Tivoli® Monitoring: Active Directory Agent

IBM

Version 6.2.0

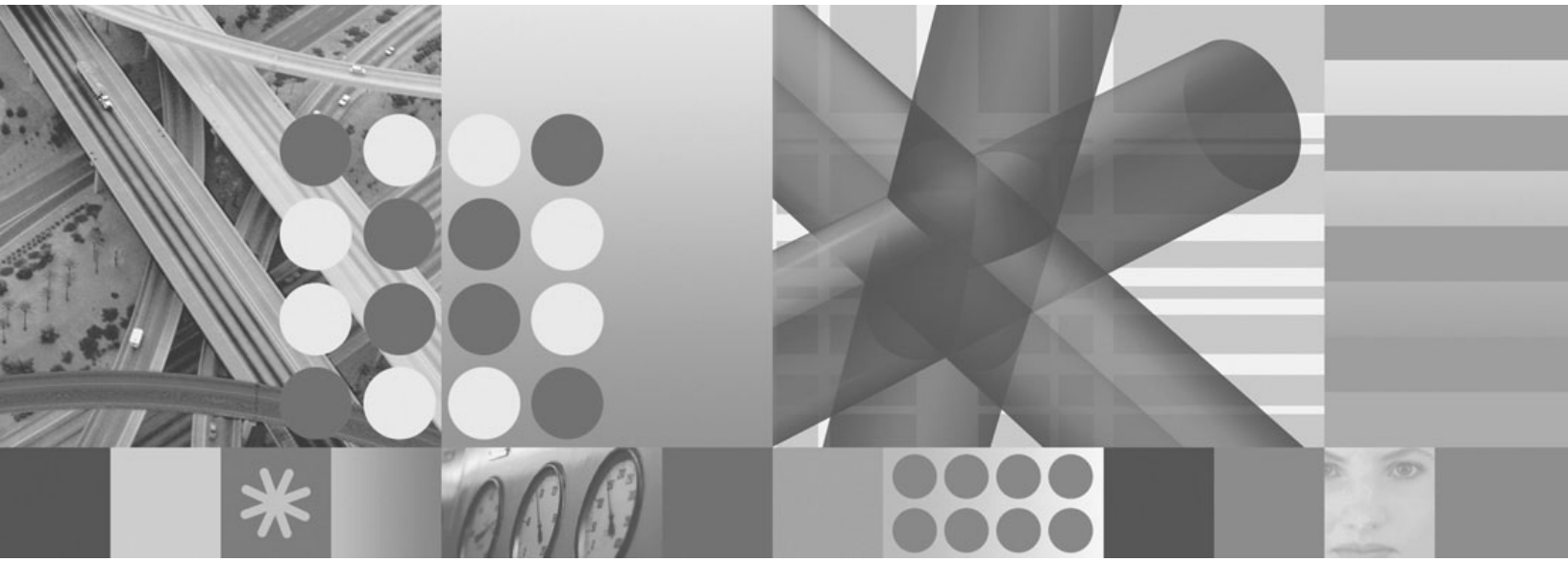
User's Guide

SC32-9444-01

Tivoli® Monitoring: Active Directory Agent

IBM

Version 6.2.0



User's Guide

SC32-9444-01

Note
Before using this information and the product it supports, read the information in "Notices" on page 121.

This edition applies to version 6.2 of IBM Tivoli Monitoring: Active Directory Agent (product number 5724-C71) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

Chapter 1. Overview of the Monitoring Agent for Active Directory

The Monitoring Agent for Active Directory provides you with the capability to monitor Windows servers with Active Directory Support. This chapter provides a description of the features, components, and interface options for the Monitoring Agent for Active Directory.

IBM Tivoli Monitoring overview

IBM Tivoli Monitoring is the base software for the Monitoring Agent for Active Directory. 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 do the following:

- 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 perform actions, schedule work, and automate manual tasks.

The Tivoli Enterprise Portal is the interface for IBM Tivoli Monitoring products. By providing a consolidated view of your environment, the Tivoli Enterprise Portal permits you to monitor and resolve performance issues throughout the enterprise.

See the IBM Tivoli Monitoring publications listed in Appendix E, “Documentation library,” on page 117 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

Features of the Monitoring Agent for Active Directory

The Monitoring Agent for Active Directory offers a central point of management for your Microsoft® Active Directory service. It provides a comprehensive means for gathering exactly the information you need to detect problems early and to prevent them. You can monitor many servers from a single workstation, and information is standardized across the system.

Use the Monitoring Agent for Active Directory to easily collect and analyze the following types of Active Directory-specific 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
- 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)

The Monitoring Agent for Active Directory provides the following benefits:

- 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 Monitoring Agent for Active Directory 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.

New in this release

For version 6.2 of the Monitoring Agent for Active Directory, the following enhancements have been made:

- Additional supported operating systems as listed in Chapter 2, "Requirements for the monitoring agent," on page 5
- Enablement of IBM® Tivoli® License Manager reporting
- New workspaces
  - Group Policy Objects
  - Lost and Found Objects
  - Replication Latency
  - Trusts
- New attribute groups
  - Group Policy Object
  - Lost and Found Objects
  - Replication Partner Latency
  - Trust
- Updated k3z.baroc file to support TEC event mapping
- Updated resource model mapping files

Note: These enhancements include ones made for the various IBM Tivoli Monitoring fix packs since the release of IBM Tivoli Monitoring 6.1.

Monitoring Agent for Active Directory components

After you install the Monitoring Agent for Active Directory (product code k3z or 3z) as directed in the *IBM Tivoli Monitoring Installation and Setup Guide*, you have an environment that contains the client, server, and monitoring agent implementation for IBM Tivoli Monitoring that contains the following components:

- Tivoli Enterprise Portal client with a Java-based user interface for viewing and monitoring your enterprise.
- Tivoli Enterprise Portal Server that is placed between the client and the Tivoli Enterprise Monitoring Server and enables retrieval, manipulation, and analysis of data from the monitoring agents.
- Tivoli Enterprise Monitoring Server, which acts as a collection and control point for alerts received from the monitoring agents, and collects their performance and availability data.
- Monitoring agent, Monitoring Agent for Active Directory, which collects and distributes data to a Tivoli Enterprise Monitoring Server.
- Operating system agents and application agents installed on the systems or subsystems you want to monitor. These agents collect and distribute data to the Tivoli Enterprise Monitoring Server.
- Tivoli Data Warehouse for storing historical data collected from agents in your environment. The data warehouse is located on a DB2®, Oracle, or Microsoft SQL database. To collect information to store in this database, you must install the Warehouse Proxy agent. To perform aggregation and pruning functions on the data, install the Warehouse Summarization and Pruning agent.
- 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. For more information, see *IBM Tivoli Monitoring Installation and Setup 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® workstation.

IBM Tivoli Enterprise Console
Event management application

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

Chapter 2. Requirements for the monitoring agent

This chapter contains information about the requirements for the Monitoring Agent for Active Directory.

In addition to the requirements described in the *IBM Tivoli Monitoring Installation and Setup Guide*, the Monitoring Agent for Active Directory has the requirements listed in Table 1.

Table 1. System requirements for the Monitoring Agent for Active Directory

Operating system	**Windows**
Operating system versions	• Windows 2000 Server (32-bit) • Windows 2000 Advanced Server (32-bit) • Windows Server 2003 Standard Edition (x86-32) • Windows Server 2003 Enterprise Edition (x86-32) • Windows Server 2003 Enterprise x64 Edition (x86-64)[1] • Windows Server 2003 R2 Standard Edition (x86-32) • Windows Server 2003 R2 Standard x64 Edition (x86-64)[1] • Windows Server 2003 R2 Enterprise Edition (x86-32) • Windows Server 2003 R2 Enterprise x64 Edition (x86-64)[1]
Memory	• 256 MB RAM • 512 MB virtual memory, plus 5 MB for each agent installed
Disk space	• 66 MB disk space for the monitoring agent • Historical data disk space: see “Disk capacity planning for historical data” on page 49

Table 1. System requirements for the Monitoring Agent for Active Directory (continued)

Operating system	**Windows**

Other requirements	• Windows Support Tools
	The latest Windows Support Tools package must be installed on the computers running the Active Directory agent. The Support Tools packages are available as downloads from the Microsoft web site. These latest versions are as follows:
	– Windows 2000: SP4
	`http://www.microsoft.com/windows2000/downloads/servicepacks/SP4/supporttools.asp`
	– Windows 2003: SP1
	`http://www.microsoft.com/downloads/details.aspx?familyid=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en`
	The Monitoring Agent for Active Directory requires that the iadstools.dll from the Support Tools be registered on the computer. If it is not, perform the following steps to register it.
	1. Go to the directory in which the Support Tools are installed. This is usually C:\Program Files\Support Tools.
	2. Run the command regsvr32 iadstools.dll. When this command completes, a pop-up window will say that the dll has been registered.
	Note: On Windows 2000, the Active Directory agent might report shutdown errors if the latest iadstools.dll file is not being used. The versions of iadstools.dll from SP4 is 1.0.0.2230. Earlier versions will cause the shutdown errors.
	• Microsoft database performance object for collection of Domain Controller Performance attribute values
	The database performance object is not installed by default with the Windows operating system. For information about installing the database performance object, go to the following Microsoft Web site:
	http://www.microsoft.com/technet/archive/windows2000serv/technologies/activedirectory/deploy/adguide/addeploy/addch09.mspx?mfr=true
	• For remote administration, the Monitoring Agent for Windows must be installed and running on the remote server. For more information, see the IBM Tivoli Monitoring Installation and Setup Guide.

Notes: 1. In toleration mode, not native 64-bit.	

Note: For the most current information about the operating systems that are supported, see the following URL:

`http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html`

When you get to that site, click **Tivoli platform and database support matrix link** at the bottom of the window.

Note: This monitoring agent is not designed to work in mixed Mode Active Directory environments.

Running as a non-Administrator user

To create a non-Administrator user and give it access to required registry paths, follow these steps:

- Create a new User ID with the authority - Domain Users, Users.
- Grant full access in the registry to HKEY_LOCAL_MACHINE\SOFTWARE\Candle *
- Grant read access in the registry to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

This is required for all Windows based agents to run as a Non-Admin ID.

Ping variables

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 2. Ping variables descriptions and default values

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

Turning ON/OFF caching during run time is done through Manage Tivoli Enterprise Monitoring Services (kinconfig.exe). The steps are as follows:

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 OFF caching, set the ADO_CACHE_INTERVAL to 0. To turn ON caching, set the ADO_CACHE_INTERVAL to any positive integer value. 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 turn off caching. Non-integers (alphabetics, special characters and alphanumerics) are not supported for the cache interval and might result in unexpected behavior of the Monitoring Agent for Active Directory. The suggested value for the cache interval is 4 minutes.

Caching configuration

When configuring caching, you can enable or disable caching and also set the cache interval. This is achieved by using an environment variable, ADO_CACHE_INTERVAL, in the environment file K3ZENV. The ADO_CACHE_INTERVAL environment variable not only acts as an ON/OFF flag, but the value given in seconds forms the caching interval (time interval between consecutive data collection). Any positive integer value turns ON the caching mechanism and a negative or zero value turns it OFF. With caching OFF the agent collects data on demand. By default caching is OFF.

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

Turning ON/OFF caching during run time is done through Manage Tivoli Enterprise Monitoring Services (kinconfig.exe). The steps are as follows:

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 OFF caching, set the ADO_CACHE_INTERVAL to 0. To turn ON caching, set the ADO_CACHE_INTERVAL to any positive integer value. 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 turn off caching. Non-integers (alphabetics, special characters and alphanumerics) are not supported for the cache interval and might result in unexpected behavior of the Monitoring Agent for Active Directory. The suggested value for the cache interval is 4 minutes.

Chapter 3. How to use a monitoring agent

After you have installed and configured a Tivoli Enterprise Monitoring Agent and the agent is running, you can begin using this agent to monitor your resources. The following sources of information are relevant to installation and configuration:

- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring Command Reference*
- Chapter 2, "Requirements for the monitoring agent" in the user's guide for the agent that you are installing and configuring

This chapter provides information about how to use a monitoring agent to perform the following tasks:

- "View real-time data that the agent collects"
- "Investigate an event" on page 10
- "Recover the operation of a resource" on page 10
- "Customize your monitoring environment" on page 11
- "Monitor with custom situations that meet your requirements" on page 12
- "Collect and view historical data" on page 13

For each of these tasks, there is a list of procedures that you perform to complete the task. For the tasks, there is a cross-reference to where you can find information about performing that procedure. Information about the procedures is located in subsequent chapters of this user's guide and in the following publications:

- *IBM Tivoli Monitoring User's Guide*
- *IBM Tivoli Monitoring Administrator's Guide*

View real-time data that the agent collects

After you install, configure, and start the Tivoli Enterprise Monitoring Agent, the agent begins monitoring.

Table 3 contains a list of the procedures for viewing the real-time data that the monitoring agent collects through the predefined situations. The table also contains a cross-reference to where you can find information about each procedure.

Table 3. View real-time data

Procedure	Where to find information
View the hierarchy of your monitored resources from a system point of view (Navigator view organized by operating system type, monitoring agents, and workspaces).	*IBM Tivoli Monitoring User's Guide:* ″Navigating through workspaces″ (in ″Monitoring: real-time and event-based″ chapter)
View the indicators of real or potential problems with the monitored resources (Navigator view).	

Table 3. View real-time data (continued)

Procedure	Where to find information
View changes in the status of the resources that are being monitored (Enterprise Message Log view).	*IBM Tivoli Monitoring User's Guide:* "Using workspaces" (in "Monitoring: real-time and event-based" chapter) Chapter 4, "Workspaces reference," on page 15 in this guide
View the number of times an event has been opened for a situation during the past 24 hours (Open Situations Account view).	*IBM Tivoli Monitoring User's Guide:* "Using workspaces" (in "Monitoring: real-time and event-based" chapter) Chapter 4, "Workspaces reference," on page 15 in this guide Chapter 6, "Situations reference," on page 51 in this guide
Manipulate the views in a workspace.	*IBM Tivoli Monitoring User's Guide:* "Using views" (in "Monitoring: real-time and event-based" chapter)

Investigate an event

When the conditions of a situation have been met, an event indicator is displayed in the Navigator. When an event occurs, you want to obtain information about that event so you can correct the conditions and keep your enterprise running smoothly.

Table 4 contains a list of the procedures for investigating an event and a cross-reference to where you can find information about each procedure.

Table 4. Investigating an event

Procedure	Where to find information
Determine which situation raised the event and identify the attributes that have values that are contributing to the alert.	*IBM Tivoli Monitoring User's Guide:* "Opening the situation event workspace" (in "Monitoring: real-time and event-based" chapter, "Responding to alerts" section)
Review available advice.	Chapter 4, "Workspaces reference," on page 15 in this guide
Notify other users that you have taken ownership of the problem related to an event and are working on it.	*IBM Tivoli Monitoring User's Guide:* "Acknowledging a situation event" (in "Monitoring: real-time and event-based" chapter, "Responding to alerts" section)
Remove the event from the Navigator.	*IBM Tivoli Monitoring User's Guide:* "Closing the situation event workspace" (in "Monitoring: real-time and event-based" chapter, "Responding to alerts" section)

Recover the operation of a resource

When you find out that a resource is not operating as desired, you can control it manually or automatically using Take Action commands.

Table 5 contains a list of the procedures for recovering the operation of a resource and a cross-reference to where you can find information about each procedure.

Table 5. Recover the operation of a resource

Procedure	Where to find information
Take an action on a resource manually.	*IBM Tivoli Monitoring User's Guide:* • ″Other views″ (in ″Custom workspaces″ chapter, ″Workspace views″ section) • ″Take action: Reflex automation″ (in Situations for event-based monitoring″ chapter, ″Event-based monitoring overview″ section) • "Take action" (in "Designing customized responses" chapter) Chapter 7, “Take Action commands reference,” on page 69 in this guide
Take an action on a system condition automatically by setting up a situation to run a Take Action command.	*IBM Tivoli Monitoring User's Guide:* ″Situations for event-based monitoring″ chapter • ″Customize a situation″ • ″Create a situation″ • ″Specify an action to take″ • ″Distribute the situation″ Chapter 7, “Take Action commands reference,” on page 69 in this guide
Take multiple actions on system conditions automatically using a policy.	*IBM Tivoli Monitoring User's Guide:* ″Policies for automation″ chapter • ″Creating a policy″ • ″Maintaining policies″ • ″Workflows window″ Chapter 8, “Policies reference,” on page 71 in this guide
Take actions across systems, agents, or computers using a policy.	

Customize your monitoring environment

You can change how your monitoring environment looks by creating new workspaces with one or more views in it.

Table 6 contains a list of the procedures for customizing your monitoring environment and a cross-reference to where you can find information about each procedure.

Table 6. Customizing your monitoring environment

Procedure	Where to find information
Display data in tables or charts (views) in the Tivoli Enterprise Portal.	*IBM Tivoli Monitoring User's Guide:* • ″Custom workspaces″ • ″Table and chart views″

Table 6. Customizing your monitoring environment (continued)

Procedure	Where to find information
Display an overview of changes in the status of situations for your monitored resources (Message Log View).	*IBM Tivoli Monitoring User's Guide:* "Message log view" (in "Situation event views: message log, situation event console and graphic" chapter)
Specify which attributes to retrieve for a table or chart so you can retrieve only the data you want by creating custom queries.	*IBM Tivoli Monitoring User's Guide:* "Creating custom queries" (in "Table and chart views" chapter) Chapter 5, "Attributes reference," on page 21 in this guide
Build links from one workspace to another.	*IBM Tivoli Monitoring User's Guide:* • "Link from a workspace" (in "Custom workspaces" chapter) • "Link from a table or chart" (in "Table and chart views" chapter)
Identify which predefined situations started running automatically when you started the Tivoli Enterprise Monitoring Server.	*IBM Tivoli Monitoring User's Guide:* "What the enterprise workspace shows" (in "Monitoring: real-time and event-based" chapter, "Using workspaces" section) Chapter 6, "Situations reference," on page 51 in this guide
Determine whether to run situations as defined, modify the values in situations, or create new situations to detect possible problems.	Chapter 6, "Situations reference," on page 51 in this guide

Monitor with custom situations that meet your requirements

When your environment requires situations with values that are different from those in the existing situations, or when you need to monitor conditions not defined by the existing situations, you can create custom situations to detect problems with resources by creating an entirely new situation.

You can specify the following information for a situation:

- Name
- Attribute group and attributes
- Qualification to evaluate multiple rows when a situation has a multiple-row attribute group (display item)
- Formula
- Take Action commands
- Run at startup
- Sampling interval
- Persistence
- Manual or automatic start
- Severity
- Clearing conditions
- Expert Advice
- When a true situation closes

- Available Managed Systems

Table 7 contains a list of the procedures for monitoring your resources with custom situations that meet your requirements and a cross-reference to where you can find information about each procedure.

Table 7. Monitor with custom situations

Procedure	Where to find information
Create an entirely new situation.	*IBM Tivoli Monitoring User's Guide:* "Creating a new situation" (in "Situations for event-based monitoring" chapter, "Creating a situation" section) Chapter 5, "Attributes reference," on page 21 in this guide
Run a situation on a managed system.	*IBM Tivoli Monitoring User's Guide:* "Situations for event-based monitoring" chapter • "Associating situations with navigator items" • "Distribute the situation" (in "Customizing a situation" section) • "Starting, stopping or deleting a situation"

Collect and view historical data

When you collect historical data, you specify the following configuration requirements:

- Attribute groups for which to collect data
- Collection interval
- Summarization and pruning of attribute groups
- Roll-off interval to a data warehouse, if any
- Where to store the collected data (at the agent or the Tivoli Enterprise Management Server)

Table 8 contains a list of the procedures for collecting and viewing historical data and a cross-reference to where you can find information about each procedure.

Table 8. Collect and view historical data

Procedure	Where to find information
Configure and start collecting short-term data (24 hours).	*IBM Tivoli Monitoring User's Guide:* "Historical reporting" (in "Table and chart views" chapter) *IBM Tivoli Monitoring Administrator's Guide* "Disk capacity planning for historical data" on page 49 in this guide
Configure and start collecting longer-term data (more than 24 hours).	
View historical data in the Tivoli Enterprise Portal.	
Create reports from historical data using third-party reporting tools.	
Filter out unwanted data to see specific areas of interest.	

Chapter 4. Workspaces reference

This chapter contains an overview of workspaces, references for detailed information about workspaces, and descriptions of the predefined workspaces included in this monitoring agent.

About workspaces

A workspace is the working area of the Tivoli Enterprise Portal application window. At the left of the workspace is a Navigator that you use to select the workspace you want to see.

As you select items in the Navigator, the workspace presents views pertinent to your selection. Each workspace has at least one view. Some views have links to workspaces. Every workspace has a set of properties associated with it.

This monitoring agent provides predefined workspaces. You cannot modify the predefined workspaces, but you can create new workspaces by editing them and saving the changes with a different name.

Based on the information that the workspaces provide, you can make changes, set up situations, and verify that your changes improve performance.

More information about workspaces

For more information about creating, customizing, and working with workspaces, see the *IBM Tivoli Monitoring User's Guide*.

For a list of the predefined workspaces for this monitoring agent and a description of each workspace, refer to the Predefined workspaces section below and the information in that section for each individual workspace.

Predefined workspaces

The Monitoring Agent for Active Directory provides the following predefined workspaces, which are organized by Navigator item:

- Active Directory
- Address Book
- DHCP
- Directory System Agent
- DNS
- DNS ADIntegrated
- Domain Controller Availability
- Domain Controller Performance
- Exchange Directory Service
- File Replication Service
- Group Policy Object
- Kerberos Key Distribution Center
- Knowledge Consistency Checker

- Lightweight Directory Access Protocol
- Local Security Authority
- Lost and Found Objects
- Name Service Provider
- Replication
  - Historical
  - Replication
- Replication Latency
- Replication Partner
- Security Accounts Manager
- Trust

Some predefined workspaces are not available from the Navigator tree item, but are accessed by selecting the link indicator next to a row of data in a view. Left-clicking a link indicator selects the default workspace associated with that link. Right-clicking a link indicator displays all linked workspaces that can be selected.

Active Directory workspace

The Active Directory workspace provides a view of the servers and their availability and a summary of the replication topology. This workspace includes the following views:

- FSMO Role Servers table
- FSMO Server Availability table
- Replication Partner Details table

Address Book workspace

The Address Book workspace displays addressing information from all of the address book providers in the profile. This workspace includes the following views:

- Address Book chart
- Address Book Details table

DHCP workspace

The DHCP workspace monitors the performance and general functioning of the Dynamic Host Configuration Protocol (DHCP) server. This workspace includes the following views:

- Circular Gauge, which includes the following gauges: DHCP Acks Sec % Increase and DHCP Requests Sec % Increase
- DHCP Details table

Directory System Agent workspace

The Directory System Agent workspace provides access to the physical storage data for the Active Directory service. This workspace includes the following views:

- Directory System Agent chart
- Directory System Agent Details table

DNS workspace

The DNS workspace monitors the activity and performance of the Domain Name System (DNS) server in general and of the DNS service in particular. It monitors the following items:

- DNS Response Time chart
- DNS Details table

DNS ADIntegrated workspace

When the DNS server runs on a domain controller that domain controller stores a copy of the corresponding DNS zone. Domain controllers can register one or more DNS records in the Active Directory. These entries are Service Location Records (SRV) that are used to identify services that are available on a host. The DNS ADIntegrated workspace monitors the server under investigation and sends an alert if any SRV is inaccurate or missing.

This workspace includes the following views:

- DNS ADIntegrated Details table
- DNS SRV Records Bad chart
- DNS SRV Records Missing chart

Domain Controller Availability workspace

The Domain Controller Availability workspace monitors the availability and stability of key domain controller services. This workspace includes the following views:

- Domain Controller Availability Details table
- FSMO Role Servers table
- FSMO Server Availability table

Domain Controller Performance workspace

The Domain Controller Performance workspace retrieves statistical information about Active Directory.

This workspace includes the following views:

- Domain Controller Performance Details table
- Cache Percent Hit chart
- File Operations Rate chart

Exchange Directory Service workspace

The Exchange Directory Service workspace provides information relate to Microsoft Exchange Server environment. This workspace includes the following views:

- Exchange Directory Service chart
- Exchange Directory Service Details table

File Replication workspace

The File Replication workspace monitors the performance of the File Replication Service (FRS). This workspace includes the following views:

- File Replication Service Details table
- FRS Change Orders chart

Group Policy Object workspace

The Group Policy Object workspace monitors Active Directory Group Policy Objects. This workspace includes the following views:

- Group Policy Objects
- Group Policy Objects Details

Kerberos Key Distribution Center workspace

The Kerberos Key Distribution Center workspace monitors session tickets and temporary session keys used in the Kerberos V5 authentication protocol. This workspace includes the following views:

- Kerberos Key Distribution Center chart
- Kerberos Key Distribution Center table

Knowledge Consistency Checker workspace

The Knowledge Consistency Checker workspace displays data associated with generating the replication topology between domain controllers. This workspace includes the following views:

- Knowledge Consistency Checker chart
- Knowledge Consistency Checker table

Lightweight Directory Access Protocol workspace

The Lightweight Directory Access Protocol (LDAP) workspace monitors the LDAP service that provides access to data and objects in a directory or network environment. This workspace includes the following views:

- LDAP chart
- LDAP table

Local Security Authority workspace

The Local Security Authority workspace monitors built-in logon authentication and user authorization for the local system. This workspace includes the following views:

- Local Security Authority chart
- Local Security Authority table

Lost and Found Objects workspace

The Lost and Found Objects workspace monitors Active Directory Lost and Found Objects. Use Replication Latency attributes to create objects on the system found in the Lost and Found workspace. The Lost and Found Objects workspace shows the Replication Latency 'Test' object if the Replication Latency workspace is selected prior to selecting the Lost and Found Objects workspace. This workspace includes the following views:

- LostandFound Objects

Name Service Provider workspace

The Name Service Provider workspace monitors communication between the Active Directory and Exchange Directory Service (XDS). This workspace includes the following views:

- Name Server Provider chart
- Name Service Provider table

Replication workspaces

This section describes the workspaces related to the Replication Navigator item.

Historical workspace

The Historical workspace is an historical view of Replication data over time. Use this workspace to see the volume of replication activity in a 24-hour period.

This workspace includes the following views:

- Bytes Total per Second
- Replication Details

Replication workspace

The Replication workspace monitors synchronization of Active Directory partition replicas between domain controllers. This workspace includes the following views:

- Replication bar chart
- Replication Bytes Traffic bar chart
- Replication Details
- Replication Inbound Details table
- Replication Outbound Details table
- USN Details table view

Replication Latency workspace

The Replication Latency workspace monitors replication latency for each replication partner. The latency is confirmed, tested, and monitored by creating a LostAndFound object that is monitored with its time stamps for the replication latency time. This workspace includes the following views:

- Replication Latency chart
- Replication Latency Details

Replication Partner workspace

The Replication Partner workspace monitors the intrasite replication process, the intersite replication process, and the efficiency of the Active Directory replication process. This workspace includes the following views:

- Replication Partner Details table
- Number Replication Failures bar chart
- Replication Health table

Security Accounts Manager workspace

The Security Accounts Manager workspace monitors the Security Accounts Manager (SAM), which maintains user account information, including groups to which a user belongs. This workspace includes the following views:

- Security Accounts Manager chart
- Security Accounts Manager table

Trust workspace

The Trust workspace monitors Active Directory trusts. This workspace includes the following views:

- Trusts
- Trusts Details

Chapter 5. Attributes reference

This chapter contains information about the following topics:

- Overview of attributes
- References for detailed information about attributes
- Descriptions of the attributes for each attribute group included in this monitoring agent
- Disk space requirements for historical data

About attributes

Attributes are the application properties being measured and reported by the Monitoring Agent for Active Directory, such as the amount of memory usage or the message ID.

Attributes are organized into groups according to their purpose. The attributes in a group can be used in the following two ways:

- Chart or table views

  Attributes are displayed in chart and table views. The chart and table views use queries to specify which attribute values to request from a monitoring agent. You use the Query editor to create a new query, modify an existing query, or apply filters and set styles to define the content and appearance of a view based on an existing query.
- Situations

  You use attributes to create situations that monitor the state of your operating system, database, or application. A situation describes a condition you want to test. When you start a situation, the Tivoli Enterprise Portal compares the values you have assigned to the situation attributes with the values collected by the Monitoring Agent for Active Directory and registers an *event* if the condition is met. You are alerted to events by indicator icons that appear in the Navigator.

More information about attributes

For more information about using attributes and attribute groups, see the *IBM Tivoli Monitoring User's Guide*.

For a list of the attributes groups, a list of the attributes in each attribute group, and descriptions of the attributes for this monitoring agent, refer to the Attribute groups and attributes section in this chapter.

Attribute groups and attributes for the Monitoring Agent for Active Directory

The following attribute groups are included:

The following sections contain descriptions of these attribute groups, which are listed alphabetically. Each description contains a list of attributes in the attribute group.

IBM Tivoli Monitoring provides other attribute groups that are available to all monitoring agents, for example Universal Time and Local Time. The attributes in these common attribute groups are documented in the Tivoli Enterprise Portal Help.

Address Book attributes

Use the Address Book attributes to create situations to monitor address book clients.

AB Browses per second Rate at which Address Book clients perform browse operations. An integer is a valid entry.

AB Client Sessions Number of connected address book client sessions. An integer is a valid entry.

AB Matches per second Rate at which address book clients perform find operations. An integer is a valid entry.

AB Property Reads per second Rate at which address book clients perform property read operations. An integer is a valid entry.

AB Proxy Lookups per second Rate at which the proxy clients perform search operations. An integer is a valid entry.

AB Searches per second Rate at which address book clients perform key search operations. An integer is a valid entry.

AB Ambiguous Name Resolutions per second Rate at which the Address Book clients perform Ambiguous Name Resolutions (ANR) operations. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

DHCP attributes

The DHCP attributes display DHCP information.

DHCP Acks sec percent increase Percent increase in DHCP Acks per second. Attributes based on previous values are valid for situations only.

DHCP Active Queue Length Active queue length.

DHCP Conflict Check Queue Length DHCP length of Conflict Check queue.

DHCP Declines Sec DHCP declines per second.

DHCP Duplicates Dropped Sec DHCP duplicates dropped per second.

DHCP Nacks Sec DHCP Nacks per second.

DHCP Packets Expired Sec DHCP packets expired per second.

DHCP Requests sec percent increase The percent increase in DHCP requests per second. Attributes based on previous values are valid for situations only.

DHCP Server Specifies whether this server is a DHCP server. Valid values include TRUE and FALSE.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Directory Services attributes

Use the Directory Services attributes to create situations to monitor the directory service agent (DSA), the Active Directory process that runs on each domain controller and manages all the directory service functions.

DS Client Binds per second The number of ntdsapi(dot)dll binds per second serviced by this domain controller. An integer is a valid entry.

DS Client Name Translations per second The number of ntdsapi(dot)dll name translations per second serviced by this domain controller. An integer is a valid entry.

DS Directory Reads per second The number of directory reads per second. An integer is a valid entry.

DS Directory Searches per second The number of directory searches per second. An integer is a valid entry.

DS Directory Writes per second The number of directory writes per second. An integer is a valid entry.

DS Monitor List Size The number of requests to be notified when objects that are currently registered with this directory service agent (DSA) are updated. An integer is a valid entry.

DS Name Cache Hit Rate The percentage of directory object name component lookups that are satisfied out of the directory service agent (DSA) name cache. An integer is a valid entry.

DS Notify Queue Size The number of pending update notifications that are queued but not yet transmitted to clients. An integer is a valid entry.

DS Other Reads The percentage of directory reads that do not come from SAM, DRA, LDAP, LSA, XDS, KCC or NSPI. An integer is a valid entry.

DS Other Searches The percentage of directory searches that do not come from SAM, DRA, LDAP, LSA, XDS, KCC or NSPI. An integer is a valid entry.

DS Other Writes The percentage of directory writes that do not come from SAM, DRA, LDAP, LSA, XDS, KCC or NSPI. An integer is a valid entry.

DS Search Suboperations per second The number of search suboperations per second. An integer is a valid entry.

DS Security Descriptor Propagations per second The number of security descriptor propagations events that are queued, but not yet processed. An integer is a valid entry.

DS Security Descriptor Propagator Average Exclusion Time The average length of time that the security descriptor propagator spends waiting for exclusive access to database elements. An integer is a valid entry.

DS Security Descriptor Propagator Runtime Queue The number of objects that remain to be examined while the current directory service security descriptor propagator event is being processed. An integer is a valid entry.

DS Security Descriptor Sub-operations per second The number of security descriptor propagation suboperations per second. An integer is a valid entry.

DS Server Binds per second The number of domain controller to domain controller binds per second that are serviced by this domain controller. An integer is a valid entry.

DS Server Name Translations per second The number of domain controller to domain controller name translations per second that are serviced by this domain controller. An integer is a valid entry.

DS Threads in Use The current number of threads that the directory service is using. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where

the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

DNS_ADIntegrated attributes

The DNS_ADIntegrated attributes display DNS information that is specifically related to AD. This attribute group has the option to cache the data it collects for some configurable period.

DAI Bad DC A domain controller in the local SRV record is invalid.

DAI Bad GC A global catalog in the local SRV record is invalid.

DAI Bad PDC A primary domain controller in the local SRV record is invalid.

DAI DC SRV Records Bad The number of invalid DC records in SRV.

DAI DC SRV Records Missing The number of DC records that are missing from SRV.

DAI Domain The default domain that is associated with this server.

DAI Forest Name The forest that is associated with this server.

DAI GC SRV Records Bad The number of invalid GC records in SRV.

DAI GC SRV Records Missing The number of GC records that are missing from SRV.

DAI Host Name The host name for this server.

DAI Missing DC A domain controller is missing from the local SRV record.

DAI Missing GC A global catalog is missing from the local SRV record.

DAI Missing Node Rec A node record is missing from the local SRV record.

DAI Missing PDC A primary domain controller is missing from the local SRV record.

DAI Node Records Missing The number of SRV records in the DNS server that are missing.

DAI PDC SRV Records Bad The number of invalid PDC records in SRV.

DAI PDC SRV Records Missing The number of PDC records that are missing from SRV.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

DNS attributes

The DNS attributes display DNS information.

DNS Caching Memory DNS caching memory.

DNS Dynamic Update Failures Pct The percent of dynamic update failures compared to total dynamic updates. Attributes based on previous values are valid for situations only.

DNS Dynamic Update Queued DNS dynamic updates that are queued.

DNS Dynamic Update Received DNS dynamic updates that were received.

DNS Dynamic Update Received Delta DNS dynamic updates that were received since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Dynamic Update Received sec DNS dynamic updates that were received per second.

DNS Dynamic Update Rejected DNS dynamic updates that were rejected.

DNS Dynamic Update Rejected Delta DNS dynamic updates that were rejected since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Dynamic Update Rejected Pct Percent of rejected DNS dynamic updates of dynamic updates received. Attributes based on previous values are valid for situations only.

DNS Dynamic Update Timeouts DNS dynamic updates timeouts.

DNS Dynamic Update Timeouts Delta DNS dynamic update timeouts since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Dynamic Update Timeouts Pct Percent of DNS dynamic update timeouts of dynamic updates received. Attributes based on previous values are valid for situations only.

DNS Server Specifies whether this is a DNS server. Valid values include TRUE and FALSE.

DNS Response Time DNS response time.

DNS Total Query Received Delta DNS total queries that were received since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Total Query Received DNS total queries that were received.

DNS Total Query Received sec DNS total queries that were received per second.

DNS Total Response Sent DNS total response that were sent.

DNS Total Response Sent Delta DNS total responses that were sent since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Total Response Sent sec DNS total responses that were sent per second.

DNS Transfer Failures Percent The percent of transfer failures compared to total transfers. Attributes based on previous values are valid for situations only.

DNS Zone Transfer Failure DNS zone transfer failures.

DNS Zone Transfer Failure Delta DNS zone transfers that failed since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Zone Transfer Request Received DNS zone transfer requests received.

DNS Zone Transfer Request Received Delta DNS zone transfer requests that were received since the last poll was taken. Attributes based on previous values are valid for situations only.

DNS Zone Transfer Success Successful DNS zone transfers.

DNS Zone Transfer Success Delta Successful DNS zone transfers since the last poll was taken. Attributes based on previous values are valid for situations only.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Domain Controller Availability attributes

The Domain Controller Availability attributes display domain controller availability information. This attribute group has the option to cache the data it collects for some configurable period.

DCA Domain Name Default domain name associated with this server.

DCA Domain Naming Master The defined Domain Naming Master.

DCA Forest Name Forest name associated with this server.

DCA FSMO Role The FSMO role, if any, for the current DC. Valid values include Domain Naming, RID Pool, Infrastructure, Schema, PDC, and none.

DCA GCs The defined number of Global Catalog servers.

DCA GCs In Site The number of Global Catalog servers defined in the local site.

DCA GCs In Site Pinged The number of pinged Global Catalog servers in the local site.

DCA GCs Pinged The number of pinged Global Catalog servers.

DCA Hostname Host name for this server.

DCA Infrastructure Master The defined Infrastructure Master.

DCA PDC Master The defined PDC Master.

DCA Ping Domain Naming Master The ping time for Domain Naming Master. Note: -1 indicates Unavailable and -2 indicates Timed Out.

DCA Ping Infrastructure Master The ping time for Infrastructure Master. Note: -1 indicates Unavailable and -2 indicates Timed Out.

DCA Ping PDC Master The ping time for PDC Master. Note: -1 indicates Unavailable and -2 indicates Timed Out.

DCA Ping RID Master The ping time for RID Master. Note: -1 indicates Unavailable and -2 indicates Timed Out.

DCA Ping Schema Master The ping time for Schema Master. Note: -1 indicates Unavailable and -2 indicates Timed Out.

DCA Previous RID Master The previously defined RID Master. Attributes based on previous values are valid for situations only.

DCA Previous Domain Naming Master The previously defined Domain Naming Master. Attributes based on previous values are valid for situations only.

DCA Previous Infrastructure Master The previously defined Infrastructure Master. Attributes based on previous values are valid for situations only.

DCA Previous Schema Master The previously defined Schema Master. Attributes based on previous values are valid for situations only.

DCA Previous PDC Master The previously defined PDC Master. Attributes based on previous values are valid for situations only.

DCA Repl Partners The assigned number of replication partners.

DCA Repl Partners Pinged The pinged number of replication partners.

DCA RID Master The defined RID Master.

DCA Schema Master The defined Schema Master.

DCA Site Name The local site name.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century

YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Domain Controller Performance attributes

The Domain Controller Performance attributes display domain controller performance information. This attribute group has the option to cache the data it collects for some configurable period.

DCP Cache Pct Hit The percent of cache hits compared to total cache requests.

DCP Cache Page Fault Stalls Sec The number of page faults per second that cannot be serviced because pages are not available for allocation from the database cache.

DCP Cache Page Faults Sec The rate of cache page faults, per second.

DCP DSA Connections The number of directory service agent (DSA) Connections.

DCP File Bytes Read Sec The rate of file bytes read, per second. A value of -1 indicates Undefined.

DCP File Bytes Written Sec The rate of file bytes written, per second. A value of -1 indicates Undefined.

DCP File Operations Sec The rate of file operations, per second. A value of -1 indicates Undefined.

DCP KB Cache Size The size in KB of schema cache.

DCP Log Record Stalls Sec The rate of log record stalls, per second.

DCP Log Threads Waiting The number of Log Threads Waiting for log access.

DCP Table Open Cache Hits Sec The rate of database tables that were opened using cached schema information, per second.

DCP Table Open Cache Misses Sec The rate of database tables that were opened not using cached schema information, per second.

DCP Table Open Cache Pct Hit The percent of database tables that were opened using cached schema information.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Exchange Directory Services attributes

Use the Exchange Directory Services attributes to create situations to monitor exchange directory related metrics.

XDS Client Sessions The number of connected XDS client sessions. An integer is a valid entry.

XDS Reads The percentage of directory reads from XDS. An integer is a valid entry.

XDS Searches The percentage of directory searches from XDS. An integer is a valid entry.

XDS Writes The percentage of directory writes from XDS. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

File Replication Service attributes

The File Replication Service attributes display file replication service information.

FRS Change Orders Aborted The number of ended change orders.

FRS Change Orders Aborted Percent The percent of ended change orders.

FRS Change Orders Evaporated The number of evaporated change orders.

FRS Change Orders Evaporated Percent The percent of evaporated change orders.

FRS Change Orders Morphed The number of morphed change orders.

FRS Change Orders Morphed Percent The percent of morphed change orders.

FRS Change Orders Retired The number of retired change orders.

FRS Change Orders Retired Percent The percent of retired change orders.

FRS Change Orders Received The number of received change orders.

FRS Change Orders Sent The number of change orders that were sent.

FRS DS Bindings The number of DS bindings.

FRS DS Bindings In Error The number of incorrect DS bindings.

FRS DS Bindings In Error Percent The percent of incorrect DS bindings.

FRS Files Installed The number of installed files.

FRS Files Installed With Error The number of files that were incorrectly installed.

FRS Files Installed With Error Percent The percent of files that were incorrectly installed.

FRS KB Staging Space Free Staging space free (KB).

FRS KB Staging Space In Use Staging space in use (KB).

FRS Packets Received The number of received packets.

FRS Packets Received In Error The number of packets received in error.

FRS Packets Received In Error Percent The percent of packets received in error.

FRS Packets Sent The number of packets that were sent.

FRS Packets Sent In Error The number of packets that were sent in error.

FRS Packets Sent In Error Percent The percent of packets that were sent in error.

FRS Usn Records Accepted The number of USN records that were accepted.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Group Policy Object attributes

Use the Group Policy Object attributes to display Active Directory Group Policy Object information.

GPO Name The Group Policy Object name.

GPO GUID The Group Policy Object GUID.

GPO Sysvol_Version The version number for the GPO from Sysvol record.

GPO Version The version number for the GPO.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Kerberos Key Distribution Center attributes

Use the Kerberos Key Distribution Center attributes to display Key Distribution Center information.

KDC Authentication Server Request The percentage of authentication server requests serviced by the KDC per second. An integer is a valid entry.

KDC Authentications The number of times per second that clients use a ticket to this domain controller to authenticate to this domain controller. An integer is a valid entry.

KDC TGS Requests The number of ticket generation (TGS) requests services by the KDC per second. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year

MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Knowledge Consistency Checker attributes

Use the Knowledge Consistency Checker attributes to create situations to monitor knowledge consistency checker metrics.

KCC Reads The percentage of directory reads from KCC. An integer is a valid entry.

KCC Searches The percentage of directory searches from KCC. An integer is a valid entry.

KCC Writes The percentage of directory writes from KCC. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Lightweight Directory Access Protocol attributes

The NTDS LDAP object provides statistics about the Lightweight Directory Access Protocol (LDAP) interface that provides the API for LDAP clients and exposes the Active Directory Services Interface (ADSI) so that additional applications might be written that can talk to Active Directory.

LDAP Active Threads The current number of threads that the LDAP subsystem of the local directory service is using. An integer is a valid entry.

LDAP Bind Time The time, in milliseconds, taken for the last successful LDAP bind. An integer is a valid entry.

LDAP Client Sessions The number of currently connected LDAP client sessions. An integer is a valid entry.

LDAP Searches The percentage of directory searches from LDAP. An integer is a valid entry.

LDAP Searches per second The rate at which LDAP clients perform search operations. An integer is a valid entry.

LDAP Successful Binds The percentage of LDAP bind attempts that are successful. An integer is a valid entry.

LDAP Successful Binds per second The number of LDAP binds per second. An integer is a valid entry.

LDAP UDP Operations per second The number of UDP operations that the LDAP server is processing per second. An integer is a valid entry.

LDAP Writes The percentage of directory writes from LDAP. An integer is a valid entry.

LDAP Writes per second The rate at which LDAP clients perform write operations. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour

MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Local Security Authority attributes

Use the Local Security Authority attributes to create situations to monitor the AD Local Security Authority.

LSA Reads The percentage of directory reads from LSA. An integer is a valid entry.

LSA Searches The percentage of directory searches from LSA. An integer is a valid entry.

LSA Writes The percentage of directory writes from LSA. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Lost and Found Objects attributes

Use the Lost and Found Objects attributes to display Active Directory Lost and Found Objects.

LFO Name The Lost and Found Object name.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Name Service Provider attributes

Use the Name Service Provider attributes to create situations to monitor statistics of the Name Service Provider Interface (NSPI), which facilitates communication between Active Directory and Exchange Directory Service (XDS).

NSPI Reads The percentage of directory reads from NSPI. An integer is a valid entry.

NSPI Searches The percentage of directory searches from NSPI. An integer is a valid entry.

NSPI Writes The percentage of directory writes from NSPI. An integer is a valid entry.

NTLM Authentications The number of NTLM authentications per second served by this domain controller. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Replication attributes

Use the Replication attributes to create situations to monitor the directory service agent (DSA), the Active Directory process that runs on each domain controller and manages all the directory service functions. This attribute group has the option to cache the data it collects for some configurable period.

DRA Bridgehead Specifies whether this system is a Bridgehead server. Valid values include TRUE and FALSE.

DRA High USN Committed High The high-order 32 bits of the highest update sequence number committed on the directory service agent (DSA). An integer is a valid entry.

DRA High USN Committed Low The low-order 32 bits of the highest update sequence number committed on the directory service agent (DSA). An integer is a valid entry.

DRA High USN Issued High The high-order 32 bits of the highest USN issued on the directory service agent (DSA). An integer is a valid entry.

DRA High USN Issued Low The low-order 32 bits of the highest USN issued on the directory service agent (DSA). An integer is a valid entry.

DRA Hostname Host name for this server.

DRA Inbound Bytes Compressed per second Before The compressed size of inbound compressed replication data, before compression. An integer is a valid entry.

DRA Inbound Bytes Compressed per second After The compressed size of inbound compressed replication data, after compression. An integer is a valid entry.

DRA Inbound Bytes Intersite Percent The percentage of inbound bytes from other sites.

DRA Inbound Bytes Not Compressed per second The number of incoming replicated bytes that were not compressed at the source. An integer is a valid entry.

DRA Inbound Bytes Total per second The total number of replicated bytes. An integer is a valid entry.

DRA Inbound Full Synch Objects Remain The number of objects remaining until the full synchronization is completed. An integer is a valid entry.

DRA Inbound Objects Update Remain Packet The number of object updates received in the current directory replication update packet that have not yet been applied to the local server. An integer is a valid entry.

DRA Inbound Objects Applied per second The rate at which replication updates that are received from the replication partner. An integer is a valid entry.

DRA Inbound Objects Filtered per second The number of objects received from inbound replication partners that contained no updates that needed to be applied. An integer is a valid entry.

DRA Inbound Objects Percent Applied The percentage of applied inbound objects.

DRA Inbound Objects Percent Filtered The percentage of filtered inbound objects.

DRA Inbound Objects per second The number of objects received from neighbors through inbound replication. An integer is a valid entry.

DRA Inbound Properties Applied per second The number of properties that incoming properties cause to be updated. An integer is a valid entry.

DRA Inbound Properties Filtered per second The number of property changes that are received during the replication. An integer is a valid entry.

DRA Inbound Properties Percent Applied The percentage of applied inbound properties.

DRA Inbound Properties Percent Filtered The percentage of filtered inbound properties.

DRA Inbound Properties Total per second The total number of object properties received from inbound replication partners. An integer is a valid entry.

DRA Inbound Values per second The number of object property values received from inbound replication partners that are DNs that reference other objects. An integer is a valid entry.

DRA Inbound Values Total per second The total number of object property values received from inbound replication partners. An integer is a valid entry.

DRA Intersite Partner Count The number of InterSite partners that are assigned to this Domain Controller.

DRA Intrasite Partner Count The number of IntraSite partners that are assigned to this Domain Controller.

DRA NetTime Status The status code that NetTime returned.

DRA Outbound Bytes Compressed per second After The compressed size of outbound compressed replication data, after compression. An integer is a valid entry.

DRA Outbound Bytes Compressed per second Before The compressed size of outbound compressed replication data before compression. An integer is a valid entry.

DRA Outbound Bytes Not Compressed per second Before The number of bytes replicated out that were not compressed. An integer is a valid entry.

DRA Outbound Bytes Total per second The total number of bytes replicated out. An integer is a valid entry.

DRA Outbound Objects Filtered per second The number of objects that were determined by outbound replication. An integer is a valid entry.

DRA Outbound Objects per second The number of objects replicated out. An integer is a valid entry.

DRA Outbound Objects Percent Filtered The percentage of Outbound Objects Filtered.

DRA Outbound Properties per second The number of properties replicated out. An integer is a valid entry.

DRA Outbound Values per second The number of object property values containing DNs sent to outbound replication partners. An integer is a valid entry.

DRA Outbound Values Total per second The number of object property values sent to outbound replication partners. An integer is a valid entry.

DRA Pending Replication Synchronizations The number of directory synchronizations that are queued for this server but not yet processed. An integer is a valid entry.

DRA Reads The percentage of directory reads from the directory replication agent. An integer is a valid entry.

DRA Searches The percentage of directory searches from the DRA. An integer is a valid entry.

DRA Site BridgeHead Count The number of bridgehead servers found in the local site.

DRA SiteLink Count The sitelink count.

DRA Sync Requests Made The number of synchronization requests made to neighbors. An integer is a valid entry.

DRA Sync Requests Success The number of synchronization requests made to neighbors that were successfully returned. An integer is a valid entry.

DRA Writes The percentage of directory writes from the DRA. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Replication Partner attributes

The Replication Partner attributes display replication partner information for each replication partner. This attribute group has the option to cache the data it collects for some configurable period.

RPL Directory Partition The directory partition for replication.

RPL Fail Reason Text Text of the error message for the replication failure for the replication partner. This text is truncated to 128 bytes.

RPL Hostname Host name for this server.

RPL Number Failures The number of failed replication attempts with the replication partner.

RPL Partner Last Attempt Times The last time replication was attempted with the replication partner.

RPL Partner Last Success Time The last time replication was successful with the replication partner.

RPL Partner Name The hostname of the replication partner.

RPL Partner Site Name The site name for the replication partner.

RPL Replication Type The type of replication partner (IntraSite or InterSite).

RPL Site Name The local site name.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Replication Partner Latency attributes

Use the Replication Partner Latency attributes to display replication latency information for each replication partner. The latency is confirmed, tested, and monitored by creating a LostAndFound object that is monitored with its time stamps for the replication latency time. This attribute group has the option to cache the data it collects for some configurable period.

RLT Clock Change Delta The change in replication partner system clock compared to local system clock. Attributes based on previous values are valid for situations only.

RLT Clock Delta The difference in system times between the local server and the replication partner.

RLT Hostname Host name for this server.

RLT Partner Name The hostname of the replication partner.

RLT Partner Site Name The site name for replication partner.

RLT Replication Latency The interval of time to replicate objects from the local server to replication partner. This attribute's value is derived from the monitoring of the created LostAndFound object. A value of -1 indicates Inconsistent.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Security Accounts Manager attributes

Use the Security Accounts Manager attributes to create situations to monitor statistics about the Security Accounts Manager (SAM) interface, that provides compatibility between Windows 2000 and Windows NT® 4 domains.

SAM Account Group Membership Evaluations per second The number of SAM account group membership evaluations per second. An integer is a valid entry.

SAM Create Machine Attempts per second The number of SAM create system or computer attempts per second. An integer is a valid entry.

SAM Create User Attempts per second The number of SAM create user attempts per second. An integer is a valid entry.

SAM Enumerations per second The number of SAM enumerations per second. An integer is a valid entry.

SAM GC Evaluations per second The number of SAM global catalog evaluations per second. An integer is a valid entry.

SAM Membership Changes per second The number of SAM membership changes per sec. An integer is a valid entry.

SAM Nontransitive Membership Evaluations per second The number of SAM nontransitive membership evaluations per second. An integer is a valid entry.

SAM Password Changes per second The number of SAM password changes per second. An integer is a valid entry.

SAM Query Displays per second The number of SAM query displays per second. An integer is a valid entry.

SAM Reads The percentage of directory reads from SAM. An integer is a valid entry.

SAM Resource Group The number of SAM resource group membership evaluations per second. An integer is a valid entry.

SAM Searches The percentage of directory searches from SAM. An integer is a valid entry.

SAM Successful Create Machines per second The number of systems or computers that were successfully created per second. An integer is a valid entry.

SAM Successful Create Users per second The number of users that were successfully created per second. An integer is a valid entry.

SAM Transitive Membership Evaluations per second The number of SAM transitive membership evaluations per second. An integer is a valid entry.

SAM Universal Group Membership Evaluations per second The number of SAM universal group membership evaluations per second. An integer is a valid entry.

SAM Writes The percentage of directory writes from SAM. An integer is a valid entry.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Services attributes

Use the Services attributes to view status and configuration information about each service installed on the NT Server.

Account ID The account name under which the service process is logged on when it runs. The ID takes the form of "DomainName\UserName" such as ".\LocalSystem".

Account ID (Unicode) The account name under which the service process is on when it runs in UTF8. The ID takes the form of "DomainName\UserName" such as ".\LocalSystem".

Binary Path The fully qualified path to the service binary executable.

Binary Path (Unicode) The fully qualified path to the service binary executable in UTF8.

Current State The current state of the service, which can be one of the following states: Stopped; Start Pending; Stop Pending; Running; Continue Pending; Paused Pending; or Paused.

Display Name The name of the service as it appears in the NT Service Control Manager applet. This string has a maximum length of 256 bytes.

Display Name (Unicode) The name of the service as it appears in the NT Service Control Manager applet in UTF8.

Load Order Group The name of the load ordering group of which this service is a member. Services can be placed in groups so that other services can have dependencies on a group of services. If the service is not in a load ordering group, this field is blank.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Service Name The internal name of the service in the Service Control Manager database. The maximum size of the string is 256 bytes.

Start Type Specifies how to start the service. This type can be Boot, System, Automatic, Manual, Disabled or Unknown.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century

YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Trust attributes

Use the Trust attributes to display Active Directory Trust information. This attribute group has the option to cache the data it collects for some configurable period.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:K3Z or deux.raleigh.ibm.com:K3Z.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp Date and time the Tivoli Enterprise Management Server samples the data. Standard character date/time format is (CYYMMDDHHMMSSmmm), where the following measures apply:

C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in this table. For example, enter 1101009130500000 to express October 9, 2010, 1:05:00 PM.

Trust Added Specifies whether this trust was recently added. Valid values include TRUE and FALSE.

Trust Direction The direction of the trust. Trust direction can be DISABLED, TWO_WAY_TRUST, INBOUND_TRUST, or OUTBOUND_TRUST.

Trust Domain Name The domain name of the trusted domain.

Trust Dropped Whether this trust was recently dropped. Valid values include TRUE and FALSE.

Trust Hostname Host name for this server.

Trust Local Domain Default domain name associated with this server.

Trust NetBIOS Name The NetBIOS name of the trusted domain.

Trust Status The status of the trust from nltest. Trust status can be Success; Failed; or None.

Trust Type The type of the trust. Trust types can be UPLEVEL, DOWNLEVEL, MIT, or DCE.

Disk capacity planning for historical data

Disk capacity planning for a monitoring agent is a prediction of the amount of disk space to be consumed for each attribute group whose historical data is being collected. Required disk storage is an important factor to consider when you are defining data collection rules and your strategy for historical data collection.

Expected number of instances is a guideline that can be different for each attribute group, because it is the number of instances of data that the agent will return for a given attribute group, and depends upon the application environment that is being monitored. For example, if your attribute group is monitoring each processor on your machine and you have a dual processor machine, the number of instances is 2.

Calculate expected disk space consumption by multiplying the number of bytes per instance by the expected number of instances, and then multiplying that product by the number of samples.Table 9 on page 50 provides the following information required to calculate disk space for the Monitoring Agent for Active Directory:

- *DB table name* is the table name as it would appear in the warehouse database, if the attribute group is configured to be written to the warehouse.
- *Bytes per instance (agent)* is an estimate of the record length for each row or instance written to the agent disk for historical data collection. This estimate can be used for agent disk space planning purposes.
- *Database bytes per instance (warehouse)* is an estimate of the record length for detailed records written to the warehouse database, if the attribute group is configured to be written to the warehouse. Detailed records are those that have been uploaded from the agent for long-term historical data collection. This estimate can be used for warehouse disk space planning purposes.
- *Aggregate bytes per instance (warehouse)* is an estimate of the record length for aggregate records written to the warehouse database, if the attribute group is configured to be written to the warehouse. Aggregate records are created by the Summarization agent for attribute groups that have been configured for summarization. This estimate can be used for warehouse disk space planning purposes.

The IBM Tivoli Monitoring Installation and Setup Guide contains formulas that can be used to estimate the amount of disk space used at the agent and in the warehouse database for historical data collection of an attribute group.

Table 9. Capacity planning for historical data logged by component ado

DB table name	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
K3ZNTDSAB	Address_Book	272	139	449
K3ZNTDSDAI	DAI	912	789	1099
K3ZNTDSDHC	DHCP	292	161	510
K3ZNTDSDNS	DNS	412	299	1158
K3ZNTDSDS	Directory_Services	320	199	977
K3ZNTDSDCA	Domain_Controller_Availability	1248	1134	1600
K3ZNTDSDCP	Domain_Controller_Performance	296	169	713
K3ZNTDSXDS	Exchange_Directory_Services	260	124	317
K3ZNTDSFRS	File_Replication_Service	344	229	881
K3ZNTDSGPO	GPO	380	244	320
K3ZNTDSKCC	Kerberos_Consistency_Checker	256	119	273
K3ZNTDSKDC	Kerberos_Key_Distribution_Centre	256	119	273
K3ZNTDSLDP	LDAP	284	154	581
K3ZNTDSLFO	LFO	308	169	206
K3ZNTDSLSA	Local_Security_Authority	256	119	273
K3ZNTDSNSP	Name_Service_Provider	260	124	317
K3ZNTDSDRA	Replication	548	454	2120
K3ZNTDSRPL	Replication_Partner	888	758	810
K3ZNTDSRLT	Replication_Partner_Latency	448	314	468
K3ZNTDSSAM	Security_Accounts_Manager	312	189	889
K3ZNTDSSVC	Services	1368	1246	1283
K3ZNTDSTRS	Trust	580	449	486

For more information about historical data collection, see the *IBM Tivoli Monitoring Administrator's Guide*.

Chapter 6. Situations reference

This chapter contains an overview of situations, references for detailed information about situations, and descriptions of the predefined situations included in this monitoring agent.

About situations

A situation is a logical expression involving one or more system conditions. Situations are used to monitor the condition of systems in your network. You can manage situations from the Tivoli Enterprise Portal by using the Situation editor.

The IBM Tivoli Monitoring monitoring agents that you use to monitor your system environment are shipped with a set of predefined situations that you can use as-is or you can create new situations to meet your requirements. Predefined situations contain attributes that check for system conditions common to many enterprises.

For situations that are created using situation qualified attributes, use the situations link to view data and attribute values once the situation starts.

Note: These situation qualified attributes are never available in a workspace.

Using predefined situations can improve the speed with which you can begin using the Monitoring Agent for Active Directory. You can examine and, if necessary, change the conditions or values being monitored by a predefined situation to those best suited to your enterprise.

Note: The predefined situations provided with this monitoring agent are not read-only. Do not edit these situations and save over them. Software updates will write over any of the changes that you make to these situations. Instead, clone the situations that you want to change to suit your enterprise.

You can display predefined situations and create your own situations using the Situation editor. The left frame of the Situation editor initially lists the situations associated with the Navigator item that you selected. When you click a situation name or create a new situation, the right frame opens with the following tabs:

Formula
Condition being tested

Distribution
List of managed systems (operating systems, subsystems, or applications) to which the situation can be distributed.

Expert Advice
Comments and instructions to be read in the event workspace

Action
Command to be sent to the system

Until Duration of the situation

More information about situations

The *IBM Tivoli Monitoring User's Guide* contains more information about predefined and custom situations and how to use them to respond to alerts.

For a list of the predefined situations for this monitoring agent and a description of each situation, refer to the Predefined situations section below and the information in that section for each individual situation.

Predefined situations

This monitoring agent contains the following predefined situations, which are organized by the workspace that the situations are associated with:

- Replication Partner Latency workspace situation
  - Replication_Latent_Warning
  - Replication_Partner_Unsync_Warn
- Group Policy Objects workspace situations
  - GPO_Inconsistent_Warning
- Trust workspace situations
  - Trust_Added_Warning
  - Trust_Dropped_Warning
  - Trust_Failing_Critical
- DHCP workspace situations
  - DHCP_Active_Queue_Warning
  - DHCP_Conflict_Queue_Warning
  - DHCP_Counters_Abnormal_Inc_Warn
  - DHCP_Counters_Sudden_Inc_Warn
  - DHCP_Decline_Rate_Warning
  - DHCP_Dup_Drops_Rate_Warning
  - DHCP_Nacks_Rate_Warning
  - DHCP_Packs_Expired_Rate_Warning
  - DHCP_Service_State_Critical
  - DHCP_Service_Status_Critical
- Directory System Agent workspace situation
  - DS_Cache_Hit_Rate_Critical
- DNS workspace situations
  - DNS_Response_Time_Critical
  - DNS_Service_State_Critical
  - DNS_Service_Status_Critical
  - DNS_Total_Dyn_Update_Warning
  - DNS_Zone_Trans_Perc_Fails_Crit
- DNS ADIntegrated workspace situations
  - DNSAD_DC_SRV_Records_Bad_Warn
  - DNSAD_DC_SRV_Recs_Missing_Warn
  - DNSAD_GC_SRV_Records_Bad_Warn
  - DNSAD_GC_SRV_Recs_Missing_Warn
  - DNSAD_Node_Records_Missing_Crit

  - DNSAD_PDC_SRV_Records_Bad_Warn
  - DNSAD_PDC_SRV_Recs_Missing_Warn
- Domain Controller Availability workspace situations
  - DC_Default_First_Site_Warning
  - DC_Dom_Naming_Master_Def_Crit
  - DC_Dom_Naming_Master_Ping_Crit
  - DC_FSMO_Server_State_Critical
  - DC_FSMO_Transfer_Warning
  - DC_GC_List_Critical
  - DC_Infra_Master_Defined_Crit
  - DC_Infra_Master_Ping_Crit
  - DC_PDC_Master_Defined_Crit
  - DC_PDC_Master_Ping_Critical
  - DC_ReplParts_Unreachable_Crit
  - DC_RID_Master_Defined_Critical
  - DC_RID_Ping_Critical
  - DC_Schema_Master_Defined_Crit
  - DC_Schema_Master_Ping_Critical
  - DC_Server_FSMO_Status_Critical
  - DC_Server_State_Critical
  - DC_Server_Status_Critical
  - DC_Site_GCs_Available_Warning
  - DC_Site_GCs_Defined_Warning
- Domain Controller Performance workspace situations
  - DCPerf_Cache_Page_Stalls_Warn
  - DCPerf_DB_Cache_Size_Value_Warn
  - DCPerf_DB_Cache_Size_Warning
  - DCPerf_DB_Tab_Cache_Size_Warn
  - DCPerf_Log_Record_Stalls_Warn
  - DCPerf_Log_Thread_Wait_Warning
  - DCPerf_NTDS_Conn_High_Warning
- File Replication Service workspace situations
  - FRS_Change_Orders_Evap_Prc_Warn
  - FRS_Chng_Orders_Aborted_Prc_Warn
  - FRS_Chng_Orders_Morphed_Prc_Warn
  - FRS_Chng_Ordrs_Retired_Prc_Warn
  - FRS_DS_Bind_In_Error_Prc_Warn
  - FRS_Files_Instd_Error_Prc_Warn
  - FRS_KB_Stage_Space_Free_Warn
  - FRS_KB_Stage_Space_In_Use_Warn
  - FRS_Num_Change_Orders_Sent_Warn
  - FRS_Number_Files_Installed_Warning
  - FRS_Packets_Rcvd_Error_Prc_Warn
  - FRS_Packets_Received_Warning
  - FRS_Packets_Sent_Error_Prc_Warn

  - FRS_USN_Records_Accepted_Warn
- Kerberos Key Distribution Center workspace situations
  - KDC_AS_Requests
  - KDC_TGS_Requests
  - Kerberos_Authentications
- Lightweight Directory Access Protocol workspace situation
  LDAP_Client_Sessions_Warning
- Name Service Provider workspace situation
  NTLM_Authentications
- Replication workspace situations
  - DRA_Comp_Inbound_Bytes_Warning
  - DRA_Comp_Outbound_Bytes_Warning
  - DRA_Highest_USN_Critical
  - DRA_Inbound_Bytes_Total_Warning
  - DRA_Inbound_Obj_Appl_Pct_Warn
  - DRA_Inbound_Obj_Filt_Pct_Warn
  - DRA_Inbound_ObjUp_Warning
  - DRA_Inbound_Prop_Appl_Pct_Warn
  - DRA_Inbound_Prop_Filt_Pct_Warn
  - DRA_Intersite_Percent_High_Warn
  - DRA_NTP_Connection_Blocked_Warn
  - DRA_Outbound_Bytes_Total_Warning
  - DRA_Outbound_Obj_Filt_Pct_Warn
  - DRA_Pending_Rep_Sync_Warning
  - DRA_Uncomp_Inbound_Bytes_Warn
  - DRA_Uncomp_Outbound_Bytes_Warn
  - Rep_InterSite_Repl_Prtnrs_Warn
  - Rep_Site_BridgeHeads_Warning
  - Rep_SiteLinks_Warning
- Replication Partner workspace situations
  - Repl_Part_Clock_Change_Warning
  - Repl_Part_Inter_Site_Stat_Crit
  - Repl_Part_Intra_Site_Stat_Crit

Note: The Address Book, Knowledge Consistency Checker, Local Security authority, Security Accounts Manager, and Exchange Directory Services workspaces do not have associated situations.

The remaining sections of this chapter contain descriptions of each of these predefined situations. The situations are organized by the workspace that the situations are associated with.

DHCP workspace situations

DHCP_Active_Queue_Warning situation

Monitors active queue length. A high value can indicate heavy traffic on the DHCP server.

The formula for this situation is as follows:

```
DHCP\Active_Queue_Length GT 100
```

DHCP_Conflict_Queue_Warning situation

Monitors the DHCP conflict queue length. A high value can indicate that conflict detection attempts have been set too high or there is heavy traffic on the DHCP server.

The formula for this situation is as follows:

```
DHCP\Conflict_Check_Queue_Length GT 100
```

DHCP_Counters_Abnormal_Inc_Warn situation

Monitors the rate of DHCP acknowledgements and the rate of requests. If the rate increases unusually over time, this can indicate that the length of DHCP lease times has been set too short.

The formula for this situation is as follows:

```
DHCP\Requests\sec\percent_increase GT 5 OR
DHCP\Acks\sec\percent_increase GT 5
```

DHCP_Counters_Sudden_Inc_Warn situation

Monitors the rate of DHCP acknowledgements and the rate of requests. If the rate increases unusually, it can indicate that the length of scope lease times has been set too short.

The formula for this situation is as follows:

```
DHCP\Requests\sec\percent_increase GT 25 OR
DHCP\Acks\sec\percent_increase GT 25
```

DHCP_Decline_Rate_Warning situation

Monitors the rate at which the DHCP server receives declines. A high value occurs when there are address conflicts between many clients and can indicate possible network problems.

The formula for this situation is as follows:

```
DHCP\Declines_sec GT 100
```

DHCP_Dup_Drops_Rate_Warning situation

Monitors the rate at which the DHCP server receives duplicate packets. A high value can indicate that the DHCP server is not responding very fast or that clients are timing out too fast.

The formula for this situation is as follows:

```
DHCP\Duplicates_Dropped_sec GT 100
```

DHCP_Nacks_Rate_Warning situation

Monitors the rate at which the DHCP server sends negative acknowledgements. A high value can indicate possible network problems.

The formula for this situation is as follows:

```
DHCP\Nacks_sec GT 100
```

DHCP_Packs_Expired_Rate_Warning situation

Monitors the number of packets that expired per second. A high value indicates that the server is taking too long to process packets or that the traffic on the network is too high for the DHCP server to handle. This can indicate a disk or memory bottleneck.

The formula for this situation is as follows:

```
DHCP\Packets_Expired_sec GT 100
```

DHCP_Service_State_Critical situation

Monitors the availability of the DHCP service.

The formula for this situation is as follows:

```
DHCP\DHCP_Server EQ TRUE AND (Service_Name MISSING) EQ DHCP
```

DHCP_Service_Status_Critical situation

Monitors the DHCP server.

The formula for this situation is as follows:

```
DHCP\DHCP_Server EQ TRUE AND Current_State EQ Stopped  AND
Service_Name  EQ DHCPServer
```

Directory System Agent workspace situation

DS_Cache_Hit_rate_Critical situation

Monitors the percentage of directory object name component look-ups that are satisfied out of the directory service agent's name cache.

The formula for this situation is as follows:

```
DS\Name_Cache_Hit_Rate LT 80
```

DNS workspace situations

DNS_Response_Time_Critical situation

Monitors DNS response time. If DNS take a long time to resolve queries, this could adversely affect the general performance of Active Directory.

The formula for this situation is as follows:

```
DNS\Response_Time GT 3
```

DNS_Service_State_Critical situation

Monitors the availability of the DHCP service.

The formula for this situation is as follows:

```
DNS\DNS_Server EQ TRUE AND (Service_Name MISSING) EQ DNS
```

DNS_Service_Status_Critical situation

Monitors the DNS server.

The formula for this situation is as follows:

```
DNS\DNS_Server EQ TRUE AND Current_State EQ Stopped AND Service_Name EQ DNS
```

DNS_Total_Dyn_Update_Warning situation
Monitors the percentage of total failures of dynamic updates.

The formula for this situation is as follows:

```
DNS\Dynamic_Update_Failures_Pct GT 30
```

DNS_Zone_Trans_Perc_Fails_Crit situation
Monitors the percentage of zone transfer failures.

The formula for this situation is as follows:

```
DNS\Transfer_Failures_Percent GT 30
```

DNS ADIntegrated workspace situations

DNSAD_DC_SRV_Records_Bad_Warn situation
Detects when the copy of the zone that is stored on the specified server contains an SRV record for a domain controller that does not correspond to any of the known domain controllers that serve the domain covered by this zone.

The formula for this situation is as follows:

```
DAI\DC_SRV_Records_Bad GT 0
```

DNSAD_DC_SRV_Recs_Missing_Warn situation
Detects when one of the domain controller SRV records is missing from the copy of the zone that is stored on the specified server.

The formula for this situation is as follows:

```
DAI\DC_SRV_Records_Missing GT 0
```

DNSAD_GC_SRV_Records_Bad_Warn situation
Detects when the copy of the zone that is stored on the specified server contains an SRV record for a global catalog that does not correspond with any of the known global catalogs that serve the forest.

The formula for this situation is as follows:

```
DAI\GC_SRV_Records_Bad GT 0
```

DNSAD_GC_SRV_Recs_Missing_Warn situation
Monitors global catalog SRV records.

The formula for this situation is as follows:

```
DAI\GC_SRV_Records_Missing GT 0
```

DNSAD_Node_Records_Missing_Crit situation
Monitors the DNS server for missing SRV records.

The formula for this situation is as follows:

```
DAI\DNS_Node_Records_Missing GT 0
```

DNSAD_PDC_SRV_Records_Bad_Warn situation
Detects when the copy of the zone that is stored on the specified server contains an SRV record for a primary domain controller that does not correspond with the known primary domain controller that serves a specified domain.

The formula for this situation is as follows:

```
DAI\PDC_SRV_Records_Bad GT 0
```

DNSAD_PDC_SRV_Recs_Missing_Warn situation

Detects when the PDC SRV record for the specified domain is missing from he copy of the zone that is stored in the specified server.

The formula for this situation is as follows:

```
DNSAD\PDC_SRV_Records_Missing GT 0
```

Domain Controller Availability workspace situations

DC_Default_First_Site_Warning situation

Monitors for Domain Controllers using default first site.

The formula for this situation is as follows:

```
DCA\Site_Name EQ 'Default-First-Site-Name' OR
DCA\Site_Name EQ 'Premier-Site-par-defaut' OR
DCA\Site_Name EQ 'Standardname-des-ersten-Standorts' OR
DCA\Site_Name EQ 'Nombre-Predeterminado-Primer-Sitio' OR
DCA\Site_Name EQ 'Nome-de-primeiro-site-predefinido'
```

DC_Dom_Naming_Master_Def_Crit situation

Monitors the domain naming master role.

The formula for this situation is as follows:

```
DCA\Domain_Naming_Master EQ ""
```

DC_Dom_Naming_Master_Ping_Crit situation

Monitors the connection to the domain controller that hold the domain-naming master role.

The formula for this situation is as follows:

```
DCA\Ping_Domain_Naming_Master LT 0
```

DC_FSMO_Server_State_Critical situation

Monitors key services of a domain controller that holds an FSMO master role for Active Directory health.

The formula for this situation is as follows:

```
DCA\FSMO_Role NE none AND
MISSING Service_Name EQ ("Dnscache" or "IsmServ" or "Netlogon" or "NtFrs" or
"RpcLocator" or "RpcSs" or "TrkSvr" or
"TrkWks" or "W32Time" or "kdc" or
"lanmanserver" or "lanmanworkstation")
```

DC_FSMO_Transfer_Warning situation

Monitors for transfer of FSMO roles.

The formula for this situation is as follows:

```
DCA\RID_Master NE DCA\Prev_RID_Master OR
DCA\Domain_Naming_Master NE DCA\Prev_Domain_Naming_Master OR
DCA\Infrastructure_Master NE DCA\Prev_Infrastructure_Master OR
DCA\Schema_Master NE DCA\Prev_Schema_Master OR
DCA\PDC_Master NE DCA\Prev_PDC_Master
DCA\FSMO_Role NE none AND
```

DC_GC_List_Critical situation
Monitors the connections to global catalog servers.

The formula for this situation is as follows:

```
DCA\GCs_Pinged EQ 0
```

DC_Infra_Master_Defined_Crit situation
Monitors the infrastructure master role for the domain. The domain controller that holds the infrastructure master role for the group's domain updates the cross-domain group-to-user reference to reflect the new name of the user. The infrastructure master updates these references locally and uses replication to bring all other replicas of the domain up to date. If the infrastructure master is unavailable, these updates are delayed.

The formula for this situation is as follows:

```
DCA\Infrastructure_Master EQ ""
```

DC_Infra_Master_Ping_Crit situation
Monitors the domain controller that holds the infrastructure master role. The domain controller that holds the infrastructure master role for the group's domain updates the cross-domain group-to-user reference to reflect the new name of the user. The infrastructure master updates these references locally and uses replication to bring all other replicas of the domain up to date. If the infrastructure master is unavailable, these updates are delayed.

The formula for this situation is as follows:

```
DCA\Ping_Infrastructure_Master LT 0
```

DC_PDC_Master_Defined_Crit situation
Monitors the primary domain controller emulator master role for the domain.

The formula for this situation is as follows:

```
DCA\PDC_Master EQ ""
```

DC_PDC_Master_Ping_Critical situation
Monitors the connection to the domain controller that holds the primary domain controller emulator master role.

The formula for this situation is as follows:

```
DCA\Ping_PDC_Master LT 0
```

DC_ReplParts_Unreachable_Crit situation
Monitors the connection to site replication partners.

The formula for this situation is as follows:

```
DCA|Repl_Partners NE DCA\Repl_Partners_Pinged
```

DC_RID_Master_Defined_Critical situation
Monitors the relative ID (RID) master pool.

The formula for this situation is as follows:

```
DCA\RID_Master EQ  ""
```

DC_RID_Ping_Critical situation

Monitors the connection to the domain controller that holds the relative ID (RID) master role in the domain.

The formula for this situation is as follows:

```
DCA\RID_Master_Ping LT 0
```

DC_Schema_Master_Defined_Crit situation

Monitors the schema master role for any domain controller in the forest.

The formula for this situation is as follows:

```
DCA\Schema_Master EQ ""
```

DC_Schema_Master_Ping_Critical situation

Monitors the connection to the domain controller that holds the schema master role.

The formula for this situation is as follows:

```
DCA\Ping_Schema_Master LT 0
```

DC_Server_FSMO_Status_Critical situation

Monitors key services of a domain controller that holds an FSMO master role for Active Directory health.

The formula for this situation is as follows:

```
DCA\FSMO_Role NE 'none' AND Current_State EQ 'Stopped' AND
Service_Name EQ 'W32Time' OR Service_Name EQ 'RpcSs' OR
Service_Name EQ 'lanmanworkstation' OR Service_Name EQ 'NtFrs' OR
Service_Name EQ 'lanmanserver'  OR Service_Name EQ 'RpcLocator' OR
Service_Name EQ 'Netlogon' OR Service_Name EQ 'kdc' OR
Service_Name EQ 'IsmServ' OR Service_Name EQ 'Dnscache' OR
Service_Name EQ 'TrkWks' OR Service_Name EQ 'TrkSvr'
```

DC_Server_State_Critical situation

Monitors domain controller key services for Active Directory health.

The formula for this situation is as follows:

```
DCA\FSMO_Role EQ none AND
MISSING (Service_Name) EQ (lanmanworkstation, W32Time, NtFrs,lanmanserver,
RpcSs, RpcLocator, Netlogon, kdc, IsmServ, Dnscache, TrkWks, TrkSvr)
```

DC_Server_Status_Critical situation

Monitors domain controller key services for Active Directory health.

The formula for this situation is as follows:

```
DCA\FSMO_Role EQ 'none' AND Current_State EQ 'Stopped' AND
Service_Name EQ 'W32Time'  OR Service_Name EQ 'RpcSs' OR
Service_Name EQ 'lanmanworkstation' OR Service_Name EQ 'NtFrs' OR
Service_Name EQ 'lanmanserver'  OR Service_Name EQ 'RpcLocator' OR
Service_Name EQ 'Netlogon' OR Service_Name EQ 'kdc' OR
Service_Name EQ 'IsmServ' OR Service_Name EQ 'Dnscache' OR
Service_Name EQ 'TrkWks' OR Service_Name EQ 'TrkSvr'
```

DC_Site_GCs_Available_Warning

Monitors the connection to the global catalogs that are defined for the site.

The formula for this situation is as follows:

```
DCA\GCs_In_Site_Pinged EQ 0
```

DC_Site_GCs_Defined_Warning situation

Monitors the number of global catalogs in the site.

The formula for this situation is as follows:

```
DCA\GCs_In_Site EQ 0
```

Domain Controller Performance workspace situations

DCPerf_Cache_Page_Stalls_Warn situation

Monitors the number of page faults per second that cannot be serviced because there are no pages available for allocation from the database cache.

The formula for this situation is as follows:

```
DCP\Cache_Page_Fault_Stalls_Sec GT 0
```

DCPerf_DB_Cache_Size_Value_Warn situation

Monitors the cache size.

The formula for this situation is as follows:

```
DCP\Cache_Size LT 2
```

DCPerf_DB_Cache_Size_Warning situation

Monitors database performance counters that are significant for cache sizing.

The formula for this situation is as follows:

```
DCP\Cache_Pct_Hit LT 20 OR DCP\Cache_Page_Faults_Sec GT 30 OR
DCP\File_Bytes_Read_Sec GT 30 OR DCP\File_Bytes_Written_Sec GT 30 OR
DCP\File_Operations_Sec GT 100
```

DCPerf_DB_Tab_Cache_Size_Warn situation

Monitors table hit statistics to determine if the ESE database table cache size is functionally too small.

The formula for this situation is as follows:

```
DCP\Table_Open_Cache_Hits_Sec LT 1000

DCP\Table_Open_Cache_Misses_Sec GT 300

DCP\Table_Open_Cache_Pct_hit LT 20
```

DCPerf_Log_Record_Stalls_Warn situation

Monitors the number of log records that cannot be added to the log buffers per second.

The formula for this situation is as follows:

```
DCP\Log_Record_Stalls_Sec GT 0
```

DCPerf_Log_Thread_Wait_Warning situation

Monitors the number of threads that are waiting for data to be written to the log.

The formula for this situation is as follows:

```
DCP\Log_Threads_Waiting GT 300
```

DCPerf_NTDS_Conn_High_Warning situation
Monitors the number of NTDS connection objects.

The formula for this situation is as follows:
`DCP\DSA_Connections GT 20`

File Replication Service workspace situations

FRS_Change_Orders_Evap_Prc_Warn situation
Monitors the percentage of change notifications that have evaporated. Evaporated change notifications refer to the number of local file updates that were never processed because the file was deleted before it could be processed.

The formula for this situation is as follows:
`FRS\Change_Orders_Evaporated_Percent GT 30`

FRS_Chng_Ordrs_Aborted_Prc_Warn situation
Monitors the percentage of change notifications that are aborted.

The formula for this situation is as follows:
`FRS\Change_Orders_Aborted_Percent GT 30`

FRS_Chng_Orders_Morphed_Prc_Warn situation
Monitors the percentage of change notifications that morphed.

The formula for this situation is as follows:
`FRS\Change_Orders_Morphed_Percent GT 30`

FRS_Chng_Ordrs_Retired_Prc_Warn situation
Monitors the percentage of change notifications that have been retired.

The formula for this situation is as follows:
`FRS\Change_Orders_Retired_Percent GT 30`

FRS_DS_Bind_In_Error_Prc_Warn situation
Monitors the percentage of Active Directory Service bindings that are in error.

The formula for this situation is as follows:
`FRS\DS_Bindings_In_Error_Percent GT 30`

FRS_Files_Instd_Error_Prc_Warn situation
Monitors the percentage of files that are installed with error.

The formula for this situation is as follows:
`FRS\Files_Installed_with_Error_Percent GT 30`

FRS_KB_Stage_Space_Free_Warn situation
Monitors the amount of free space in the staging directory that is used by FRS to temporarily store files.

The formula for this situation is as follows:
`FRS\KB_Staging_Space_Free LT 660,000`

FRS_KB_Stage_Space_In_Use_Warn situation
Monitors available space in the staging directory that is currently in use.

The formula for this situation is as follows:

```
FRS\KB_Staging_Space_In_Use GT 600,000
```

FRS_Num_Change_Orders_Sent_Warn situation
Monitors the change notifications that are sent to outbound replication partners in idle state. A high value could indicate heavy replication traffic. In the idle state, when no replication is taking place, this number should be zero.

The formula for this situation is as follows:

```
FRS\KB_Staging_Space_In_Use EQ 0 AND FRS\Change_Orders_Sent GT 0
```

FRS_Number_Files_Installed_Warning situation
Monitors the number of files installed in idle state.

The formula for this situation is as follows:

```
FRS\KB_Staging_Space_In_Use EQ 0 AND FRS\Files_Installed GT 0
```

FRS_Packets_Rcvd_Error_Prc_Warn situation
Monitors the percentage of packets received in error.

The formula for this situation is as follows:

```
FRS\Packets_Received_In_Error_Percent GT 30
```

FRS_Packets_Received_Warning situation
Monitors the number of packets received in idle state.

The formula for this situation is as follows:

```
FRS\KB_Staging_Space_In_Use EQ 0 AND FRS\Packets_Received GT 0
```

FRS_Packets_Sent_Error_Prc_Warn situation
Monitors the percentage of packets that are sent in error.

The formula for this situation is as follows:

```
FRS\Packets_Sent_In_Error_Percent GT 30
```

FRS_USN_Records_Accepted_Warn situation
Monitors the number of counter Usn records that are accepted.

The formula for this situation is as follows:

```
FRS\Usn_Records_Accepted GT 40
```

Group Policy Objects workspace situations

GPO_Inconsistent_Warning
Monitors GPOs for consistency between Sysvol and Active Directory.

The formula for this situation is as follows:

```
GPO\Sysvol_Version NE GPO\Version
```

Kerberos Key Distribution Center workspace situations

KDC_AS_Requests situation

Monitors the number of authentication server (AS) requests serviced by the KDC per second. Authentication server (AS) requests are used by client to obtain a ticket granting ticket.

The formula for this situation is as follows:

```
KDC\Authentication_Server_Request GT 99,999
```

KDC_TGS_Requests situation

Monitors the number of ticket generation (TGS) requests serviced by the KDC per second. Ticket generation (TGS) requests are used by the client to obtain a ticket to a resource.

The formula for this situation is as follows:

```
KDC\TGS_Requests GT 99,999
```

Kerberos_Authentications situation

Monitors the number of times per second that clients use a ticket to authenticate to this domain controller.

The formula for this situation is as follows:

```
KDC\Authentications GT 99,999
```

Lightweight Directory Access Protocol workspace situation

LDAP_Client_Sessions_Warning situation

Monitors the number of connected LDAP client sessions.

The formula for this situation is as follows:

```
LDAP\Client_Sessions GT 1,000
```

Name Service Provider workspace situation

NTLM_Authentications situation

Monitors the number of NTLM authentications per second serviced by a domain controller.

The formula for this situation is as follows:

```
NTLM\Authentications GT 1,000
```

Replication workspace situations

DRA_Comp_Inbound_Bytes_Warning situation

Monitors compressed inbound bytes per second.

The formula for this situation is as follows:

```
DRA\Inbound_Bytes\Compressed_Per_Sec_Before GT 100
```

DRA_Comp_Outbound_Bytes_Warning situation

Monitors compressed outbound bytes.

The formula for this situation is as follows:

DRA\Outbound_Bytes\Compressed_Per_Sec_Before GT 100

DRA_Highest_USN_Critical situation

Monitors the high-order 32 bits of the highest USN issued on the directory service agent (DSA).

The formula for this situation is as follows:

DRA\High_USN_Committed_High EQ 99,999

DRA_Inbound_Bytes_Total_Warning situation

Monitors the number of directory service agent (DSA) inbound bytes per second. If this value greatly exceeds the baseline value that was taken when the system was running under normal conditions, it might indicate that the system needs to be adjusted or upgraded to accommodate the increased load.

The formula for this situation is as follows:

DRA\Inbound_Bytes\Total_Per_Sec GT 35,000

DRA_Inbound_Obj_Appl_Pct_Warn situation

Monitors the percentage of inbound replication objects that are received from replication partners and applied by the local service directory.

The formula for this situation is as follows:

DRA\Inbound_Objects\Percent_Applied LT 70

DRA_Inbound_Obj_Filt_Pct_Warn situation

Monitors the percentage of inbound replication objects received from replication partners that contains no updated to be applied.

The formula for this situation is as follows:

DRA\Inbound_Objects\Percent_Filtered GT 50

DRA_Inbound_ObjUp_Warning situation

Monitors the Active Directory Inbound Object Updates Remaining in Packet Performance counter. This is an arbitrary value that needs to be adjusted for each unique setup after setting a baseline. Administrators can use this situation to determine if the Active Directory replication is performing at acceptable levels as defined at their site.

The formula for this situation is as follows:

DRA\Inbound_Objects_Update\Remain_Packet GT 15

DRA_Inbound_Prop_Appl_Pct_Warn situation

Monitors the percentage of inbound replication properties that are received from replication partners and applied by the local service directories.

The formula for this situation is as follows:

DRA\Inbound_Properties\Percent_Applied LT 70

DRA_Inbound_Prop_Filt_Pct_Warn situation

Monitors the percentage of inbound replication properties received from replication partners that did not contain any updates to be applied.

The formula for this situation is as follows:

DRA\Inbound_Properties\Percent_Filtered GT 50

DRA_Intersite_Percent_High_Warn situation
Monitors ratio of intersite to intrasite inbound bytes.

The formula for this situation is as follows:

```
DRA\Inbound_Bytes\Intersite_Percent GT 70
```

DRA_NTP_Connection_Blocked_Warn situation
Monitors the Net Time Protocol connection.

The formula for this situation is as follows:

```
DRA\NetTime_Status NE 0
```

DRA_Outbound_Bytes_Total_Warning situation
Monitors the number of directory service agent (DSA) outbound bytes per second. If this value greatly exceeds the baseline value that was taken when the system was running under normal conditions, it might indicate that the system needs to be adjusted or upgraded to accommodate the increased load.

The formula for this situation is as follows:

```
DRA\Outbound_Bytes\Total_Per_Sec GT 35,000
```

DRA_Outbound_Obj_Filt_Pct_Warn situation
Monitors the percentage of outbound replication objects that are already received by the outbound partner.

The formula for this situation is as follows:

```
DRA\Outbound_Objects\Percent_Filtered GT 50
```

DRA_Pending_Rep_Sync_Warning situation
Monitors the Active Directory Pending Replications Performance counter. This is an arbitrary value that needs to be adjusted for each unique setup after setting a baseline. Administrators can use this rule to determine if the Active Directory replication is performing at acceptable levels as defined at their site.

The formula for this situation is as follows:

```
DRA\Pending_Replication_Synchronizations_GT 80
```

DRA_Uncomp_Inbound_Bytes Warn situation
Monitors the inbound rate for bytes that are not compressed.

The formula for this situation is as follows:

```
DRA\Inbound_Bytes\Not_Compressed_Per_Sec GT 100
```

DRA_Uncomp_Outbound_Bytes Warn situation
Monitors the outbound rate for bytes that are not compressed.

The formula for this situation is as follows:

```
DRA\Outbound_Bytes\Not_Compressed_Per_Sec GT 100
```

Rep_InterSite_Repl_Prtnrs_Warn situation
Monitors whether the domain controller that is acting as a bridgehead server has a replication partner in an intersite replication process.

The formula for this situation is as follows:

```
DRA\InterSite_Partner_Court EQ 0
```

Rep_Site_BridgeHeads_Warning situation
Monitors the number of bridgehead servers.

The formula for this situation is as follows:

```
DRA\Site_BridgeHead_Court EQ 0
```

Rep_SiteLinks_Warning situation
Monitors the site links for the specified site.

The formula for this situation is as follows:

```
DRA\SiteLink_Count EQ 0
```

Replication Partner workspace situations

Repl_Part_Inter_Site_Stat_Crit situation
Monitors intersite replication processes.

The formula for this situation is as follows:

```
RPL\Partner_Last_Attempt_Time NE RPL\Partner_Last Success_Time
AND RPL\Replication_Type EQ InterSite
```

Repl_Part_Intra_Site_Stat_Crit situation
Monitors intrasite replication.

The formula for this situation is as follows:

```
RPL\Partner_Last_Attempt_Time NE RPL\Partner_Last_Success_Time
AND RPL\Replication_Type EQ IntraSite
```

Replication Partner Latency workspace situation

Replication_Latent_Warning situation
Monitors replication time between domain controller and partners. The latency is confirmed, tested, and monitored by creating a LostAndFound object that is monitored with its time stamps for replication latency time. Units for Replication Latency are seconds, 3600 equals one hour.

The formula for this situation is as follows:

```
RLT\Replication_Latency GT 3600
```

Repl_Part_Clock_Change_Warning situation
Monitors the clock of replication partners against local system clock.

The formula for this situation is as follows:

```
RLT\Clock_Change_Delta GT 0
OR RLT\Clock_Change_Delta LT -5
```

Replication_Partner_Unsync_Warn situation
Monitors synchronization of replication partner system clock.

The formula for this situation is as follows:

```
RLT\Clock_Delta GT 0
OR RLT\Clock_Delta LT -1
```

Trust workspace situations

Trust_Added_Warning situation

Monitors for added trust relationships.

The formula for this situation is as follows:

```
Trust\Added EQ TRUE
```

Trust_Dropped_Warning situation

Monitors for dropped trust relationships.

The formula for this situation is as follows:

```
Trust\Dropped EQ true
```

Trust_Failing_Critical situation

Monitors the status of a trust.

The formula for this situation is as follows:

```
Trust\Status EQ Failed
```

Chapter 7. Take Action commands reference

This chapter contains an overview of Take Action commands and references for detailed information about Take Action commands.

About Take Action commands

Take Action commands can be run from the desktop or included in a situation or a policy.

When included in a situation, the command executes when the situation becomes true. A Take Action command in a situation is also referred to as reflex automation. When you enable a Take Action command in a situation, you automate a response to system conditions. For example, you can use a Take Action command to send a command to restart a process on the managed system or to send a text message to a cell phone.

Advanced automation uses policies to perform actions, schedule work, and automate manual tasks. A policy comprises a series of automated steps called activities that are connected to create a workflow. After an activity is completed, Tivoli Enterprise Portal receives return code feedback, and advanced automation logic responds with subsequent activities prescribed by the feedback.

More information about Take Action commands

For more information about working with Take Action commands, see the *IBM Tivoli Monitoring User's Guide*.

Predefined Take Action commands

This monitoring agent does not have any predefined Take Action commands. However, you can run commands yourself, and include those that you use often in a list of available commands.

Chapter 8. Policies reference

This chapter contains an overview of policies and references for detailed information about policies.

About policies

Policies are an advanced automation technique for implementing more complex workflow strategies than you can create through simple automation.

A *policy* is a set of automated system processes that can perform actions, schedule work for users, or automate manual tasks. You use the Workflow Editor to design policies. You control the order in which the policy executes a series of automated steps, which are also called activities. Policies are connected to create a workflow. After an activity is completed, Tivoli Enterprise Portal receives return code feedback and advanced automation logic responds with subsequent activities prescribed by the feedback.

Note: For monitoring agents that provide predefined policies, predefined policies are not read-only. Do not edit these policies and save over them. Software updates will write over any of the changes that you make to these policies. Instead, clone the policies that you want to change to suit your enterprise.

More information about policies

For more information about working with policies, see the *IBM Tivoli Monitoring User's Guide*.

For information about using the Workflow Editor, see the *IBM Tivoli Monitoring Administrator's Guide* or the Tivoli Enterprise Portal online help.

Predefined policies

This monitoring agent does not have any predefined policies.

Appendix A. Upgrading for warehouse summarization

The Monitoring Agent for Active Directory made changes to the warehouse collection and summarization characteristics for some agent attribute groups. These changes correct and improve the way warehouse data is summarized, producing more meaningful historical reports. This appendix explains those changes and the implications to your warehouse collection and reporting.

Warehouse summarization is controlled on a per-table basis. How the rows in each table are summarized is determined by a set of attributes in each table that are designated as primary keys. There is always one primary key representing the monitored resource, and data is minimally summarized based on this value. For all agents, this primary key is represented internally by the column name, ORIGINNODE; however, the external attribute name varies with each monitoring agent.

One or more additional primary keys are provided for each attribute group to further refine the level of summarization for that attribute group. For example, in an OS agent disk attribute group, a primary key might be specified for the logical disk name that allows historical information to be reported for each logical disk in a computer.

Tables in the warehouse

For a monitoring agent, there are two main types of warehouse tables:

- Raw tables:

  These tables contain the raw information reported by a monitoring agent and written to the warehouse by the Warehouse Proxy agent. Raw tables are named for the attribute group that they represent, for example, k3zntdsab.
- Summary tables:

  These tables contain summarized information based on the raw tables and written to the warehouse by the Summarization and Pruning agent. Summarization provides aggregation results over various reporting intervals, for example, hours, days, and so on. Summary table names are based on the raw table name with an appended suffix, for example, k3zntdsab_H, k3zntdsab_D, and so on.

Effects on summarized attributes

When tables are summarized in the warehouse, the summary tables and summary views are created to include additional columns to report summarization information. Table 10 contains a list of the time periods and the suffixes for the summary tables and views.

Table 10. Time periods and suffixes for summary tables and views

Data collection time period	Summary table suffixes	Summary view suffixes
Hourly	_H	_HV
Daily	_D	_DV
Weekly	_W	_WV
Monthly	_M	_MV

Table 10. Time periods and suffixes for summary tables and views (continued)

Data collection time period	Summary table suffixes	Summary view suffixes
Quarterly	_Q	_QV
Yearly	_Y	_YV

Table 11 shows the expansion to summary columns of some of the most commonly used attribute types.

Table 11. Additional columns to report summarization information

Attribute name	Aggregation type	Additional summarization columns
MyGauge	GAUGE	MIN_MyGauge MAX_MyGauge SUM_MyGauge AVG_MyGauge
MyCounter	COUNTER	TOT_MyCounter HI_MyCounter LO_MyCounter LAT_MyCounter
MyProperty	PROPERTY	LAT_Property

These additional columns are provided only for attributes that are not primary keys. In the cases when an existing attribute is changed to be a primary key, the Summarization and Pruning agent no longer creates summarization values for the attributes, but the previously created column names remain in the table with any values already provided for those columns. These columns cannot be deleted from the warehouse database, but as new data is collected, these columns will not contain values. Similarly, when the primary key for an existing attribute has its designation removed, that attribute has new summarization columns automatically added. As new data is collected, it is used to populate these new column values, but any existing summarization records do not have values for these new columns.

The overall effect of these primary key changes is that summarization information is changing. If these changes result in the old summarization records no longer making sense, you can delete them. As a part of warehouse upgrade, summary views are dropped. The views will be recreated by the Summarization and Pruning agent the next time it runs. Dropping and recreating the views ensure that they reflect the current table structure.

Upgrading your warehouse with limited user permissions

The IBM Tivoli Monitoring warehouse agents (Warehouse Proxy and Summarization and Pruning agents) can dynamically adjust warehouse table definitions based on attribute group and attribute information being loaded into the warehouse. These types of table changes must be done for this monitoring agent for one or both of the following conditions:

- The monitoring agent has added new attributes to an existing attribute group and that attribute group is included in the warehouse.
- The monitoring agent has added a new attribute group and that attribute group is included in the warehouse.

For the warehouse agents to automatically modify the warehouse table definitions, they must have permission to alter warehouse tables. You might not have granted these agents these permissions, choosing instead to manually define the raw tables and summary tables needed for the monitoring agents. Or, you might have granted these permissions initially, and then revoked them after the tables were created.

You have two options to effect the required warehouse table changes during the upgrade process:

- Grant the warehouse agents temporary permission to alter tables

  If using this option, grant the permissions, start historical collection for all the desired tables, allow the Warehouse Proxy agent to add the new data to the raw tables, and allow the Summarization and Pruning agent to summarize data for all affected tables. Then, remove the permission to alter tables
- Make the warehouse table updates manually

  If using this option, you must determine the table structures for the raw and summary tables. If you manually created the tables in the earlier warehouse definition, you already have a methodology and tools to assist you in this effort. You can use a similar technique to update and add new tables for this warehouse migration.

  For a method of obtaining raw table schema, refer to the IBM Redbook,*Tivoli Management Services Warehouse and Reporting*, January 2007, SG24-7290. The chapter that explains warehouse tuning includes a section on creating data tables manually.

Appendix B. IBM Tivoli Enterprise Console event mapping

Each event class corresponds to an attribute group in the monitoring agent. For a description of the event slots for each event class, see Table 12 on page 78. For more information about mapping attribute groups to event classes, see the *IBM Tivoli Monitoring Administrator's Guide*.

Generic event mapping provides useful event class and attribute information for situations that do not have specific event mapping defined. BAROC files are found on the Tivoli Enterprise Monitoring Server in the installation directory in TECLIB (that is, *install_dir*/cms/TECLIB for Windows systems and *install_dir*/tables/*TEMS_hostname*/TECLIB for UNIX® systems). IBM Tivoli Enterprise Console event synchronization provides a collection of ready-to-use rule sets that you can deploy with minimal configuration. Be sure to install IBM Tivoli Enterprise Console event synchronization to access the correct Sentry.baroc, which is automatically included during base configuration of IBM Tivoli Enterprise Console rules if you indicate that you want to use an existing rulebase. See the *IBM Tivoli Monitoring Installation and Setup Guide* for details.

To determine what event class is sent when a given situation is triggered, look at the first referenced attribute group in the situation predicate. The event class that is associated with that attribute group is the one that is sent. This is true for both pre-packaged situations and user-defined situations. See the table below for attribute group to event classes and slots mapping information.

For example, if the situation is monitoring the AB Browses per second attribute from the Address_Book attribute group, the event class that is sent once the situation is triggered is ITM_Address_Book.

Note: There are cases where these mappings generate events that are too large for the Tivoli Enterprise Console. In these cases, the event class names and the event slot names are the same, but some of the event slots are omitted.

Each of the event classes is a child of K3Z_Base. The K3Z_Base event class can be used for generic rules processing for any event from the Monitoring Agent for Active Directory

Table 12. Overview of attribute groups to event classes and slots

Attribute group	event class and slots
Address_Book	ITM_Address_Book event class with these slots: • server_name: STRING • timestamp: STRING • k3z_ab_anr_per_sec: INTEGER • k3z_ab_browses_per_sec: INTEGER • k3z_ab_client_sessions: INTEGER • k3z_ab_matches_per_sec: INTEGER • k3z_ab_property_reads_per_sec: INTEGER • k3z_ab_proxy_lookups_per_sec: INTEGER • k3z_ab_searches_per_sec: INTEGER • parameter: STRING • k3z_value: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Replication	ITM_Replication event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dra_high_usn_commited_high: INTEGER • k3z_dra_high_usn_commited_low: INTEGER • k3z_dra_high_usn_issued_high: INTEGER • dra_high_usn_issued_low: INTEGER • k3z_dra_inbound_bytes_compressed_per_sec_before: INTEGER • dra_inbound_bytes_compressed_per_sec_after: INTEGER • k3z_dra_inbound_bytes_not_compressed_per_sec: INTEGER • k3z_dra_inbound_bytes_total_per_sec: INTEGER • k3z_dra_inbound_full_sync_objects_remain: INTEGER • k3z_dra_inbound_objects_update_remain_packet: INTEGER • k3z_dra_inbound_objects_applied_per_sec: INTEGER • k3z_dra_inbound_objects_filtered_per_sec: INTEGER • k3z_dra_inbound_objects_per_sec: INTEGER • k3z_dra_inbound_properties_applied_per_sec: INTEGER • k3z_dra_inbound_properties_filtered_per_sec: INTEGER • k3z_dra_inbound_properties_total_per_sec: INTEGER • k3z_dra_inbound_values_per_sec: INTEGER • k3z_dra_inbound_values_total_per_sec: INTEGER • k3z_dra_outbound_bytes_compressed_per_sec_after INTEGER Continued on the next page.

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Replication continued	• k3z_dra_outbound_bytes_compressed_per_sec_before: INTEGER • k3z_dra_outbound_bytes_not_compressed_per_sec_before: INTEGER • k3z_dra_outbound_bytes_total_per_sec: INTEGER • k3z_dra_outbound_objects_filtered_per_sec: INTEGER • k3z_dra_outbound_objects_per_sec: INTEGER • k3z_dra_outbound_properties_per_sec: INTEGER • k3z_dra_outbound_values_per_sec: INTEGER • k3z_dra_outbound_values_total_per_sec: INTEGER • k3z_dra_pending_replication_synchronizations: INTEGER • k3z_dra_reads: INTEGER • k3z_dra_searches: INTEGER • k3z_dra_sync_requests_made: INTEGER • k3z_dra_sync_requests_success: INTEGER • k3z_dra_writes: INTEGER • k3z_dra_site_bridgehead_count: INTEGER • k3z_dra_sitelink_count: INTEGER • k3z_dra_intersite_partner_count: INTEGER • k3z_dra_intrasite_partner_count: INTEGER • k3z_dra_inbound_objects_percent_applied: INTEGER • k3z_dra_inbound_objects_percent_filtered: INTEGER • k3z_dra_inbound_properties_percent_applied: INTEGER • k3z_dra_inbound_properties_percent_filtered: INTEGER • k3z_dra_outbound_objects_percent_filtered: INTEGER • k3z_dra_nettime_status: INTEGER • k3z_dra_bridgehead: STRING • k3z_dra_bridgehead_enum: STRING • k3z_dra_hostname: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Directory_Services	ITM_Directory_Services event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_ds_client_binds_per_sec: INTEGER • k3z_ds_client_name_translations_per_sec: INTEGER • k3z_ds_directory_reads_per_sec: INTEGER • k3z_ds_directory_searches_per_sec: INTEGER • k3z_ds_directory_writes_per_sec: INTEGER • k3z_ds_monitor_list_size: INTEGER • k3z_ds_name_cache_hit_rate: INTEGER • k3z_ds_notify_queue_size: INTEGER • k3z_ds_other_reads: INTEGER • k3z_ds_other_searches: INTEGER • k3z_ds_other_writes: INTEGER • k3z_ds_search_sub_operations_per_sec: INTEGER • k3z_ds_security_descriptor_propagations_per_sec: INTEGER • k3z_ds_security_descriptor_propagator_average_exclusion_time: INTEGER • k3z_ds_security_descriptor_propagator_runtime_queue INTEGER • k3z_ds_security_descriptor_sub_operations_per_sec: INTEGER • k3z_ds_server_binds_per_sec: INTEGER • k3z_ds_server_name_translations_per_sec: INTEGER • k3z_ds_threads_in_use: INTEGER
Kerberos_Consistency_Checker	ITM_Kerberos_Consistency_Checker event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_kcc_reads: INTEGER • k3z_kcc_searches: INTEGER • k3z_kcc_writes: INTEGER

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Kerberos_Key_Distribution_Centre	ITM_Kerberos_Key_Distribution_Centre event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_kdc_as_request: INTEGER • k3z_kdc_tgs_requests: INTEGER • k3z_kdc_authentications: INTEGER
LDAP	ITM_LDAP event class with these slots: • k3z_ldap_active_threads: INTEGER • k3z_ldap_bind_time: INTEGER • k3z_ldap_client_sessions: INTEGER • k3z_ldap_searches: INTEGER • k3z_ldap_searches_per_sec: INTEGER • k3z_ldap_successful_binds: INTEGER • k3z_ldap_successful_binds_per_sec: INTEGER • k3z_ldap_udp_operations_per_sec: INTEGER • k3z_ldap_writes: INTEGER • k3z_ldap_writes_per_sec: INTEGER • timestamp: STRING • server_name: STRING • parameter: STRING • k3z_value: STRING
Local_Security_Authority	ITM_Local_Security_Authority event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_lsa_reads: INTEGER • k3z_lsa_searches: INTEGER • k3z_lsa_writes: INTEGER
Name_Service_Provider	ITM_Name_Service_Provider event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_nspi_reads: INTEGER • k3z_nspi_searches: INTEGER • k3z_nspi_writes: INTEGER • k3z_ntlm_authentications: INTEGER

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Security_Accounts_Manager	ITM_Security_Accounts_Manager event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_sam_account_group_membership_ evaluations_per_sec: INTEGER • k3z_sam_create_machine_attempts_per_sec: INTEGER • k3z_sam_create_user_attempts_per_sec: INTEGER • k3z_sam_enumerations_per_sec: INTEGER • k3z_sam_gc_evaluations_per_sec: INTEGER • k3z_sam_membership_changes_per_sec: INTEGER • k3z_sam_non_transitive_membership_ evaluations_per_sec: INTEGER • k3z_sam_password_changes_per_sec: INTEGER • k3z_sam_query_displays_per_sec: INTEGER • k3z_sam_reads: INTEGER • k3z_sam_resource_group: INTEGER • k3z_sam_searches: INTEGER • k3z_sam_successful_create_machines_ per_sec: INTEGER • k3z_sam_successful_create_users_per_sec: INTEGER • k3z_sam_transitive_membership_ evaluations_per_sec: INTEGER • k3z_sam_universal_group_membership_ evaluations_per_sec: INTEGER • k3z_sam_writes: INTEGER
Exchange_Directory_Services	ITM_Exchange_Directory_Services event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_xds_client_sessions: INTEGER • k3z_xds_reads: INTEGER • k3z_xds_searches: INTEGER • k3z_xds_writes: INTEGER

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Replication_Partner	ITM_Replication_Partner event class with these slots: • server_name: STRING • timestamp: STRING • k3z_value: STRING • parameter: STRING • k3z_rpl_partner_name: STRING • k3z_rpl_partner_last_attempt_time: STRING • k3z_rpl_partner_last_success_time: STRING • k3z_rpl_directory_partition: STRING • k3z_rpl_number_failures: INTEGER • k3z_rpl_replication_type: STRING • k3z_rpl_partner_site_name: STRING • k3z_rpl_site_name: STRING • k3z_rpl_hostname: STRING • k3z_rpl_fail_reason_text: STRING • k3z_rpl_replication_type_enum: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
File_Replication_Service	ITM_File_Replication_Service event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_frs_change_orders_received: INTEGER • k3z_frs_change_orders_evaporated: INTEGER • k3z_frs_change_orders_evaporated_percent: INTEGER • k3z_frs_packets_sent: INTEGER • k3z_frs_packets_sent_in_error: INTEGER • k3z_frs_packets_sent_in_error_percent: INTEGER • k3z_frs_ds_bindings_in_error: INTEGER • k3z_frs_ds_bindings: INTEGER • k3z_frs_ds_bindings_in_error_percent: INTEGER • k3z_frs_change_orders_retired: INTEGER • k3z_frs_change_orders_retired_percent: INTEGER • k3z_frs_change_orders_morphed: INTEGER • k3z_frs_change_orders_morphed_percent: INTEGER • k3z_frs_kb_staging_space_in_use: INTEGER • k3z_frs_files_installed_with_error: INTEGER • k3z_frs_files_installed: INTEGER • k3z_frs_files_installed_with_error_percent: INTEGER • k3z_frs_packets_received: INTEGER • k3z_frs_packets_received_in_error: INTEGER • k3z_frs_packets_received_in_error_percent: INTEGER • k3z_frs_usn_records_accepted: INTEGER • k3z_frs_change_orders_aborted: INTEGER • k3z_frs_change_orders_aborted_percent: INTEGER • k3z_frs_kb_staging_space_free: INTEGER • k3z_frs_change_orders_sent: INTEGER

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Domain_Controller_Availability	ITM_Domain_Controller_Availability event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dca_repl_partners: INTEGER • k3z_dca_repl_partners_pinged: INTEGER • k3z_dca_gcs: INTEGER • k3z_dca_gcs_pinged: INTEGER • k3z_dca_gcs_in_site: INTEGER • k3z_dca_gcs_in_site_pinged: INTEGER • k3z_dca_fsmo_role: STRING • k3z_dca_rid_master: STRING • k3z_dca_ping_rid_master: INTEGER • k3z_dca_domain_naming_master: STRING • k3z_dca_ping_domain_naming_master: INTEGER • k3z_dca_infrastructure_master: STRING • k3z_dca_ping_infrastructure_master: INTEGER • k3z_dca_schema_master: STRING • k3z_dca_ping_schema_master: INTEGER • k3z_dca_pdc_master: STRING • k3z_dca_ping_pdc_master: INTEGER • k3z_dca_prev_rid_master: STRING • k3z_dca_prev_domain_naming_master: STRING • k3z_dca_prev_infrastructure_master: STRING • k3z_dca_prev_schema_master: STRING • k3z_dca_prev_pdc_master: STRING • k3z_dca_site_name: STRING • k3z_dca_hostname: STRING • k3z_dca_forest_name: STRING • k3z_dca_domain_name: STRING • k3z_dca_fsmo_role_enum: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Domain_Controller_Performance	ITM_Domain_Controller_Performance event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dcp_cache_pct_hit: INTEGER • k3z_dcp_cache_page_faults_sec: INTEGER • k3z_dcp_file_bytes_read_sec: INTEGER • k3z_dcp_file_bytes_written_sec: INTEGER • k3z_dcp_file_operations_sec: INTEGER • k3z_dcp_log_threads_waiting: INTEGER • k3z_dcp_table_open_cache_hits_sec: INTEGER • k3z_dcp_table_open_cache_misses_sec: INTEGER • k3z_dcp_table_open_cache_pct_hit: INTEGER • k3z_dcp_kb_cache_size: INTEGER • k3z_dcp_log_record_stalls_sec: INTEGER • k3z_dcp_cache_page_fault_stalls_sec: INTEGER • k3z_dcp_dsa_connections: INTEGER • k3z_dcp_file_bytes_read_sec_enum: STRING • k3z_dcp_file_bytes_written_sec_enum: STRING • k3z_dcp_file_operations_sec_enum: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DHCP	ITM_DHCP event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dhcp_requests_sec_percent_increase: INTEGER • k3z_dhcp_acks_sec_percent_increase: INTEGER • k3z_dhcp_dhcp_server: STRING • k3z_dhcp_declines_sec: INTEGER • k3z_dhcp_conflict_check_queue_length: INTEGER • k3z_dhcp_duplicates_dropped_sec: INTEGER • k3z_dhcp_nacks_sec: INTEGER • k3z_dhcp_packets_expired_sec: INTEGER • k3z_dhcp_active_queue_length: INTEGER • k3z_dhcp_dhcp_server: STRING • k3z_dhcp_dhcp_server_enum: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS	ITM_DNS event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dns_dns_server: STRING • k3z_dns_dns_server_enum: STRING • k3z_dns_dynamic_update_failures_pct: INTEGER • k3z_dns_response_time: INTEGER • k3z_dns_transfer_failures_percent: INTEGER • k3z_dns_caching_memory: INTEGER • k3z_dns_dynamic_update_queued: INTEGER • k3z_dns_dynamic_update_received: INTEGER • k3z_dns_dynamic_update_received_sec: INTEGER • k3z_dns_dynamic_update_rejected: INTEGER • k3z_dns_dynamic_update_timeouts: INTEGER • k3z_dns_total_query_received: INTEGER • k3z_dns_total_query_received_sec: INTEGER • k3z_dns_total_response_sent: INTEGER • k3z_dns_total_response_sent_sec: INTEGER • k3z_dns_zone_transfer_failure: INTEGER • k3z_dns_zone_transfer_request_received: INTEGER • k3z_dns_zone_transfer_success: INTEGER • k3z_dns_dynamic_update_rejected_pct: INTEGER • k3z_dns_dynamic_update_timeouts_pct: INTEGER • k3z_dns_total_response_sent_delta: INTEGER • k3z_dns_total_query_received_delta: INTEGER • k3z_dns_dynamic_update_received_delta: INTEGER • k3z_dns_dynamic_update_rejected_delta: INTEGER • k3z_dns_dynamic_update_rejected_delta: INTEGER

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS (continued)	• k3z_dns_dynamic_update_timeouts_delta: INTEGER • k3z_dns_zone_transfer_failure_delta: INTEGER • k3z_dns_zone_transfer_request_ received_delta: INTEGER • k3z_dns_zone_transfer_success_delta: INTEGER
DAI	ITM_DAI event class with these slots: • server_name: STRING • timestamp: STRING • server_name: STRING • parameter: STRING • k3z_dai_gc_srv_records_missing: INTEGER • k3z_dai_gc_srv_records_bad: INTEGER • k3z_dai_node_records_missing: INTEGER • k3z_dai_dc_srv_records_missing: INTEGER • k3z_dai_dc_srv_records_bad: INTEGER • k3z_dai_pdc_srv_records_missing: INTEGER • k3z_dai_pdc_srv_records_bad: INTEGER • k3z_dai_forest_name: STRING • k3z_dai_hostname: STRING • k3z_dai_domain: STRING • k3z_dai_missing_gc: STRING • k3z_dai_bad_gc: STRING • k3z_dai_missing_node_rec: STRING • k3z_dai_missing_dc: STRING • k3z_dai_bad_dc: STRING • k3z_dai_missing_pdc: STRING • k3z_dai_bad_pdc: STRING

Table 12. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Services	ITM_Services event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • display_name: STRING • current_state: STRING • start_type: STRING • binary_path: STRING • account_id: STRING • load_order_group: STRING • service_name: STRING • display_name_u: STRING • binary_path_u: STRING • account_id_u: STRING • start_type_enum: STRING

Appendix C. Monitoring Agent for Active Directory data collection

In general, the Monitoring Agent for Active Directory gathers data when requested to satisfy a workspace refresh, situation sampling of attributes, or historical data collection. All attributes in the attribute groups that make up a workspace or situation are gathered at that time. The default refresh/sampling intervals were chosen such that the agent will not put a significant load on the system as it gathers the data.

Most of the attributes gathered by the Monitoring Agent for Active Directory come from Application Programming Interfaces (API). When there is not an API available for a particular function, Command Language (CL) commands have been used.

The Monitoring Agent for Active Directory maintains long running processes for the agent that communicate with the Tivoli Enterprise Management Server and the collector that drives data collection. Depending on the data to collect there are also short running processes used to access system data, data queues created to receive events from the system, and long running processes to interact with performance data gathering APIs.

The following table shows each attribute group, the mechanism used to gather the attributes, and notes. The abbreviations used in the Collection Methods column are:

- API - Application Programming Interface
- CL - Command Language command

Table 13. Mechanisms used to gather attributes

Attribute group	Collection methods	API/CL names
Address_Book	API	Performance Data Helper
Replication	API	Performance Data Helper
Replication	API	IADsTools
Replication	CL	net time
Directory_Services	API	Performance Data Helper
Kerberos_Consistency_ Checker	API	Performance Data Helper
Kerberos_Key_Distribution_ Centre	API	Performance Data Helper
LDAP	API	Performance Data Helper
Local_Security_Authority	API	Performance Data Helper
Name_Service_Provider	API	Performance Data Helper
Security_Accounts_Manager	API	Performance Data Helper
Exchange_Directory_Services	API	Performance Data Helper
Replication_Partner	API	IADsTools
File_Replication_Service	API	Performance Data Helper

Table 13. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	API/CL names
Domain_Controller_ Availability	API	IADsTools
Domain_Controller_ Availability	CL	ping
Domain_Controller_ Performance	API	Performance Data Helper
Domain_Controller_ Performance	API	IADsTools
DHCP	API	Performance Data Helper
DNS	API	Performance Data Helper
DAI	API	IADsTools
DAI	API	DnsQuery
Services	API	Service Control Manager
Trust	API	IADsTools
Trust	CL	netdom verify
GPO	API	IADsTools
LFO	API	IADsTools
LFO	API	Active Directory Service Interfaces
Replication_Partner_Latency	API	IADsTools
Replication_Partner_Latency	API	Active Directory Service Interfaces

Appendix D. Problem determination

This appendix explains how to troubleshoot the IBM Tivoli Monitoring: Active Directory Agent. Troubleshooting, or problem determination, is the process of determining why a certain product is malfunctioning.

Note: You can resolve some problems by ensuring that your system matches the system requirements listed in Chapter 2, "Requirements for the monitoring agent," on page 5.

This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information. Also see "Support for problem solving" on page 114 for other problem-solving options.

Gathering product information for IBM Software Support

Before contacting IBM Software Support about a problem you are experiencing with this product, gather the following information that relates to the problem:

Table 14. Information to gather before contacting IBM Software Support

Information type	Description
Log files	Collect trace log files from failing systems. Most logs are located in a `logs` subdirectory on the host computer. See "Trace logging" on page 96 for lists of all trace log files and their locations. See the *IBM Tivoli Monitoring User's Guide* for general information about the IBM Tivoli Monitoring environment.
Operating system	Operating system version number and patch level
Messages	Messages and other information displayed on the screen
Version numbers for IBM Tivoli Monitoring	Version number of the following members of the monitoring environment: • IBM Tivoli Monitoring. Also provide the patch level, if available. • IBM Tivoli Monitoring: Active Directory Agent
Screen captures	Screen captures of incorrect output, if any.
(*UNIX only*) Core dump files	If the system stops on UNIX systems, collect core dump file from *install_dir*/bin directory, where *install_dir* is the directory path where you installed the monitoring agent.

Upload files for review to the following FTP site: `ftp.emea.ibm.com`. Log in as **anonymous** and place your files in the directory that corresponds to the IBM Tivoli Monitoring component that you use.

Built-in problem determination features

The primary troubleshooting feature in the IBM Tivoli Monitoring: Active Directory Agent is logging. *Logging* refers to the text messages and trace data generated by the IBM Tivoli Monitoring: Active Directory Agent. Messages and trace data are sent to a file.

Trace data captures transient information about the current operating environment when a component or application fails to operate as designed. IBM Software Support personnel use the captured trace information to determine the source of an error or unexpected condition. See "Trace logging" on page 96 for more information.

Problem classification

The following types of problems might occur with the IBM Tivoli Monitoring: Active Directory Agent:

- Installation and configuration
- General usage and operation
- Display of monitoring data
- Take Action commands

This appendix provides symptom descriptions and detailed workarounds for these problems, as well as describing the logging capabilities of the monitoring agent. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Trace logging

Trace logs capture information about the operating environment when component software fails to operate as intended. The principal log type is the RAS (Reliability, Availability, and Serviceability) trace log. These logs are in the English language only. The RAS trace log mechanism is available for all components of IBM Tivoli Monitoring. Most logs are located in a `logs` subdirectory on the host computer. See the following sections to learn how to configure and use trace logging:

- "Principal trace log files" on page 97
- "Examples: using trace logs" on page 99
- "Setting RAS trace parameters" on page 100

Note: The documentation refers to the RAS facility in IBM Tivoli Monitoring as "RAS1".

IBM Software Support uses the information captured by trace logging to trace a problem to its source or to determine why an error occurred. The default configuration for trace logging, such as whether trace logging is enabled or disabled and trace level, depends on the source of the trace logging. Trace logging is always enabled.

Overview of log file management

Table 15 on page 98 provides the names, locations, and descriptions of RAS1 log files. The log file names adhere to the following naming convention:

hostname_product_program_timestamp-nn`.log`

where:

- *hostname* is the host name of the machine on which the monitoring component is running.
- *product* is the two-character product code. For Monitoring Agent for Active Directory, the product code is 3z.
- *program* is the name of the program being run.
- *timestamp* is an 8-character hexadecimal timestamp representing the time at which the program started.
- *nn* is a rolling log suffix. See "Examples of trace logging" on page 97 for details of log rolling.

Examples of trace logging

For example, if a Active Directory monitoring agent is running on computer ″server01″, the RAS log file for the Monitoring Agent for Active Directory might be named as follows:

```
server01_3z_k3zcma_437fc59-01.log
```

For long-running programs, the *nn* suffix is used to maintain a short history of log files for that startup of the program. For example, the k3zcma program might have a series of log files as follows:

```
server01_3z_k3zcma_437fc59-01.log
server01_3z_k3zcma_437fc59-02.log
server01_3z_k3zcma_437fc59-03.log
```

As the program runs, the first log (*nn*=01) is preserved because it contains program startup information. The remaining logs ″roll." In other words, when the set of numbered logs reach a maximum size, the remaining logs are overwritten in sequence.

Each time a program is started, a new timestamp is assigned to maintain a short program history. For example, if the Monitoring Agent for Active Directory is started twice, it might have log files as follows:

```
server01_3z_k3zcma_437fc59-01.log
server01_3z_k3zcma_437fc59-02.log
server01_3z_k3zcma_437fc59-03.log

server01_3z_k3zcma_537fc59-01.log
server01_3z_k3zcma_537fc59-02.log
server01_3z_k3zcma_537fc59-03.log
```

Each program that is started has its own log file. For example, the Monitoring Agent for Active Directory would have agent logs in this format:

```
server01_3z_k3zcma_437fc59-01.log
```

Other logs, such as logs for collector processes and Take Action commands, have a similar syntax as in the following example:

```
server01_3z_k3zpgm_447fc59-01.log
```

where **k3zpgm** is the program name.

Note: When you communicate with IBM Software Support, you must capture and send the RAS1 log that matches any problem occurrence that you report.

Principal trace log files

Table 15 on page 98 contains locations, file names, and descriptions of trace logs that can help determine the source of problems with agents.

Table 15. Trace log files for troubleshooting agents

System where log is located	File name and path	Description
On the computer that hosts the monitoring agent See "Definitions of variables" on page 99 for descriptions of the variables in the file names in column two.	The RAS1 log files are named *hostname*_3z_*program*_*timestamp*-*nn*.log and are located in the *install_dir*\tmaitm6\logs path. **Note:** File names for RAS1 logs include a hexadecimal time stamp.	Traces activity of the monitoring agent. **Note:** Other logs, such as logs for collector processes and Take Action commands (if available), have a similar syntax and are located in this directory path.
	The *.LG0 file is located in the *install_dir*\tmaitm6\logs path.	A new version of this file is generated every time the agent is restarted. IBM Tivoli Monitoring generates one backup copy of the *.LG0 file with the tag .LG1. View .LG0 to learn the following details regarding the current monitoring session: • Status of connectivity with the monitoring server. • Situations that were running. • The success or failure status of Take Action commands.
On the Tivoli Enterprise Monitoring Server See "Definitions of variables" on page 99 for descriptions of the variables in the file names in column two.	**On UNIX:** The candle_installation.log file in the *install_dir*/logs path. **On Windows:** The file in the *install_dir*\InstallITM path.	Provides details about products that are installed. **Note:** Trace logging is enabled by default. A configuration step is not required to enable this tracing.
	The Warehouse_Configuration.log file is located in the following path on Windows: *install_dir*\InstallITM.	Provides details about the configuration of data warehousing for historical reporting.
	The RAS1 log file is named *hostname*_ms_*timestamp*-*nn*.log and is located in the following path: • **On Windows:** *install_dir*\logs • **On UNIX:** *install_dir*/logs **Note:** File names for RAS1 logs include a hexadecimal time stamp **Also on UNIX, a log with a decimal time stamp is provided:** *hostname*_ms_*timestamp*.log and *hostname*_ms_*timestamp*.pid*nnnnn* in the *install_dir*/*logs* path, where *nnnnn* is the process ID number.	Traces activity on the monitoring server.

Table 15. Trace log files for troubleshooting agents (continued)

System where log is located	File name and path	Description
On the Tivoli Enterprise Portal Server See "Definitions of variables" for descriptions of the variables in the file names in column two.	The RAS1 log file is named *hostname*_cq_*timestamp-nn*.log and is located in the following path: • **On Windows:** *install_dir*\logs • **On UNIX:** *install_dir*/logs **Note:** File names for RAS1 logs include a hexadecimal time stamp **Also on UNIX, a log with a decimal time stamp is provided:** *hostname*_cq_*timestamp*.log and *hostname*_cq_*timestamp*.pid*nnnnn* in the *install_dir/logs* path, where *nnnnn* is the process ID number.	Traces activity on the portal server.
	The TEPS_ODBC.log file is located in the following path on Windows: *install_dir*\InstallITM.	When you enable historical reporting, this log file traces the status of the warehouse proxy agent.
Definitions of variables for RAS1 logs: • *hostname* is the host name of the machine on which the agent is running. • *install_dir* represents the directory path where you installed the IBM Tivoli Monitoring component. *install_dir* can represent a path on the computer that hosts the monitoring server, the monitoring agent, or the portal server. • *product* is the two character product code. For Monitoring Agent for Active Directory, the product code is 3z. • *program* is the name of the program being run. • *timestamp* is an eight-character hexadecimal time stamp representing the time at which the program started. • *nn* is a rolling log suffix. See "Examples of trace logging" on page 97 for details of log rolling.		

See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on the complete set of trace logs that are maintained on the monitoring server.

Examples: using trace logs

Typically IBM Software Support applies specialized knowledge to analyze trace logs to determine the source of problems. However, you can open trace logs in a text editor such as **vi** to learn some basic facts about your IBM Tivoli Monitoring environment. You can use the **ls -ltr** command to list the log files in the *install_dir*/logs directories, sorted by time they were last updated.

Example one

This excerpt shows the typical log for a failed connection between a monitoring agent and a monitoring server with the host name **server1a**:

```
(Thursday, August 11, 2005, 08:21:30-{94C}kdcl0cl.c,105,"KDCL0_ClientLookup") status=1c020006,
    "location server unavailable", ncs/KDC1_STC_SERVER_UNAVAILABLE
(Thursday, August 11, 2005, 08:21:35-{94C}kraarreg.cpp,1157,"LookupProxy") Unable to connect to
    broker at ip.pipe:: status=0, "success", ncs/KDC1_STC_OK
(Thursday, August 11, 2005, 08:21:35-{94C}kraarreg.cpp,1402,"FindProxyUsingLocalLookup") Unable
    to find running CMS on CT_CMSLIST <IP.PIPE:#server1a>
```

Example two

The following excerpts from the trace log *for the monitoring server* show the status of an agent, identified here as "Remote node." The name of the computer where the agent is running is **SERVER5B**:

```
(42C039F9.0000-6A4:kpxreqhb.cpp,649,"HeartbeatInserter") Remote node SERVER5B:K3Z is ON-LINE.
. . .
(42C3079B.0000-6A4:kpxreqhb.cpp,644,"HeartbeatInserter") Remote node SERVER5B:K3Z is OFF-LINE.
```

Key points regarding the preceding excerpt:

- The monitoring server appends the **K3Z** product code to the server name to form a unique name (`SERVER5B:K3Z`) for this instance of Monitoring Agent for Active Directory. This unique name enables you to distinguish multiple monitoring products that might be running on **SERVER5B**.
- The log shows when the agent started (ON-LINE) and later stopped (OFF-LINE) in the environment.
- For the sake of brevity an ellipsis (...) represents the series of trace log entries that were generated while the agent was running.
- Between the ON-LINE and OFF-LINE log entries, the agent was communicating with the monitoring server.
- The ON-LINE and OFF-LINE log entries are always available in the trace log. All trace levels that are described in "Setting RAS trace parameters" provide these entries.

On Windows, you can use the following method to view trace logs:

1. In the Windows **Start** menu, choose **Program Files > IBM Tivoli Monitoring > Manage Tivoli Monitoring Service**. The Manage Tivoli Enterprise Monitoring Services window is displayed.
2. Right-click a component and select **Advanced > View Trace Log** in the pop-up menu. The program displays the Select Log File window that lists the RAS1 logs for the monitoring agent.
3. Select a log file from the list and click **OK**. You can also use this viewer to access remote logs.

   Note: The viewer converts time stamps in the logs to a readable format.

Setting RAS trace parameters

Objective

Pinpoint a problem by setting detailed tracing of individual components of the monitoring agent and modules.

Background Information

Monitoring Agent for Active Directory uses RAS1 tracing and generates the logs described in Table 15 on page 98. The default RAS1 trace level is ERROR.

RAS1 tracing has control parameters to manage to the size and number of RAS1 logs. Use the procedure described in this section to set the parameters.

Note: The **KBB_RAS1_LOG** parameter also provides for the specification of the log file directory, log file name, and the inventory control file directory and name. Do not modify these values or log information can be lost.

Before you begin

See "Overview of log file management" on page 96 to ensure that you understand log rolling and can reference the correct log files when you managing log file generation.

After you finish

Monitor the size of the **logs** directory. Default behavior can generate a total of 45 to 60 MB for each agent that is running on a computer. For example, each database instance that you monitor could generate 45 to 60 MB of log data. See the

"Procedure" section to learn how to adjust file size and numbers of log files to prevent logging activity from occupying too much disk space.

Regularly prune log files other than the RAS1 log files in the **logs** directory. Unlike the RAS1 log files which are pruned automatically, other log types can grow indefinitely, for example, the logs in Table 15 on page 98 that include a process ID number (PID).

Consider using collector trace logs (described in Table 15 on page 98) as an additional source of problem determination information.

Note: The **KDC_DEBUG** setting and the Maximum error tracing setting can generate a large amount of trace logging. Use them only temporarily, while you are troubleshooting problems. Otherwise, the logs can occupy excessive amounts of hard disk space.

Procedure

Specify RAS1 trace options in the **K3ZENV** file. You can manually edit the configuration file to set trace logging:

1. Open the trace options file: *install_dir*\tmaitm6\K3ZENV.
2. Edit the line that begins with **KBB_RAS1=** to set trace logging preferences.

   For example, if you want detailed trace logging, set the Maximum Tracing option:

   ```
   KBB_RAS1=ERROR (UNIT:k3z ALL) (UNIT:kra ALL)
   ```
3. Edit the line that begins with **KBB_RAS1_LOG=** to manage the generation of log files:
   - Edit the following parameters to adjust the number of rolling log files and their size.
     - **MAXFILES**: the total number of files that are to be kept for all startups of a given program. Once this value is exceeded, the oldest log files are discarded. Default value is 9.
     - **LIMIT**: the maximum size, in megabytes (MB) of a RAS1 log file. Default value is 5.
   - IBM Software Support might guide you to modify the following parameters:
     - **COUNT**: the number of log files to keep in the rolling cycle of one program startup. Default value is 3.
     - **PRESERVE**: the number of files that are not to be reused in the rolling cycle of one program startup. Default value is 1.

   Note: The **KBB_RAS1_LOG** parameter also provides for the specification of the log file directory, log file name, and the inventory control file directory and name. Do not modify these values or log information can be lost.
4. Restart the monitoring agent so that your changes take effect.

(*Windows only*) **Alternate method to edit trace logging parameters:**

1. Open the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click the icon of the monitoring agent whose logging you want to modify.
3. Select **Advanced** > **Edit Trace Parms**. The Tivoli Enterprise Monitoring Server Trace Parameters window is displayed.
4. Select a new trace setting in the pull-down menu in the **Enter RAS1 Filters** field or type a valid string.

The selections are as follows:

- No error tracing. `KBB_RAS1=-none-`
- General error tracing. `KBB_RAS1=ERROR`
- Intensive error tracing. `KBB_RAS1=ERROR (UNIT:k3z ALL)`
- Maximum error tracing. `KBB_RAS1=ERROR (UNIT:k3z ALL) (UNIT:kra ALL)`

Note: As this example shows, you can set multiple RAS tracing options in a single statement.

5. Modify the value for ″Maximum Log Size Per File (MB)″ to change the log file size (changes LIMIT value).
6. Modify the value for ″Maximum Number of Log Files Per Session″ to change the number of logs files per startup of a program (changes COUNT value).
7. Modify the value for ″Maximum Number of Log Files Total″ to change the number of logs files for all startups of a program (changes MAXFILES value).
8. (*Optional*) Click Y (Yes) in the **KDC_DEBUG Setting** menu to log information that can help you diagnose communications and connectivity problems between the monitoring agent and the monitoring server.

   Note: The **KDC_DEBUG** setting and the Maximum error tracing setting can generate a large amount of trace logging. Use them only temporarily, while you are troubleshooting problems. Otherwise, the logs can occupy excessive amounts of hard disk space.
9. Click **OK**. You see a message reporting a restart of the monitoring agent so that your changes take effect.

Problems and workarounds

The following sections provide symptoms and workarounds for problems that might occur with Monitoring Agent for Active Directory:

- “Installation and configuration problem determination” on page 102
- “Agent problem determination” on page 107
- “Workspace problem determination” on page 110
- “Problem determination for remote deployment” on page 109
- “Situation problem determination” on page 111

Note: You can resolve some problems by ensuring that your system matches the system requirements listed in Chapter 2, “Requirements for the monitoring agent,” on page 5.

This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Installation and configuration problem determination

This section provides tables that show solutions for installation, configuration, and uninstallation problems.

Table 16. Problems and solutions for installation and configuration

Problem	Solution
When you upgrade to IBM Tivoli Monitoring, you might need to apply fixpacks to Candle®, Version 350, agents.	Fixpacks for Candle, Version 350, are delivered as each monitoring agent is upgraded to IBM Tivoli Monitoring. **Note:** The IBM Tivoli Monitoring download image or CD provides application fixpacks for the monitoring agents that are installed from that CD (for example, the agents for operating systems such as Windows, Linux®, UNIX, and i5/OS®). The upgrade software for other agents is located on the download image or CDs for that specific monitoring agent, such as the agents for database applications. If you do not upgrade the monitoring agent to IBM Tivoli Monitoring, the agent continues to work. However, you must upgrade to have all the functionality that IBM Tivoli Monitoring offers.
The following message is displayed in the installation log for some Windows agents when upgrading from Tivoli OMEGAMON® V350: `<REPLACELINE> Pair missing 1=[KBB_RAS1=ERROR] no 2, skipped.`	There is no workaround. The previous value of KBB_RAS1 from the OMEGAMON V350 agent is used, preserving prior customer settings for this variable. The problem has no adverse effect on the installation or subsequent operation of the monitoring agent .
Presentation files and customized OMEGAMON screens for Candle monitoring agents need to be upgraded to a new Linux on z/Series system.	The upgrade from version 350 to IBM Tivoli Monitoring handles export of the presentation files and the customized OMEGAMON screens.
(*UNIX only*) During a command-line installation, you choose to install a component that is already installed, and you see the following warning: `WARNING - you are about to install the SAME version of "component"` where *component* is the name of the component that you are attempting to install. **Note:** This problem affects UNIX command-line installations. If you monitor only Windows environments, you would see this problem if you choose to install a product component (for example, a monitoring server) on UNIX.	You must exit and restart the installation process. You cannot return to the list where you selected components to install. When you run the installer again, do not attempt to install any component that is already installed.
A problem can arise when you install and configure a new monitoring agent to a computer where other agents are running as described in this example: • Agents are running on computer and communicating with a Tivoli Enterprise Monitoring Server, called **TEMS1**. • You install a new agent on the same computer and you want this agent to communicate with a different monitoring server, called **TEMS2**. • When you configure the new agent to communicate with **TEMS2**, all the existing agents are re-configured to communicate with **TEMS2**.	You must reconfigure the previously existing agents to restore their communication connection with **TEMS1**. For example, you can right-click the row for a specific agent in the Manage Tivoli Enterprise Monitoring Services, and select **Reconfigure**. See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on reconfiguration.

Table 16. Problems and solutions for installation and configuration (continued)

Problem	Solution
Error Message - Could not open DNS registry key	This message is informational only. No action is required. The Windows agent reports the fact that it could not find a registry entry for the DNS Server Event Log. This means that the DNS Server Event Log is not installed. To clear this error message, stop all situations and recycle the Tivoli Enterprise Monitoring Server, making sure that you have no situations set to ACTIVATE AT STARTUP. In this case, no message would be written to the trace log.
Diagnosing problems with product browse settings.	When you have problems with browse settings, perform the following steps: 1. Click on **Start > Programs > IBM Tivoli Monitoring > Manage Tivoli Enterprise Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services is displayed. 2. Right-click the Monitoring Agent for Active Directory and select **Browse Settings**. A text window is displayed. 3. Click **Save As** and save the information in the text file. If requested, you can forward this file to IBM Software Support for analysis.
A message similar to ″Unable to find running CMS on CT_CMSLIST″ in the log file is displayed.	If a message similar to ″Unable to find running CMS on CT_CMSLIST″ is displayed in the Log file, the agent is not able to connect to the monitoring server. Confirm the following points: • Do multiple network interface cards (NICs) exist on the system? • If multiple NICs exist on the system, find out which one is configured for the monitoring server. Ensure that you specify the correct host name and port settings for communication in the IBM Tivoli Monitoring environment.
The system is experiencing high CPU usage.	**Agent process:** View the memory usage of the K3ZCMA process. If CPU usage seems to be excessive, recycle the monitoring agent. **Network Cards:** The network card configurations can decrease the performance of a system. Each of the stream of packets that a network card receives (assuming it is a broadcast or destined for the under-performing system) must generate a CPU interrupt and transfer the data through the I/O bus. If the network card in question is a bus-mastering card, work can be off-loaded and a data transfer between memory and the network card can continue without using CPU processing power. Bus-mastering cards are generally 32-bit and are based on PCI or EISA bus architectures.
You successfully migrate an OMEGAMON monitoring agent to IBM Tivoli Monitoring, Version 6.2.0. However, when you configure historical data collection, you see an error message that includes, `Attribute name may be invalid, or attribute file not installed for warehouse agent`.	Install the agent's application support files on the Tivoli Enterprise Monitoring Server, using the following steps: 1. Open the Manage Tivoli Enterprise Monitoring Services window. 2. Right-click the name of the monitoring server. 3. Select **Advanced > Add TEMS Application Support** in the pop-up menu. Add application support if any for any agent that is missing from the list. See in IBM Tivoli Monitoring Installation and Setup Guide for more information on adding application support. Ensure that the agent's application support files are pushed to the system that houses the Warehouse Proxy Agent. The Warehouse Proxy must be able to access the short attribute names for tables and columns. That way, if the longer versions of these names exceed the limits of the Warehouse database, the shorter names can be substituted.

Table 16. Problems and solutions for installation and configuration (continued)

Problem	Solution
Historical Data Collection loses Summarization and Pruning settings during upgrade from IBM Tivoli Monitoring: Active Directory Agent v6.1 to IBM Tivoli Monitoring: Active Directory Agent v6.2.	Reconfiguring, unconfiguring, restarting the attribute groups failed to keep the settings. The problem only applies to IBM Tivoli Monitoring: Active Directory Agent v6.1 install images acquired before June 2006 that have not been updated to Fix Pack 1 level or above. This is a known limitation for the agent. When updating IBM Tivoli Monitoring: Active Directory Agent v6.1, note the current Summarization and Pruning settings and reapply those settings after upgrade.

Table 17. General problems and solutions for uninstallation

Problem	Solution
On Windows, uninstallation of IBM Tivoli Monitoring fails to uninstall the entire environment.	Be sure that you follow the general uninstallation process described in the *IBM Tivoli Monitoring Installation and Setup Guide*: 1. Uninstall monitoring agents first, as in the following examples: • Uninstall a single monitoring agent for a specific database. —OR— • Uninstall all instances of a monitoring product, such as IBM Tivoli Monitoring for Databases. 2. Uninstall IBM Tivoli Monitoring. See the *IBM Tivoli Monitoring Problem Determination Guide* and the section on installation problems for more information on how to remove the entire environment.
The way to remove inactive managed systems (systems whose status is OFFLINE) from the Enterprise navigation tree in the portal is not obvious.	When you want to remove a managed system from the navigation tree, complete the following steps: 1. Click **Enterprise** in the navigation tree. 2. Right-click **Workspace -> Managed System Status**. 3. Right-click the offline managed system and select **Clear offline entry**.

Unique names for monitoring components

If you have multiple instances of a monitoring agent, you must decide how to name the monitoring agents. This name is intended to uniquely identify that monitoring agent. The agent's default name is composed of three qualifiers:

- Optional instance name
- Machine network hostname
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network hostname portion of the agent name. For example, instead of just the hostname myhost1 being used, the resulting hostname might be myhost1.acme.north.prod.com. Inclusion of the network domain name causes the agent name in the example above to expand to SERVER1:myhost1.acme.north.prod.com:KXX. This resulting name is 39 characters long. It is truncated to 32 characters resulting in the name SERVER1:myhost1.acme.north.prod.

The agent name truncation is only a problem if there is more than one monitoring agent on the same system. In this case, the agent name truncation can result in collisions between agent products attempting to register using the same truncated name value. When truncated agent names collide on the same system, this can lead

to Tivoli Enterprise Monitoring Server problems with corrupted EIB tables. The agent name collision in the Tivoli Enterprise Monitoring Server might cause a registered name to be associated with the wrong product.

In general, create names that are short but meaningful within your environment. Use the following guidelines:

- Each name must be unique. One name cannot match another monitoring agent name exactly.
- Each name must begin with an alpha character.
- Do not use blanks or special characters, including $, #, and @.
- Each name must be between 2 and 32 characters in length.
- Monitoring agent naming is case-sensitive on all operating systems.

Create the names by completing the following steps:

1. Open the configuration file for the monitoring agent, which is located in the following path:
   - **On Windows:** *install_dir*\tmaitm6\K*product_code*CMA.INI. For example, the product code for the Monitoring Agent for Windows OS is NT file name for is KNTCMA.INI.
   - **On UNIX and Linux:** *install_dir*/tmaitm6/*product_code*.ini and *product_code*.config. For example, the file names for the Monitoring Agent for UNIX OS is ux.ini and ux.config.
2. Find the line the begins with **CTIRA_HOSTNAME=**.
3. Type a new name for host name that is a unique, shorter name for the host computer. The final concatenated name including the subsystem name, new host name, and 3Z, cannot be longer than 32 characters.

   Note: You must ensure that the resulting name is unique with respect to any existing monitoring component that was previously registered with the Tivoli Enterprise Monitoring Server.
4. Save the file.
5. Restart the agent.
6. If you do not find the files mentioned in Step 1, perform the workarounds listed in the next paragraph.

If you do not find the files mentioned in the preceding steps, perform the following workarounds:

1. Change **CTIRA_HOSTNAME** environment variable in the configuration file of the monitoring agent.
   - Find the K3ZENV file in the same path mentioned in the preceding row.
   - For z/OS® agents, find the **RKANPAR** library.
   - For i5/OS agents, find the **QAUTOTMP/KMSPARM** library in member **KBBENV**.
2. If you cannot find the **CTIRA_HOSTNAME** environment variable, you must add it to the configuration file of the monitoring agent:
   - **On Windows:** Use the **Advanced > Edit Variables** option.
   - **On UNIX and Linux:** Add the variable to the config/*product_code*.ini and to config/*product_code*.config files.
   - **On z/OS:** Add the variable to the **RKANPAR** library, member K*product_code*ENV.

- **On i5/OS:** Add the variable to the **QAUTOTMP/KMSPARM** library in member **KBBENV**.

3. Some monitoring agents (for example, the monitoring agent for MQ Series) do not reference the **CTIRA_HOSTNAME** environment variable to generate component names. Check the documentation for the monitoring agent that you are using for information on name generation. If necessary, contact IBM Software Support.

Agent problem determination

This section lists problems that might occur with agents.

This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Table 18. Agent problems and solutions

Problem	Solution
A configured and running instance of the monitoring agent is not displayed in the Tivoli Enterprise Portal, but other instances of the monitoring agent on the same system do appear in the portal.	Tivoli Monitoring products use Remote Procedure Call (RPC) to define and control product behavior. RPC is the mechanism that allows a client process to make a subroutine call (such as GetTimeOfDay or ShutdownServer) to a server process somewhere in the network. Tivoli processes can be configured to use TCP/UDP, TCP/IP, SNA, and SSL as the desired protocol (or delivery mechanism) for RPCs. "IP.PIPE" is the name given to Tivoli TCP/IP protocol for RPCs. The RPCs are socket-based operations that use TCP/IP ports to form socket addresses. IP.PIPE implements virtual sockets and multiplexes all virtual socket traffic across a single physical TCP/IP port (visible from the netstat command). A Tivoli process derives the physical port for IP.PIPE communications based on the configured, well-known port for the HUB Tivoli Enterprise Monitoring Server. (This well-known port or BASE_PORT is configured using the 'PORT:' keyword on the KDC_FAMILIES / KDE_TRANSPORT environment variable and defaults to '1918'.) The physical port allocation method is defined as (BASE_PORT + 4096*N) where N=0 for a Tivoli Enterprise Monitoring Server process and N={1, 2, ..., 15} for a non-Tivoli Enterprise Monitoring Server. Two architectural limits result as a consequence of the physical port allocation method: • No more than one Tivoli Enterprise Monitoring Server reporting to a specific Tivoli Enterprise Monitoring Server HUB can be active on a system image. • No more that 15 IP.PIPE processes can be active on a single system image. A single system image can support any number of Tivoli Enterprise Monitoring Server processes (address spaces) provided that each Tivoli Enterprise Monitoring Server on that image reports to a different HUB. By definition, there is one Tivoli Enterprise Monitoring Server HUB per monitoring Enterprise, so this architecture limit has been simplified to one Tivoli Enterprise Monitoring Server per system image. No more that 15 IP.PIPE processes or address spaces can be active on a single system image. With the first limit expressed above, this second limitation refers specifically to Tivoli Enterprise Monitoring Agent processes: no more that 15 agents per system image. This limitation can be circumvented (at current maintenance levels, IBM Tivoli Monitoring V6.1 Fix Pack 4 and later) if the Tivoli Enterprise Monitoring Agent process is configured to use EPHEMERAL IP.PIPE. (This is IP.PIPE configured with the 'EPHEMERAL:Y' keyword in the KDC_FAMILIES / KDE_TRANSPORT environment variable). There is no limitation to the number of ephemeral IP.PIPE connections per system image. However, EPHEMERAL endpoints are restricted: data warehousing cannot be performed on an ephemeral endpoint.

Table 18. Agent problems and solutions (continued)

Problem	Solution
After an attempt to restart the agents in the Tivoli Enterprise Portal, the agents are still not running.	For UNIX, NetWare, or Windows, log on to the applicable system and perform the appropriate queries.
Attributes do not allow non-ASCII input in the situation editor.	None. Any attribute that does not include ″(Unicode)″ -- for example, ″Description (Unicode)″ might support only ASCII characters.
No performance data is displayed in workspace views, no data is available for situations, and no data is available for historical logging.	When the Windows operating system detects a problem in one of its extensible performance monitoring DLL files, it marks the DLL as ″disabled.″ Any DLL that is disabled cannot provide performance data through the Windows Performance Monitor interfaces (Perfmon or Performance Monitor APIs). This prevents IBM Tivoli Monitoring agents from gathering data supplied by the disabled DLL. For more information, see Microsoft Support Knowledge Base article 248993 at the following Web address: http://support.microsoft.com/default.aspx?scid=kb;EN-US;248993 Follow the Resolution instructions provided in this article (248993) to re-enable any performance monitoring extension DLL files disabled by Windows. Then, restart the monitoring agent.
The monitoring agent fails to run.	If the Windows Support Tools utility is missing, the monitoring agent fails to run. Install the Windows Support Tools that come with the operating system. See the downloaded installation image or the installation CDs. You might also need to load the IADsTools.dll. See Chapter 2, “Requirements for the monitoring agent,” on page 5 for further information.
When you edit the configuration for an existing monitoring agent, the values displayed are not correct.	The original configuration settings might include non-ASCII characters. These values were stored incorrectly and result in the incorrect display. Enter new values using only ASCII characters.

Problem determination for remote deployment

Table 19 on page 110 lists problems that might occur with remote deployment. This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

This section describes problems and solutions for remote deployment and removal of agent software Agent Remote Deploy:

Table 19. Remote deployment problems and solutions

Problem	Solution
While you are using the remote deployment feature to install Monitoring Agent for Active Directory, an empty command window is displayed on the target computer. This problem occurs when the target of remote deployment is a Windows computer. (See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on the remote deployment feature.)	Do not close or modify this window. It is part of the installation process and will be dismissed automatically.
The removal of a monitoring agent fails when you use the remote removal process in the Tivoli Enterprise Portal desktop or browser.	This problem might happen when you attempt the remote removal process immediately after you have restarted the Tivoli Enterprise Monitoring Server. You must allow time for the monitoring agent to refresh its connection with the Tivoli Enterprise Monitoring Server before you begin the remote removal process.

Workspace problem determination

Table 20 shows problems that might occur with workspaces. This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Table 20. Workspace problems and solutions

Problem	Solution
You see the following message: `KFWITM083W Default link is disabled for the selected object; please verify link and link anchor definitions.`	You see this message because some links do not have default workspaces. Right-click the link to access a list of workspaces to select.
The name of the attribute does not display in a bar chart or graph view.	When a chart or graph view that includes the attribute is scaled to a small size, a blank space is displayed instead of a truncated name. To see the name of the attribute, expand the view of the chart until there is sufficient space to display all characters of the attribute's name.
You start collection of historical data but the data cannot be seen.	Managing options for historical data collection: • Basic historical data collection populates the Warehouse with raw data. This type of data collection is turned off by default. See Chapter 2, "Requirements for the monitoring agent," on page 5 for information on managing this feature including how to set the interval at which data is collected. By setting a more frequent interval for data collection you reduce the load on the system incurred every time data is uploaded. • You use the Summarization and Pruning monitoring agent to collect specific amounts and types of historical data. Be aware that historical data is not displayed until the Summarization and Pruning monitoring agent begins collecting the data. By default, this agent begins collection at 2 AM daily. At that point, data is visible in the workspace view. See the IBM Tivoli Monitoring Administrator's Guide to learn how to modify the default collection settings.
At the bottom of each view, you see the following Historical workspace KFWITM220E error: **Request failed during execution**, and a red icon.	Ensure that you configure all groups that supply data to the view. In the Historical Configuration view, ensure that data collection is started all groups that supply data to the view.

Situation problem determination

This section provides information about both general situation problems and problems with the configuration of situations. See the *IBM Tivoli Monitoring Problem Determination Guide* for more information about problem determination for situations.

Situation problems and solutions

Table 21 lists problems that might occur with specific situations.

Table 21. Specific situation problems and solutions

Problem	Solution
You want to change the appearance of situations when they are displayed in a Workspace view.	1. Right-click an item in the Navigation tree. 2. Select **Situations** in the pop-up menu. The Situation Editor window is displayed. 3. Select the situation that you want to modify. 4. Use the **Status** pull-down menu in the lower right of the window to set the status and appearance of the Situation when it triggers. **Note:** This status setting is not related to severity settings in IBM Tivoli Enterprise Console.
Situations are triggered in the Tivoli Enterprise Monitoring Server, but events for the situation are not sent to the Tivoli Enterprise Console server. The Tivoli Enterprise Monitoring Server is properly configured for event forwarding, and events for many other situations are sent to the event server.	This condition can occur when a situation is only monitoring the status of other situations. The event forwarding function requires an attribute group reference in the situation in order to determine the correct event class to use in the event. When the situation only monitors other situations, no attribute groups are defined and the event class cannot be determined. Because the event class cannot be determined, no event is sent. This is a limitation of the Tivoli Enterprise Monitoring Server event forwarding function. Situations that only monitor other situations do not send events to the event server.
Monitoring activity requires too much disk space.	Check the RAS trace logging settings that are described in “Setting RAS trace parameters” on page 100. For example, trace logs grow rapidly when you apply the **ALL** logging option.
A formula that uses mathematical operators appears to be incorrect. For example, if you were monitoring Linux, a formula that calculates when **Free Memory** falls under 10 percent of **Total Memory** does not work: `LT #'Linux_VM_Stats.Total_Memory' / 10`	This formula is incorrect because situation predicates support only logical operators. Your formulas cannot have mathematical operators. **Note:** The Situation Editor provides alternatives to math operators. Regarding the example, you can select **% Memory Free** attribute and avoid the need for math operators.
Situations that you create display the severity UNKNOWN in IBM Tivoli Enterprise Console.	For a situation to have the correct severity in TEC for those situations which are not mapped, you need to ensure that an entry exists in the **tecserver.txt** file for the situation and that **SEVERITY** is specified. See the “Configuring Tivoli Enterprise Console integration” chapter in the *IBM Tivoli Monitoring Administrator's Guide* for more information.
You see the 'Unable to get attribute name' error in the Tivoli Enterprise Monitoring Server log after creating a situation.	Install the agent's application support files on the Tivoli Enterprise Monitoring Server, using the following steps: 1. Open the Manage Tivoli Enterprise Monitoring Services window. 2. Right-click the name of the monitoring server. 3. Select **Advanced > Add TEMS Application Support** in the pop-up menu. Add application support if any for any agent that is missing from the list. See in IBM Tivoli Monitoring Installation and Setup Guide for more information on adding application support.

Table 21. Specific situation problems and solutions (continued)

Problem	Solution
Events received at the Tivoli Enterprise Console server from IBM Tivoli Monitoring do not have values for all event attributes (slots) even though the values are visible in workspace views.	The problem is due to a limitation in the IBM Tivoli Monitoring interface code that generates Tivoli Enterprise Console events from situations. The situation results are provided in a chain of buffers of 3000 bytes each. The interface code currently extracts event information from only the first buffer. When situations or agent table data expands into a second buffer, this additional data is not examined, and it is not included in events sent to the Tivoli Enterprise Console server.
Tivoli Enterprise Console events from IBM Tivoli Monitoring 6.2 for IBM Tivoli Monitoring 5.x migrated situations receive parsing errors in the Tivoli Enterprise Console server.	Complete the following two steps: 1. Ensure that you have the IBM Tivoli Monitoring 6.2 Event Sync installed on your Tivoli Enterprise Console server. 2. Obtain updated baroc files from IBM Tivoli Monitoring 6.2 for the monitoring agent's events. Updated baroc files are on the Tivoli Enterprise Monitoring Server in the *CANDLEHOME*/CMS/TECLIB/itm5migr directory.
You are receiving Tivoli Business Systems Management events that cannot be associated due to application_oid and application_class not being set.	The problem is due to IBM Tivoli Monitoring 6.2 sending Tivoli Enterprise Console events for IBM Tivoli Monitoring 5.x migrated situations. These events are not able to set the cited slot values. Replace the *agent_name*_forward_tbsm_event_cb.sh script on the Tivoli Enterprise Console server with the version of this file from the Tivoli Enterprise Monitoring Server in the CANDLEHOME/CMS/TECLIB/itm5migr directory.

Problems with configuration of situations

Table 22 lists problems that might occur with situations.

This section provides information for problem determination for agents. Be sure to consult the *IBM Tivoli Monitoring Problem Determination Guide* for more general problem determination information.

Table 22. Problems with configuring situations that you solve in the Situation Editor

Problem	Solution
Note: To get started with the solutions in this section, perform these steps: 1. Launch the Tivoli Enterprise Portal. 2. Click **Edit > Situation Editor**. 3. In the tree view, choose the agent whose situation you want to modify. 4. Choose the situation in the list. The Situation Editor view is displayed.	
The situation for a specific agent is not visible in the Tivoli Enterprise Portal.	Open the Situation Editor. Access the All managed servers view. If the situation is absent, confirm that application support for Monitoring Agent for Active Directory has been added to the monitoring server. If not, add application support to the server, as described in the *IBM Tivoli Monitoring Installation and Setup Guide.*
The monitoring interval is too long.	Access the Situation Editor view for the situation that you want to modify. Check the **Sampling interval** area in the **Formula** tab. Adjust the time interval as needed.
The situation did not activate at startup.	Manually recycle the situation as follows: 1. Right-click the situation and choose **Stop Situation**. 2. Right-click the situation and choose **Start Situation**. **Note:** You can permanently avoid this problem by placing a check mark in the **Run at Startup** option of the Situation Editor view for a specific situation.

Table 22. Problems with configuring situations that you solve in the Situation Editor (continued)

Problem	Solution
The situation is not displayed.	Click the **Action** tab and check whether the situation has an automated corrective action. This action can occur directly or through a policy. The situation might be resolving so quickly that you do not see the event or the update in the graphical user interface.
An Alert event has not occurred even though the predicate has been properly specified.	Check the logs, reports, and workspaces.
A situation fires on an unexpected managed object.	Confirm that you have distributed and started the situation on the correct managed system.
The product did not distribute the situation to a managed system.	Click the **Distribution** tab and check the distribution settings for the situation.
The situation does not fire. Incorrect predicates are present in the formula that defines the situation. For example, the managed object shows a state that normally triggers a monitoring event, but the situation is not true because the wrong attribute is specified in the formula.	In the **Formula** tab, analyze predicates as follows: 1. Click the *fx* icon in the upper-right corner of the Formula area. The Show formula window is displayed. a. Confirm the following details in the **Formula** area at the top of the window: • The attributes that you intend to monitor are specified in the formula. • The situations that you intend to monitor are specified in the formula. • The logical operators in the formula match your monitoring goal. • The numerical values in the formula match your monitoring goal. b. (*Optional*) Click the **Show detailed formula** check box in the lower left of the window to see the original names of attributes in the application or operating system that you are monitoring. c. Click **OK** to dismiss the Show formula window. 2. (*Optional*) In the Formula area of the **Formula** tab, temporarily assign numerical values that will immediately trigger a monitoring event. The triggering of the event confirms that other predicates in the formula are valid. **Note:** After you complete this test, you must restore the numerical values to valid levels so that you do not generate excessive monitoring data based on your temporary settings.

Table 23. Problems with configuration of situations that you solve in the Workspace area

Problem	Solution
Situation events are not displayed in the Events Console view of the workspace.	Associate the situation with a workspace. **Note:** The situation does not need to be displayed in the workspace. It is sufficient that the situation be associated with any workspace.
You do not have access to a situation.	**Note:** You must have administrator privileges to perform these steps. 1. Select **Edit** > **Administer Users** to access the Administer Users window. 2. In the Users area, select the user whose privileges you want to modify. 3. In the Permissions tab, Applications tab, and Navigator Views tab, select the permissions or privileges that correspond to the user's role. 4. Click **OK**.
A managed system seems to be offline.	1. Select Physical View and highlight the Enterprise Level of the navigator tree. 2. Select **View** > **Workspace** > **Managed System Status** to see a list of managed systems and their status. 3. If a system is offline, check network connectivity and status of the specific system or application.

Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- "Using IBM Support Assistant"
- "Obtaining fixes"
- "Contacting IBM Software Support" on page 115

Using IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

The IBM Support Assistant saves you the time it takes to search the product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, and to download the IBM Support Assistant Version 3, see http://www.ibm.com/software/support/isa. After you download and install the IBM Support Assistant, follow these steps to install the plug-in for IBM Tivoli Monitoring:

1. Start the IBM Support Assistant application.
2. Select **Updater** on the Welcome page.
3. Select **New Properties and Tools**.
4. Under Tivoli, select **IBM Tivoli Monitoring 6.2**, and then click **Install**. Be sure to read the license and description.
5. Restart the IBM Support Assistant.

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your Tivoli software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Under **Select a brand and/or product**, select **Tivoli** and click **Go**.
3. Under **Select a category**, select a product and click **Go**.
4. Under **Download**, click the name of a fix to read its description and, optionally, to download it.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. The easiest way to obtain that assistance is to open a PMR or ETR directly from the IBM Support Assistant (see "Using IBM Support Assistant" on page 114).

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and WebSphere® products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online

  Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm .

  By phone

  For the phone number to call in your country, go to the IBM Software Support Web site at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink™, CATIA, Linux, OS/390®, iSeries®, pSeries®, zSeries®, and other support agreements, go to the IBM Support Line Web site at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information" on page 116
3. "Submitting problems" on page 116

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Use the following criteria TO understand and assess the business impact of the problem that you are reporting:

Severity 1
The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4
The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- Which software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online
Click **Submit and track problems** on the IBM Software Support site athttp://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone
For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix E. Documentation library

This appendix contains information about the publications related to the Monitoring Agent for Active Directory. These publications are listed in the following categories:

- Monitoring Agent for Active Directory library
- Prerequisite publications
- Related publications

See the *IBM Tivoli Monitoring and OMEGAMON XE Products Documentation Guide*, for information about accessing and using publications. You can find the *IBM Tivoli Monitoring and OMEGAMON XE Products Documentation Guide* in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

To find a list of new and changed publications, click **What's new** on the Welcome page of the IBM Tivoli Monitoring and OMEGAMON XE Information Center. To find publications from the previous version of a product, click **Previous information centers** on the Welcome page for the product.

Monitoring Agent for Active Directory library

There is one document specific to the Monitoring Agent for Active Directory: *IBM Tivoli Monitoring: Active Directory Agent User's Guide*. This user's guide provides agent-specific reference and problem determination information for configuring and using the IBM Tivoli Monitoring for Active Directory Agent.

Use the configuration chapter in this guide with the *IBM Tivoli Monitoring Installation and Setup Guide* to set up the software.

Use the information in this guide with the *IBM Tivoli Monitoring User's Guide* to monitor Active Directory resources.

Prerequisite publications

To use the information in this publication effectively, you must have some prerequisite knowledge, which you can obtain from the following IBM Tivoli Monitoring publications:

- *Exploring IBM Tivoli Monitoring*
- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring Agent Builder User's Guide*
- *IBM Tivoli Monitoring Command Reference*
- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring: Messages*
- *IBM Tivoli Monitoring Migration Toolkit User's Guide*
- *IBM Tivoli Monitoring Problem Determination Guide*
- *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*
- *IBM Tivoli Monitoring User's Guide*
- *IBM Tivoli Monitoring: Upgrading from V5.1.2*

- *IBM Tivoli Monitoring Configuring Tivoli Enterprise Monitoring Server on z/OS*
- *IBM Tivoli Monitoring: Windows OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX OS Agent User's Guide*
- *IBM Tivoli Monitoring: Linux OS Agent User's Guide*
- *IBM Tivoli Monitoring: i5/OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX Log Agent User's Guide*
- *IBM Tivoli Monitoring Universal Agent User's Guide*
- *IBM Tivoli Monitoring Universal Agent API and Command Programming Reference Guide*
- *Introducing IBM Tivoli Monitoring Version 6.1.0*

Related publications

The following documents also provide useful information:

- *IBM Tivoli Enterprise Console Adapters Guide*
- *IBM Tivoli Enterprise Console Event Integration Facility User's Guide*
- *IBM Tivoli Enterprise Console Reference Manual*
- *IBM Tivoli Enterprise Console Rule Builder's Guide*

Other sources of documentation

You can also obtain technical documentation about Tivoli Monitoring and OMEGAMON XE products from the following sources:

- IBM Tivoli Open Process Automation Library (OPAL)

  http://www.ibm.com/software/tivoli/opal

  OPAL is an online catalog that contains integration documentation as well as other downloadable product extensions. This library is updated daily.
- Redbooks

  http://www.redbooks.ibm.com/

  IBM Redbooks®, Redpapers, and Redbooks Technotes provide information about products from platform and solution perspectives.
- Technotes

  You can find Technotes through the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html, or more directly through your product Web site, which contains a link to Technotes (under **Solve a problem**).

  Technotes provide the latest information about known product limitations and workarounds.

Appendix F. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in this product enable users to do the following:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Navigating the interface using the keyboard

Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Magnifying what is displayed on the screen

You can enlarge information on the product windows using facilities provided by the operating systems on which the product is run. For example, in a Microsoft Windows environment, you can lower the resolution of the screen to enlarge the font sizes of the text on the screen. Refer to the documentation provided by your operating system for more information.

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:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

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 systems. 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 system 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.

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

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

Trademarks

IBM, the IBM logo, IBMLink, AIX®, Candle, CandleNet Portal®, DB2, developerWorks®, eServer, i5/OS, iSeries, Lotus, MVS™, OMEGAMON, OS/390, Passport Advantage, pSeries, Rational, Redbooks, Tivoli, the Tivoli logo, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

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

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds 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, and service names may be trademarks or service marks of others.

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Printed in USA

SC32-9444-01