IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent
Version 6.3.1

Installation and Configuration Guide

SC27-5659-00

IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent
Version 6.3.1

Installation and Configuration Guide

SC27-5659-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 23

This edition applies to version 6.3.1 of IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent (product number 5724-U17) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

Chapter 1. Overview of the agent

The IBM® Tivoli® Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent provides you with the capability to monitor Active Directory. You can also use the agent to take basic actions with the Active Directory.

IBM Tivoli Monitoring is the base software for the Microsoft Active Directory agent.

IBM Tivoli Monitoring

IBM Tivoli Monitoring provides a way 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 IBM Tivoli Monitoring publications listed in “Prerequisite publications” on page 21 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

New in this release

For version 6.3.1 of the Microsoft Active Directory agent, the following enhancements were made since version 6.3, including the fix packs:

- Changes related to system requirements. See the information about system requirements in Software product compatibility reports (http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html).
- New attribute groups:
  - Remote Access Server
  - Direct Access Server
- Modified attribute groups:
  - RID Pool Information
  - LDAP Attributes
  - Root Directory Server
  - Replication Partner
  - Replication Partner Latency
- New workspaces:
  - Domain Controller Response Time History
  - Remote Access workspace

- Modified workspaces:
  - RID Pool Information
  - LDAP Attributes
  - Root Directory Server
  - Replication Partner
- New views:
  - Exhausted RID Status
  - Domain Controller Response Time History
  - Remote Access Server
  - Direct Access Server
- New situations:
  - RID_Consumption_Crit
  - RID_Consumption_Warn
  - DC_Response_Time_Crit
- Added new Cognos® data models and reports
- Updated the k3z.baroc file to support event mapping
- Added the Prerequisite Scanner report to verify the availability of tables and views in the Tivoli Data Warehouse for the predefined reports

Components of the IBM Tivoli Monitoring environment

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

This 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. The Tivoli Enterprise Monitoring Server is also a repository for historical data.

Tivoli Enterprise Monitoring Agent, Microsoft Active Directory agent
This monitoring agent collects data and distributes the data to the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Enterprise Portal, Tivoli Data Warehouse, and Tivoli Integrated Portal.

Multiple copies of this agent can run on the same system.

IBM Tivoli Netcool/OMNIbus
Tivoli Netcool/OMNIbus is an optional component and the recommended event management component. The Netcool/OMNIbus software is a service level management (SLM) system that delivers real-time, centralized monitoring of complex networks and IT domain events. Event information is tracked in a high-performance, in-memory database and presented to specific users through individually configurable filters and views. The software includes automation functions that you can use to perform intelligent processing on managed events. You can use this software to forward events for Tivoli Monitoring situations to Tivoli Netcool/OMNIbus.

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 Tivoli Monitoring situations to the Tivoli Enterprise Console component. If you do not already use Tivoli Enterprise Console and need an event management component, you can choose to use IBM Tivoli Netcool/OMNIbus.

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 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 Tivoli Monitoring and TADDM.

Tivoli Integrated Portal
Tivoli Integrated Portal helps the interaction and secure passing of data between Tivoli products through a common portal. Within the same dashboard view, you can launch from one application to another and research different aspects of your managed enterprise. This component is installed automatically with the first Tivoli product that uses the Tivoli Integrated Portal framework. Subsequent products can install updated versions of Tivoli Integrated Portal. After version 2.2, this component is replaced by the Dashboard Application Services Hub.

Agent Management Services

You can use IBM Tivoli Monitoring Agent Management Services to manage the Microsoft Active Directory 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 Microsoft Active Directory agent available, and to provide information about the status of the product to the Tivoli Enterprise Portal. IBM Tivoli Monitoring V6.2.2, Fix Pack 2 or later provides support for Agent Management Services. 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 IBM Tivoli Monitoring software and other integrated applications provides various interfaces that you can use to work with your resources and data.

The following interfaces are available:

Tivoli Enterprise Portal user interface
You can run the Tivoli Enterprise Portal as a desktop application or a browser application. The client interface is a graphical user interface (GUI) based on Java on a Windows or Linux workstation. The browser application is automatically installed with the Tivoli Enterprise Portal

Server. The desktop application is installed by using the Tivoli Monitoring installation media or with a Java Web Start application. To start the Tivoli Enterprise Portal browser client in your Internet browser, enter the URL for a specific Tivoli Enterprise Portal browser client installed on your web server.

Command-line interface
You can use Tivoli Monitoring commands to manage the Tivoli Monitoring components and their configuration. You can also run commands at the Tivoli Enterprise Console event server or the Tivoli Netcool/OMNIbus ObjectServer to configure event synchronization for enterprise situations.

Manage Tivoli Enterprise Monitoring Services window
You can use the window for the Manage Tivoli Enterprise Monitoring Services utility to configure the agent and start Tivoli services not designated to start automatically.

IBM Tivoli Netcool/OMNIbus event list
You can use the Netcool/OMNIbus event list to monitor and manage events. An event is created when the Netcool/OMNIbus ObjectServer receives an event, alert, message, or data item. Each event is made up of columns (or fields) of information that are displayed in a row in the ObjectServer alerts.status table. The Tivoli Netcool/OMNIbus web GUI is also a web-based application that processes network events from one or more data sources and presents the event data in various graphical formats.

IBM Tivoli Enterprise Console
You can use the Tivoli Enterprise Console to help ensure the optimal availability of an IT service for an organization. The Tivoli Enterprise Console is an event management application that integrates system, network, database, and application management. If you do not already use Tivoli Enterprise Console and need an event management component, you can choose to use Tivoli Netcool/OMNIbus.

IBM Tivoli Common Reporting
Use the Tivoli Common Reporting web user interface for specifying report parameters and other report properties, generating formatted reports, scheduling reports, and viewing reports. This user interface is based on the Dashboard Application Services Hub for Tivoli Common Reporting 3.1 and on Tivoli Integrated Portal for earlier versions.

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

IBM Tivoli Business Service Manager
The Tivoli Business Service Manager console provides a graphical user interface 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 moment in time or how the enterprise performed over a time period.

Tivoli Integrated Portal
Web-based products that are built on the Tivoli Integrated Portal framework share a common user interface where you can launch applications and share information. After version 2.2, this interface is replaced by the Dashboard Application Services Hub.

Functions of the Microsoft Active Directory agent

You can use the Microsoft Active Directory agent to collect and analyze Active Directory-specific information that is needed to detect problems and prevent them.

The Microsoft Active Directory agent provides a central point of management for your Microsoft Active Directory service. It provides a comprehensive way for gathering information that is needed to detect problems early and to prevent them. You can monitor many servers from a single workstation, and information is standardized across the system.

The Microsoft Active Directory agent collects and analyzes the following types of Active Directory-specific information:

- Sysvol replication details
- Forest-wide trust relationship details
- Time drift monitoring information
- Network replication status and performance details
- Directory system utilization information
- Local security authority details
- Name Service (NS) details
- Security Account Manager (SAM) details
- File Replication Service (FRS) details
- Distributed File Replication (DFS-R) details
- Active Directory network status
- DNS details relevant to Active Directory
- DHCP details relevant to Active Directory
- Physical storage details for Active Directory
- Knowledge Consistency Checker details
- Kerberos Key Distribution Center details
- Lightweight Directory Access Protocol details
- Address book performance and utilization details
- Built-in logon authentication and user authorization information
- Communication data between the Active Directory and Exchange Directory Service (XDS)
- Active Directory database and details of log files
- Event log entries that are related to the Directory Services or the Domain Naming System (DNS) Server of Active Directory.
- Conflict objects details
- Details of organizational units that are moved or deleted
- RID pool resource availability
- Netlogon authentication performance
- Information about the Active Directory Password Settings objects
- Deleted objects information
- Offline domain join performance details
- Domain controller response time details

The Microsoft Active Directory agent provides the following benefits:

- Supports 64-bit operating system
- Supports dynamic reorganization of the Active Directory logical view
- Provides bind functionality to check server availability
- Provides a graphical representation of the Trust Topology
- Increases knowledge with extensive reporting capabilities that provide real-time access to reliable, up-to-the-minute data. You can make faster, better-informed operating decisions.
- Enhances system performance because you can integrate, monitor, and manage your system, environment, console, and mission-critical applications. For example, the Microsoft Active Directory agent can alert you when conditions in your environment meet or exceed the thresholds you set. These alerts notify your system administrator to limit and control system traffic.
- Simplifies application and system management by managing applications, platforms, and resources across your system.

- Identifies bottlenecks and performance issues.
- Aids in capacity planning and analysis.

Data sources

Monitoring agents collect data from specific data sources.

The Microsoft Active Directory agent collects data from the following sources:

API Most of the attributes gathered by the Monitoring agent for Active Directory come from Application Programming Interfaces (API).

CL When there is no API available for a particular function, Command Language (CL) commands have been used.

Table 1. Mechanisms used to gather attributes

Attribute group	Collection source	API/CL names
Address Book	API	Performance Data Helper
Containers	API	Active Directory Service Interfaces
DNS ADIntegrated	API	• Active Directory Service Interfaces • Windows API
DNS ADIntegrated Details	API	• Active Directory Service Interfaces • Windows API
DFS Replication Connections	API	Performance Data Helper
DFS Service Volumes	API	Performance Data Helper
DFS Replication Folders	API	Performance Data Helper
DHCP	API	Performance Data Helper
Direct Access Server	API	Performance Data Helper
Directory Services	API	Performance Data Helper
DNS	API	Performance Data Helper
Domain Controller Availability	API	• Windows API • Active Directory Service Interfaces
Domain Controller Availability	CL	ping
Domain Controller Performance	API	• Performance Data Helper • Windows API • Active Directory Service Interfaces
Exchange Directory Services	API	Performance Data Helper
File Replication Service	API	Performance Data Helper
Forest Topology	API	Active Directory Service Interfaces
Kerberos Consistency Checker	API	Performance Data Helper
Kerberos Key Distribution Centre	API	Performance Data Helper
Lightweight Directory Access Protocol	API	• Performance Data Helper • Active Directory Service Interfaces
Lost and Found Objects	API	Active Directory Service Interfaces
Local Security Authority	API	Performance Data Helper

Table 1. Mechanisms used to gather attributes (continued)

Attribute group	Collection source	API/CL names
Name Service Provider	API	Performance Data Helper
Remote Access Server	API	Performance Data Helper
Replication	API	• Performance Data Helper • Windows API • Active Directory Service Interfaces
Replication	CL	net time
Replication Partner	API	• Windows API • Active Directory Service Interfaces
Replication Partner Latency	API	• Windows API • Active Directory Service Interfaces
Root Directory Server	API	Active Directory Service Interfaces
Security Accounts Manager	API	Performance Data Helper
Services	API	Service Control Manager
Sysvol Replication	API	Windows API
Sysvol Replication	CL	ntfrsutl
Trust	API	Windows API
Trust	CL	netdom verify
Trust Topology	API	Active Directory Service Interfaces
Event Logs	API	Windows Event Log API
Active Directory Database Information	API	Windows API
Replication Conflict Objects	API	Active Directory Service Interfaces
Moved or Deleted Organizational Units	API	Active Directory Service Interfaces
RID Pool Information	API	Active Directory Services Interfaces
Netlogon Attributes	API	Performance Data Helper
Password Settings Object	API	Active Directory Service Interfaces

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.

This chapter contains information about the requirements and configuration for the IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent.

With the self-describing agent capability, new or updated IBM Tivoli Monitoring agents can become operational after installation without having to perform 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 the *IBM Tivoli Monitoring Administrator's Guide* for additional information about using this capability.

Requirements

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

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

Installing language packs

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

Before you 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, ensure that you have installed the product in English. Perform the following steps depending on the operating system that you are using.

Installing language packs on Windows systems

You can install the language packs on a Windows system.

Procedure

1. Double-click `lpinstaller.bat` file in the language pack CD to start the installation program.
2. Select the language of the installer and click **OK**.
3. Click **Next** on the Introduction panel.
4. Click **Add/Update** and click **Next**.
5. Select the folder in which the National Language Support package (NLSPackage) files are located.

   Note: Usually the NLSPackage files are located in the nlspackage folder where the executable installer is located.
6. Select the language support for the agent of your choice and click **Next**.

   Note: You can select multiple languages by pressing the Ctrl key.
7. Select the languages that you want to install and click **Next**.
8. Examine the installation summary page and click **Next** to start the installation.

9. Click **Finish** after the installation completes.
10. Restart the Tivoli Enterprise Portal (if on the Tivoli Enterprise Portal Server) or restart the Tivoli Enterprise Portal Server (if on the Tivoli Enterprise Portal Server component).

Installing language packs on UNIX or Linux systems

You can install the language packs on a UNIX or Linux system.

Procedure

1. Run the following command to create a temporary directory on the computer. Ensure that the full path of the directory does not contain any spaces:
   ```
   mkdir dir_name
   ```
2. Mount the language pack CD to the temporary directory that you have 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 UNIX and Linux systems.
4. Select the language of the installer and click **OK**.
5. Click **Next** on the Introduction panel.
6. Click **Add/Update** and click **Next**.
7. Select the folder in which the National Language Support package (NLSPackage) files are located.

   Note: Usually, the NLSPackage files are located in the `nlspackage` folder where the installer executable is located.
8. Select the language support for the agent of your choice and click **Next**.

   Note: You can select multiple languages by pressing the Ctrl key.
9. Select the languages that you want to install and click **Next**.
10. Examine the installation summary page and click **Next** to start the installation.
11. Click **Finish** after the installation completes.
12. Restart the Tivoli Enterprise Portal (if on the Tivoli Enterprise Portal Server) or restart the Tivoli Enterprise Portal Server (if on the Tivoli Enterprise Portal Server component).

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" on page 11.
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 located 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 of the following steps 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
```

Prerequisites checking

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

For the Microsoft Active Directory agent, the Prerequisite Scanner verifies the following requirements:

- Memory
- Disk
- Operating systems
- Active Directory versions

Additionally, the Prerequisite Scanner verifies whether the user, who installs the agent, is a member of the Administrators group.

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

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

Agent-specific installation and configuration

In addition to the installation and configuration information in the *IBM Tivoli Monitoring Installation and Setup Guide*, use this agent-specific installation and configuration information to install the Microsoft Active Directory agent.

Running as a non-administrator user

You can run the Microsoft Active Directory agent as a non-administrator user.

About this task

You can run the monitoring agent for Active Directory as a non-administrator user; however, Trust Topology attributes and Sysvol Replication attributes might not be available. These attributes are available only to domain users.

To view the Trust Topology attributes, a non-administrator user must have the following registry permissions:

- Grant full access to the `HKEY_LOCAL_MACHINE\SOFTWARE\Candle` directory.
- Grant read access to the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib` directory.

To view the Sysvol Replication attributes, a non-administrator user must have full access to the `Sysvol` folder on all domain controllers in a domain.

The following table contains the attribute groups for the Active Directory agent that display data for domain users and performance monitoring users.

Table 2. Attribute groups for domain users and performance monitoring users

User right	Attribute group
Domain users	• RID Pool Information • Services • Event Logs • DNS • DNS ADIntegrated Details • DNS ADIntegrated • DHCP • Trust • Group Policy Objects • Lost and Found Objects • Exchange Directory Service • Replication Conflict Objects • LDAP Attribute • Root Directory Server • Containers • Replication Partner • Domain Controller Availability • Replication Partner Latency • Forest Topology

Table 2. Attribute groups for domain users and performance monitoring users (continued)

User right	Attribute group
Domain users and performance monitoring users	All attribute groups that are mentioned for the domain users and the following additional attribute groups: • Address Book • Replication • Directory Services • Knowledge Consistency Checker • Kerberos Key Distribution Center • Lightweight Directory Access Protocol • Local Security Authority • Name Service Provider • Security Accounts Manager • File Replication Service • Distributed File System Replication • DFS Replication Connections • DFS Replicated Folders • DFS Service Volume • Domain Controller Performance • Remote Access Server • Direct Access Server • Netlogon Attributes

Note: Additionally, the following attribute groups display data for users who are members of the *Administrators* group:

- Active Directory Database Information
- Moved or Deleted Organizational Unit
- Password Setting Objects

For information about running the agent as an administrator user refer "Running as an administrator user" on page 15

Procedure

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Expand the domain in which you want to create the user by clicking the plus sign (+) next to the name of a domain.
3. Right-click **Users**, and then click **New > User**.
4. Create a new user by using the New Object - User wizard. By default, a new user is a member of the *Domain Users* group.
5. Right-click the new user that is created in the *Domain Users* group, and click **Properties**. The "*username* Properties" window opens, where *username* is the name of the new user. Complete the following steps in the "*username* Properties" window:
   a. Click the **Member of** tab. In the **Member of** area, add the **Performance Monitor Users** group.
   b. Click **Apply**, and then click **OK**.
6. Navigate to the `Candle_Home` directory. The default path is `C:\IBM\ITM`.
7. Right-click the `ITM` folder and click **Properties**. The ITM Properties window opens. Complete the following steps in the ITM Properties window:
   a. On the **Security** tab, click **Edit**.

b. Click **Add** to add the new user and grant full access to this user.
c. Click **Apply**, and then click **OK**.

8. Click **Start > Run**, and then type `services.msc`. The Services window opens. Complete the following steps in the Services window:
   a. Right-click the Monitoring Agent for Active Directory service, and click **Properties**.
   b. In the Monitoring Agent for Active Directory Properties window, on the **Log On** tab, click **This Account**. Enter the user credentials.
   c. Click **Apply**, and then click **OK**.
9. Restart the agent service.

Running as an administrator user

You can run the Microsoft Active Directory agent as an administrator user.

About this task

You can run the monitoring agent for Active Directory as an administrator user. All attribute groups are available to the users who are members of the administrators group.

Procedure

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Expand the domain in which you want to create the user by clicking the plus sign (+) next to the name of a domain.
3. Right-click **Users**, and then click **New > User**.
4. Create a new user by using the New Object - User wizard. By default, a new user is a member of the *Domain Users* group.
5. Right-click the new user that is created in the *Domain Users* group, and click **Properties**. The "*username* Properties" window opens, where *username* is the name of the new user. Complete the following steps in the "*username* Properties" window:
   a. Click the **Member of** tab. In the **Member of** area, add the **Administrators** group.
   b. Click **Apply**, and then click **OK**.
6. Click **Start > Run**, and then type `services.msc`. The Services window opens. Complete the following steps in the Services window:
   a. Right-click the Monitoring Agent for Active Directory service, and click **Properties**.
   b. In the Monitoring Agent for Active Directory Properties window, on the **Log On** tab, click **This Account**. Enter the user credentials.
   c. Click **Apply**, and then click **OK**.
7. Restart the agent service.

Configuring caching

You can enable or disable the caching for the Microsoft Active Directory agent.

About this task

When configuring caching, you can enable or disable caching and set the cache interval by using the **ADO_CACHE_INTERVAL** environment variable in the `K3ZENV` file. Use the **ADO_CACHE_INTERVAL** environment variable to turn caching ON or OFF and to specify the caching interval in seconds. Caching interval is the time interval between two consecutive data collections. You can turn the caching ON by specifying any positive integer value. You can turn the caching OFF by specifying the value 0. With caching OFF, the agent collects data on demand. By default, caching is ON, and the caching interval value is 240.

The following attribute groups have an option for caching the data they collect for some configurable period:

- Domain Controller Availability
- DNS ADIntegrated
- Domain Controller Performance
- Replication
- Replication Latency
- Replication Partner
- Trusts
- Trust Topology

Procedure

Complete the following steps to turn caching ON or OFF during run time by using the Manage Tivoli Enterprise Monitoring Services:

1. In Manage Tivoli Enterprise Monitoring Services (`kinconfig.exe`), select the Monitoring Agent for Active Directory.
2. Right click and go to **Advanced options**.
3. Select **Edit ENV File** from the options. This opens the `K3ZENV` file for editing. The **`ADO_CACHE_INTERVAL`** variable exists in the `K3ZENV` file.
4. To turn caching OFF, set the **`ADO_CACHE_INTERVAL`** variable to `0`. To turn caching ON, set the **`ADO_CACHE_INTERVAL`** to any positive integer value. The default value is `240`. This value forms the caching interval in seconds. For instance, a value of `180` would mean a 3-minute interval.
5. After editing the `K3ZENV` file, save and close the file to implement the new cache interval value.
6. A message box appears asking if the agent needs to be recycled to include the changes in agent functionality. Clicking **Yes** recycles the agent with the new caching interval value. Clicking **No** lets the agent continue to run without the changes to the caching interval. When the agent is restarted, the changes are implemented.

   Note: Negative or zero value turns off caching. Non-integers (alphabets, special characters, and alphanumeric characters) are not supported for the cache interval and might result in unexpected behavior of the Microsoft Active Directory agent. The value can be raised to a higher interval.

Configuring ping variables

You can configure the ping variables to change the number of ping requests, the time to wait for each ping response, and the size of the ping packet to send.

About this task

The values for ping count, ping timeout, and ping size are configurable through environment variables when the agent is started. The default values are consistent with the current behavior of the agent. Default values are used if no value or an unsupported value is set in the environment. The following table lists the variables with their descriptions and default values.

Table 3. Ping variables descriptions and default values

Variable	Description	Default value	Unit
ADO_PING_COUNT	The number of ping requests to make.	1	
ADO_PING_ TIMEOUT	The time to wait for each ping response.	2000	Milli-seconds

Table 3. Ping variables descriptions and default values (continued)

Variable	Description	Default value	Unit
ADO_PING_SIZE	The size of the ping packet to send.	32	Bytes

Procedure

Complete the following steps to set the ping environment variables by using the Manage Tivoli Enterprise Monitoring Services (`kinconfig.exe`):

1. In Manage Tivoli Enterprise Monitoring Services (`kinconfig.exe`), select the Monitoring agent for Active Directory.
2. Right-click and select **Advanced options**.
3. Select **Edit ENV File** from the options. This option opens the `K3ZENV` file for editing. The **ADO_PING** variables exists in the `K3ZENV` file.
4. After editing the `K3ZENV` file, save and close the file to implement the new ping behavior.
5. A message is displayed asking if the agent should be recycled to include the changes in agent functionality. Clicking **Yes** recycles the agent with the new ping values. Clicking **No** lets the agent continue to run without the changes to the ping values. When the agent is restarted, the changes are implemented.

   Note: Non-integers (alphabetics, special characters, and alphanumerics) are not supported for the ping variables and might result in unexpected behavior of the Monitoring agent for Active Directory.

Configuring Active Directory logical view

You can configure the Active Directory logical view and assign it to the user.

Procedure

1. Open Tivoli Enterprise Portal, and log in as a system administrator.
2. In the Tivoli Enterprise Portal, open the Administer Users window, and select **SYSADMIN**.
3. In the Navigator View, click the arrow that assigns the Active Directory view to the user.

Environment variables for Event Log attributes

The **EVENT_LOG_LEVEL** and **EVENT_LOG_DURATION** environment variables are used to support the Event Log attributes.

The following environment variables are introduced in the agent to support the Event Log attributes:

- **EVENT_LOG_LEVEL**: This environment variable determines the level of details of the events that are logged by the Active Directory Server. This variable can have the following values:
  - ERROR
  - WARNING
  - AUDIT_FAILURE

  The default value of this variable is ERROR. If the value of this variable is WARNING, the warning and error logs that are related to the DNS server and the Directory services are displayed in the Event Logs workspace. If the value of this variable is AUDIT_ FAILURE, the audit failure, warning, and error logs that are related to the DNS server and the Directory services are displayed in the Event Logs workspace.
- **EVENT_LOG_DURATION**: This environment variable determines the number of days for which event logs are displayed in the Event Logs workspace. The value of this variable must be in the range 1 – 7. The default value of this variable is 1 day.

Environment variables for LDAP attributes

The **ADO_NUMBEROFOBJECTS_TIMEOUT**, **MAX_PASSWORD_AGE**, and **USER_INACTIVE_DAYS** environment variables are used to support the LDAP attributes.

The following environment variables are introduced for LDAP attributes:

- **ADO_NUMBEROFOBJECTS_TIMEOUT**: This environment variable is introduced for LDAP attributes. The default value of this variable is 1800 seconds. This variable helps you to restrict the time taken to collect data for the LDAP Attributes Object in Domain in the LDAP Attributes attribute group on a large network. You can set the value of this variable as per your requirement. The minimum value of this variable must be 1800 seconds.
- **MAX_PASSWORD_AGE**: This environment variable determines the number of days after which an account password expires if a user has not changed the password. The default value is 42 days. If the value of this variable is set to 0, it indicates that the password never expires.
- **USER_INACTIVE_DAYS**: This environment variable determines the number of days after which a user becomes inactive if the user has not logged in to the system. The value of this variable must be more than 15. You can disable this feature by specifying the value of this variable as 0. The default value is 0. If you specify a value that is more than 0 and less than 15, the value is automatically set to 15.

Environment variable for Organizational Units attributes

The **OU_INFORMATION_DURATION** environment variable is used to support the Organizational Units attributes.

The **OU_INFORMATION_DURATION** environment variable determines the number of days for which information about modified organizational units is displayed on the Tivoli Enterprise Portal. The value of this variable must be in the range 1 - 30. The default value of this variable is 1 day. If the value of this variable is 0, information about modified organizational units is not displayed on the Tivoli Enterprise Portal.

Environment variable for Replication Conflict Object attributes

The **ADO_CNFOBJ_CACHE_INTERVAL** environment variable is used to support the Replication Conflict Object attributes.

The **ADO_CNFOBJ_CACHE_INTERVAL** environment variable determines the duration (in minutes) after which the monitoring agent collects the list of replication conflict objects from the Active Directory Service Interfaces (ADSI). The value of this variable must be equal to or greater than 0. The value of this variable must be greater than or equal to 0. The default value of this variable is 30 minutes. If the value of this variable is 0, the replication conflict objects are not collected.

Environment variables for Sysvol replication

The **ADO_SYSVOL_FORCE_REPLICATION_FLAG**, **ADO_SYSVOL_REPLICATION_TEST_INTERVAL**, and **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL** environment variables are used to support Sysvol replication.

Sysvol replication can be performed between domain controllers in the same domain only. The Sysvol replication test is supported for the File Replication Service.

The following environment variables are introduced in the agent to support Sysvol replication:

- **ADO_SYSVOL_FORCE_REPLICATION_FLAG**: This environment variable determines whether the force replication that is initiated by the agent is enabled or disabled. The default value of this variable is TRUE. To disable force replication, change the value of this variable to FALSE.
- **ADO_SYSVOL_REPLICATION_TEST_INTERVAL**: This environment variable determines the time interval between two Sysvol replication tests. The Active Directory agent performs the Sysvol replication test at regular intervals only when the time interval is a positive integer.

- **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL**: This environment variable determines the amount of time that the agent waits to verify the results of Sysvol replication after completing the Sysvol replication test.

  The unit of time for the preceding environment variables is in minutes. The default value for both the environment variables is `0` minutes. However, if the value of the **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** variable is `0` minutes, the agent cannot complete the Sysvol replication test. The value of the **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** variable must be greater than the value of the **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL** variable.

  After the two environment variables are assigned valid values, the Active Directory agent creates one file on the `Sysvol` shared folder of the managed system and initializes forced Sysvol replication. This forced replication is initialized from the managed system to the `Sysvol` shared folders of the Sysvol replication partners. After verifying the results of the replication test, the agent removes the files that are created and replicated from the managed system and Sysvol replication partners.

Appendix. ITCAM for Microsoft Applications documentation library

Various publications are relevant to the use of ITCAM for Microsoft 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 Microsoft Applications Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamms.doc_6.3.1/welcome_msapps631.htm)

- Quick Start Guides
- 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 at the IBM Tivoli Monitoring Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp) to gain prerequisite knowledge:

- 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

Printed in USA

SC27-5659-00