** column.
3. To add a new threshold setting, select **Create (F5)**. Type the transaction name in the **WORKLOAD** field. The following wildcards are accepted for the **WORKLOAD** value:
   - * matches multiple characters
   - + matches any single character
4. Type the threshold value, in milliseconds, in the **THRESHOLD** field. Select **Save** to save this setting. New and changed threshold values do not take effect immediately, but take effect under either of the following conditions:
   - The agent is restarted.
   - The agent reopens its RFC connection to the SAP system. This procedure occurs every 12 heartbeats, which, by default, is about every 2 hours and 10 minutes.

Results

The value entered for the **Threshold** column is returned in the Dialog Step Response Threshold attribute of the R/3_Transacation_Performance attribute group.

CEN CCMS reporting

Centralized (CEN) Computing Center Management System (CCMS) is a SAP monitoring capability.

Use this capability to report CCMS alerts for multiple SAP systems to a central monitoring hub. You monitor the SAP environment from one CCMS console. Centralized CCMS reporting is best used in the following environments:

- Primarily a CCMS operation where CCMS alerts are the only monitoring data needed.
- Centralized CCMS is part of the SAP environment.
- Large SAP environments with many SAP systems such as ISV and ISP.
- IBM Tivoli Monitoring V5.x integration with SAP agent CCMS adapters.
- Collect alerts from non-ABAP SAP components and application servers.

The SAP agent supports Centralized CCMS for reporting alerts only. Then, you place one SAP agent on a Centralized SAP system and view CCMS alerts for the entire SAP environment. This support is provided in the following ways:

- When reporting CCMS alerts, the agent checks if the alerts are associated with the SAP system that is directly monitored by the agent. If the agent determines that an alert belongs to a different SAP system, it assumes Centralized CCMS and automatically creates additional R3_Group managed systems.
- The <local_SID>-All_CCMS_alerts:Grp managed system is used to report the complete set of alerts from all remote SAP systems. The value of <local_SID> is the system identifier for the SAP system that is directly monitored. For example, if the local SAP system is QA1, this group name would be QA1-All_CCMS_alerts:Grp.
- The <local_SID>-<remote_SID>_CCMS_alerts:Grp managed system is used to report all alerts for one remote SAP system. The value of <local_SID> is the system identifier for the SAP system that is

directly monitored. The value of <remote_SID> is the system identifier for the remote SAP system. For example, if the local SAP system is QA1 and the remote SAP system is QA2, this group name would be QA1-QA2_CCMS_alerts:Grp.

- Each of these managed systems in the Navigator tree has the complete set of workspaces under it, but only the Alerts workspace has meaningful data.

The SAP agent maintains its definitions of Centralized CCMS groups in the Advanced Business Application Programming (ABAP) code in the directly managed SAP system. You might need to modify these definitions if a SAP system for which you are receiving centralized alerts is also being monitored directly by another instance of the SAP agent. You do not want alerts reported under both systems. You can limit the centralized alert reporting as follows:

- Use the `/IBMMON/ITM_CONFIG` transaction to Maintain Managed Groups. Change the All CCMS alerts group. Remove the remote system from this list by editing the group definition to EXCLUDE the remote system identifier.
- Use the`/IBMMON/ITM_CONFIG` transaction to Maintain Managed Groups. Delete the <remote_SID> CCMS alerts group. For example, if the remote SAP system is QA2, this group name would be QA2 CCMS alerts.

Alternatively, you can use Centralized CCMS to report alerts from all SAP systems, but prevent alert reporting from each locally installed agent. Use the following steps to set up this configuration:

- Configure an instance of the SAP agent to monitor the Centralized CCMS system. Allow the agent to detect and report all alerts from all remote SAP systems.
- Configure an instance of the SAP agent to monitor each remote SAP system. Disable alert collection and reporting for these agent instances by using the /IBMMON/ITM_CONFIG transaction to Select Monitor Sets and Monitors. Within this function, clear the check boxes for all monitors and save this configuration.

The SAP agent support for Centralized CCMS is used in a pure CCMS monitoring environment to view all alerts on a common console. Also, it can be used with its complete set of functions to provide situations, policies, and Take Action commands for the remote SAP systems.

Uninstalling the Advanced Business Application Programming (ABAP) transport from the SAP system

If you choose to remove the SAP agent from your system, you must import Delete transport to the SAP system. Delete transport deletes the SAP agent dictionary objects and function modules.

Before you begin

If the SAP system is version 7.20 or later, before you import the delete transport, in your transport profile, you must add the following transport profile parameter: **`tadirdeletions=true`**. This transport profile parameter is available in tp version 375.57.68 and also in the R3trans version 6.14 release 700 or higher. For more information about removing transport requests from the SAP system, see Deleting transport requests.

Procedure

1. Go to the`/ABAP` directory on the product CD.
2. Copy the transport files into the SAP environment.
3. Copy the `K711_00xxx_DELETE` and `R711_00xxx_DELETE` files to the SAP Transport System data directory as follows:
   a. Copy the `K711_00xxx_DELETE` file to the `cofiles` directory.
   b. Copy the `R711_00xxx_DELETE` file to the `data` directory.
4. Run the following commands:

a. **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***PROFILE_NAME*

b. **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *PROFILE_NAME*
where:

SID Target SAP system ID

PROFILE_NAME
Name of the tp profile file

nnn Number for the target client where the agent is to run

SAP instance customization

By default, all the instances of the SAP system are monitored and shown on the Tivoli Enterprise Portal.

As an administrator, you choose which SAP instance you want to monitor. Also as an administrator, you can turn off an SAP instance that you do not want to monitor.

The `/IBMMON/ITM_INSTANCE` custom transaction links to the `/IBMMON/ITM_CONFIG` transaction.

You select the **SAP Instances** option to view the available instances of the SAP server. Then, you select the instance that you want to monitor. These instances are displayed on the Tivoli Enterprise Portal. Any inactive or cleared instances are not shown on the Tivoli Enterprise Portal.

Test Connection feature

The Test Connection feature allows you to verify that you can connect your agent to the SAP system that is monitored.

You enter parameters on the GUI to complete the test connection procedure. If you connect to the SAP system successfully, a success message is displayed. Alternatively, if the connection fails, then a failure message is displayed.

The **Test Connection** button is available only in the Manage Tivoli Enterprise Monitoring Service (MTEMS) window.

Important:

The Test Connection feature has limitations as it works only when you configure your agent instance from the Manage Tivoli Enterprise Monitoring Service (MTEMS) window. If you configure your system from the Tivoli Enterprise Portal the **Test Connection** button is visible only but it is does not function.

Enabling CCMS design

Computing Center Management System (CCMS) monitoring is enhanced to collect CCMS records that are in an open or closed state from the last sample period. You can configure the Sample period and by default it has a value of 3 minutes. However, you must ensure that the transport files that are referenced by the SAP agent and the Advanced Business Application Programming (ABAP) transport are the same version.

Procedure

1. Log on to the SAP GUI.
2. Open the `SE16` transaction and add the `/IBMMON/ITM_CNFG` table name to the transaction.
3. To run the `/IBMMON/ITM_CNFG` ABAP function module and to provide configurations for the ABAP program, press **Enter** and then press **F8**.
4. To create a new entry to which you add new configuration parameters, press **F5.**

5. To create a new configuration parameter called **ISNEWCCMSDESIGN** with the value *YES* on the SAP server, in the **PARM NAME** field enter ISNEWCCMSDESIGN and in the **VALUE CHAR** field, enter YES.
6. Click **Save**. You can ignore the VALUE INT field.

Modifying the threshold value of an alert

You can modify the **max ccms alert** threshold value that is associated with an alert. By default, the value is 1000, which means that you can view 1000 alerts in the Tivoli Enterprise Portal. Older alerts are removed from the cache

Procedure

1. Complete one of the following steps:
   - On Windows operating system, open the <cancle home>\tmaitm6\KSAENV file.
   - On a Non-Windows operating system open the <candle home>/config/sa.ini file.
2. Add the *MAX_CCMS_ALERT_THRESHOLD=< Value>* to the end of the file.

   Note: The value must be greater than 100.

Disabling CCMS design

You can disable Computing Center Management System (CCMS) design.

Procedure

1. Log on to the SAP GUI.
2. Open the SE16 transaction and add the /IBMMON/ITM_CNFG table name to the transaction.
3. To run the /IBMMON/ITM_CNFG ABAP function module and to provide configurations for the ABAP program, press **Enter** and then press **F8**.
4. To delete the existing entry, select and right-click **ISNEWCCMSDESIGN**, and then click **Delete**.

Verifying CCMS design

After you enable Computing Center Management System (CCMS) design, you can verify that it is enabled to ensure that CCMS alerts are triggered for the SAP system.

Procedure

1. Log on to the SAP GUI.
2. Open the SE16 transaction and type /IBMMON/ITM_CNFG.
3. To run the /IBMMON/ITM_CNFG ABAP function module and to provide configurations for the ABAP programs, press **Enter** and then press **F8**.
4. Check whether the ISNEWCCMSDESIGN=YES entry is present. If the *ISNEWCCMSDESIGN* variable is set to YES, then CCMS design is enabled. Alternatively if this variable is set to NO, then CCMS design is disabled.
5. Click **Save**.
6. Open the agent log file that is saved to one of the following paths:
   - On Windows systems: \tmaitm6\logs_sa__ksaagent_<8 digit num>-01.log.
   - On Non-Windows systems: /logs/_sa__ksaagent_<8 digit num>-01.log.
7. Search the agent log file for the following messages:

   New CCMS design is enabled on ABAP side
   The CCMS design is enabled.

   CCMS alerts cache capacity MAX_CCMS_ALERT_THRESHOLD is set to <1000>
   The max alert threshold is set to a value of 1000.

New CCMS Design calling function module: <IBMMON/ITM_ALERTS>
The SAP agent logs this message before it requests CCMS alerts data from the SAP system.

Verifying MAI Alerts

To ensure that Solution Manager MAI is configured correctly for monitoring the MAI Alert Inbox in Technical Monitoring, you must verify that you receive MAI Alerts as output.

Procedure

1. Enter the Transaction code SOLMAN_WORKCENTER and click **Enter**. Check if you can view MAI Alerts in the Solution Manager MAI Alert Inbox under Technical Monitoring.
2. Check for BAdi implementation by using the following steps:
   a. Enter the Transaction code: SE19 and click **Enter**
   b. Enter /IBMMON/ITM_IMPL_ALRTINBX in the **Enhancement Implementation** field.
   c. Click **Display** and check if BAdi implementation is active in **Runtime Behavior** section.
3. Check if the database /IBMMON/ITM_ALIX contains MAI Alerts by using the following steps:
   a. Enter the Transaction code: SE16 and press **Enter**.
   b. In the **Table Name** field and enter /IBMMON/ITM_ALIX and run it. Ensure that you are receiving MAI Alerts in the table.
4. Enter the Transaction code: SE37 and click **Enter**.
5. In the **Function Module Name** field and enter /IBMMON/ITM_MAIALRT_INX and press F8. You must see MAI Alerts as output.

What to do next

If you are not able to view MAI Alerts in the /IBMMON/ITM_ALIX database, you must verify the settings in the Third Party Component.

Verifying configuration settings specific to Third Party Component

If you are not able to view MAI Alerts, then you must verify the settings in the Third Party Component.

Procedure

1. Verify that Third Party Component is active.
2. Verify that in OS Adapter, under **BAdi Implementation**, **Alert Reaction** is available. If **Alert Reaction** is not available, remove the default settings, and select the **BAdi implementation - Alert Reaction**.
3. Check the template settings by using the following steps:
   a. Verify the settings that are used to transfer specific alerts to the Third Party System such as SAP ABAP 7.0.0.
   b. Select **Expert Mode**, select **Alerts**, and then click **Third Party Component**. Ensure that you are able to view the Alert Reaction BAdi name.

      Note: Ensure that the latest SAP notes are implemented. For Solution Manager V7.1 Service Pack 8, check if the following notes are implemented:
      - https://service.sap.com/sap/support/notes/1959978
      - https://service.sap.com/sap/support/notes/1820727
4. If you are not able to view MAI Alerts in the /IBMMON/ITM_MAIALRT_INX database, you must run the following Solution Manager MAI configurations steps for Third Party Component:
   a. Enter the Transaction code: SOLMAN_SETUP and click **Enter**.
   b. In Technical Monitoring, select **System Monitoring**.
   c. Click **Configure Infrastructure** tab and then click **Default Settings** tab.

d. Click **Third Party Components** tab and then click **Edit**.
e. Select **Active** from the list.
f. Ensure that scope filter is set as **All alerts, Events and Metrics (with Internal Events)** for the selected connector.

Note: OS Command Adapter is also one of the methods to push data to the third party connector. To configure the OS Command Adapter, read the configuration detail settings in the How-to guide for OS Command Adapter.

Appendix. ITCAM for Applications documentation library

Various publications are relevant to the use of ITCAM for Applications .

For information about how to access and use the publications, see *Using the publications* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/common/using_publications.htm).

To find publications from the previous version of a product, click **Previous versions** under the name of the product in the **Contents** pane.

Documentation for this product is in the ITCAM for Applications Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcama.doc_7.2.1/welcome_apps721.html):

- Quick Start Guide
- Offering Guide
- Download instructions
- Links to Prerequisites
- Installation and Configuration Guide for each agent
- Link to Reference information for each agent
- Link to Troubleshooting Guide for each agent

Prerequisite publications

To use the information about the agents effectively, you must have some prerequisite knowledge.

See the following information at the IBM Tivoli Monitoring Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp) to gain prerequisite knowledge:

- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring High Availability Guide for Distributed Systems*
- IBM Tivoli Monitoring: Installation and Configuration Guides for the following agents: Operating System agents and Warehouse agents
- IBM Tivoli Monitoring: User's Guides for the following agents: Agentless OS monitors, Log file agent, System p agents, Systems Director base agent
- *IBM Tivoli Monitoring Agent Builder User's Guide*
- *IBM Tivoli Monitoring Command Reference*
- *IBM Tivoli Monitoring: Messages*
- *IBM Tivoli Monitoring Troubleshooting Guide*
- IBM Tivoli Monitoring: References for the following agents: Operating System agents and Warehouse agents
- IBM Tivoli Monitoring: Troubleshooting Guides for the following agents: Operating System agents and Warehouse agents
- *Tivoli Enterprise Portal User's Guide*

Related publications

The publications in related information centers provide useful information.

See the following information centers, which you can find by accessing Tivoli Documentation Central (http://www.ibm.com/tivoli/documentation):

- Tivoli Monitoring
- Tivoli Application Dependency Discovery Manager
- Tivoli Business Service Manager
- Tivoli Common Reporting
- Tivoli Enterprise Console
- Tivoli Netcool/OMNIbus

Tivoli Monitoring Community on Service Management Connect

Service Management Connect (SMC) is a repository of technical information that is organized by communities.

Access Service Management Connect at https://www.ibm.com/developerworks/servicemanagement.

For information about Tivoli products, see the Application Performance Management community (http://www.ibm.com/developerworks/servicemanagement/apm/index.html).

Connect, learn, and share with Service Management professionals. Get access to developers and product support technical experts who provide their perspectives and expertise. You can use SMC for these purposes:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the Application Performance Management community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

Other sources of documentation

You can obtain additional technical documentation about monitoring products from other sources.

See the following sources of technical documentation about monitoring products:

- IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary/) is an online catalog that contains integration documentation as well as other downloadable product extensions.
- IBM Redbook publications (http://www.redbooks.ibm.com/) include Redbooks® publications, Redpapers, and Redbooks technotes that provide information about products from platform and solution perspectives.
- Technotes (http://www.ibm.com/support/entry/portal/software), which are found through the IBM Software Support website, provide the latest information about known product limitations and workarounds.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM‘s application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Intel, Intel logo, and Intel Xeon, are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

Numerics

A

B

C

D

E

F

R

S

T

U

V

W

Printed in USA

SC27-5672-02