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

User's Guide - Beta 1 Draft

SC23-8879-07

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

User's Guide - Beta 1 Draft

SC23-8879-07

Note
Before using this information and the product it supports, read the information in "Notices" on page 241

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

Contents

Tables

Chapter 1. Overview of the agent

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

IBM® Tivoli® Monitoring is the base software for the Microsoft Active Directory agent. The Microsoft Active Directory agent monitors the following functions:

- Availability and resources
- Performance
- Error and event log
- Historical data

IBM Tivoli Monitoring

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

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

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

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

See the IBM Tivoli Monitoring publications listed in “Prerequisite publications” on page 237 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

New in this release

For the Microsoft Active Directory agent, the following enhancements have been made since version 6.3, including the fix packs:

- Modified attribute groups:
  - RID Pool Information
- Modified workspaces:
  - RID Pool Information
- New views:
  - Exhausted RID Status
- New situations:

- RID_Consumption_Crit
- Updated k3z.baroc file to support Tivoli Enterprise Console® event mapping

Components of the IBM Tivoli Monitoring environment

After you install the Microsoft Active Directory agent (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. This environment 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, Microsoft Active Directory agent, 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 an IBM 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.
- IBM Tivoli Enterprise Console® event synchronization component for synchronizing the status of situation events that are forwarded to the event server. When the status of an event is updated because of 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*.

Agent Management Services

You can use IBM Tivoli Monitoring Agent Management Services to manage the Microsoft Active Directory agent. These services are available in the following IBM Tivoli Monitoring OS agents: Windows, Linux, and UNIX. The services are designed to keep the Microsoft Active Directory agent available, and to provide information about the status of the product to the Tivoli Enterprise Portal. IBM Tivoli Monitoring V6.2.2, Fix Pack 2 or later provides support for Agent Management Services. For more information about Agent Management Services, see the *IBM Tivoli Monitoring Administrator's Guide*, "Agent Management Services" chapter.

User interface options

Installation of the base Tivoli Monitoring 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 client interface is a graphical user interface (GUI) based on Java on a Windows or Linux workstation. You can run the Tivoli Enterprise Portal as a desktop application or a browser application. The browser application is automatically installed with the Tivoli Enterprise Portal Server. The desktop application is installed using the Tivoli Monitoring installation media or with Java Web Start. Tivoli Enterprise Portal Server. To start Tivoli Enterprise Portal browser client in your Internet browser, enter the URL for a specific Tivoli Enterprise Portal browser client installed on your web server.

Command Line Interface
You can use IBM Tivoli Monitoring commands to manage Tivoli Monitoring components and their configuration. There are also commands that you can run at the Tivoli Enterprise Console event server

IBM Tivoli Enterprise Console
An event management application that integrates system, network, database, and application management to help ensure optimal availability of an IT service for an organization.

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 designated to start automatically.

Features of the Microsoft Active Directory agent

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

Use the Microsoft Active Directory agent to easily collect and analyze the following types of Active Directory-specific information:

- Sysvol replication details
- Forest-wide trust relationship details
- Time drift monitoring information
- Network replication status and performance details
- Directory system utilization information
- Local security authority details
- Name Service (NS) details
- Security Account Manager (SAM) details
- File Replication Service (FRS) details
- Distributed File Replication (DFS-R) details
- Active Directory network status
- DNS details relevant to Active Directory
- DHCP details relevant to Active Directory
- Physical storage details for Active Directory
- Knowledge Consistency Checker details
- Kerberos Key Distribution Center details
- Lightweight Directory Access Protocol details

- Address book performance and utilization details
- Built-in logon authentication and user authorization information
- Communication data between the Active Directory and Exchange Directory Service (XDS)
- Active Directory database and details of log files
- Event log entries that are related to the Directory Services or the Domain Naming System (DNS) Server of Active Directory.
- Conflict objects details
- Details of organizational units that are moved or deleted
- RID pool resource availability
- Netlogon authentication performance
- Information about the Active Directory Password Settings objects

The Microsoft Active Directory agent provides the following benefits:

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

Data sources

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

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

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

Table 1. Mechanisms used to gather attributes

Attribute group	Collection source	API/CL names
Address Book	API	Performance Data Helper
Containers	API	Active Directory Service Interfaces
DNS ADIntegrated	API	• Active Directory Service Interfaces • Windows API
DNS ADIntegrated Details	API	• Active Directory Service Interfaces • Windows API

Table 1. Mechanisms used to gather attributes (continued)

Attribute group	Collection source	API/CL names
DFS Replication Connections	API	Performance Data Helper
DFS Service Volumes	API	Performance Data Helper
DFS Replication Folders	API	Performance Data Helper
DHCP	API	Performance Data Helper
Directory Services	API	Performance Data Helper
DNS	API	Performance Data Helper
Domain Controller Availability	API	• Windows API • Active Directory Service Interfaces
Domain Controller Availability	CL	ping
Domain Controller Performance	API	• Performance Data Helper • Windows API • Active Directory Service Interfaces
Exchange Directory Services	API	Performance Data Helper
File Replication Service	API	Performance Data Helper
Forest Topology	API	Active Directory Service Interfaces
Kerberos Consistency Checker	API	Performance Data Helper
Kerberos Key Distribution Centre	API	Performance Data Helper
Lightweight Directory Access Protocol	API	• Performance Data Helper • Active Directory Service Interfaces
Lost and Found Objects	API	Active Directory Service Interfaces
Local Security Authority	API	Performance Data Helper
Name Service Provider	API	Performance Data Helper
Replication	API	• Performance Data Helper • Windows API • Active Directory Service Interfaces
Replication	CL	net time
Replication Partner	API	• Windows API • Active Directory Service Interfaces
Replication Partner Latency	API	• Windows API • Active Directory Service Interfaces
Root Directory Server	API	Active Directory Service Interfaces
Security Accounts Manager	API	Performance Data Helper
Services	API	Service Control Manager
Sysvol Replication	API	Windows API
Sysvol Replication	CL	ntfrsutl
Trust	API	Windows API
Trust	CL	netdom verify
Trust Topology	API	Active Directory Service Interfaces

Table 1. Mechanisms used to gather attributes (continued)

Attribute group	Collection source	API/CL names
Event Logs	API	Windows Event Log API
Active Directory Database Information	API	Windows API
Replication Conflict Objects	API	Active Directory Service Interfaces
Moved or Deleted Organizational Units	API	Active Directory Service Interfaces
RID Pool Information	API	Active Directory Services Interfaces
Netlogon Attributes	API	Performance Data Helper
Password Settings Object	API	Active Directory Service Interfaces

Chapter 2. Agent installation and configuration

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

With the self-describing agent capability, new or updated IBM Tivoli Monitoring agents can become operational after installation without having to perform additional product support installation steps. To take advantage of this capability, see "Enabling self-describing agent capability at the hub monitoring server" in the *IBM Tivoli Monitoring Installation and Setup Guide*. Also, see the *IBM Tivoli Monitoring Administrator's Guide* for additional information about using this capability.

Requirements

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

For information about requirements, see the Prerequisites topic for the agent in the IBM Tivoli Composite Application Manager for Microsoft Applications Information Center http://publib.boulder.ibm.com/infocenter/ tivihelp/v24r1/topic/ com.ibm.itcamms.doc_6.3/welcome_msapps63.html).

Installing language packs

Before you install a language pack for the agent support files on the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Monitoring Agent, and the Tivoli Enterprise Portal Server, ensure that you have installed the product in English. Perform the following steps depending on the operating system that you are using.

Windows systems

This section contains the procedure for installing a language pack on a Windows system.

Procedure

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

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

   Note: You can select multiple languages by pressing the Ctrl key.

7. Select the languages that you want to install and click **Next**.
8. Examine the installation summary page and click **Next** to start the installation.
9. Click **Finish** after the installation completes.
10. Restart the Tivoli Enterprise Portal (if on the Tivoli Enterprise Portal Server) or restart the Tivoli Enterprise Portal Server (if on the Tivoli Enterprise Portal Server component).

UNIX or Linux systems

This section contains the procedure for installing a language pack on a UNIX or Linux system.

Procedure

1. Run the following command to create a temporary directory on the computer. Ensure that the full path of the directory does not contain any spaces:

   ```
   mkdir dir_name
   ```

2. Mount the language pack CD to the temporary directory that you have created.
3. Run the following command to start the installation program:

   ```
   cd dir_name
   lpinstall.sh ITM Home Directory
   ```

   where *ITM Home Directory* is the location where you have installed IBM Tivoli Monitoring. Usually it is `/opt/IBM/ITM` for AIX® and Linux.
4. Select the language of the installer and click **OK**.
5. Click **Next** on the Introduction panel.
6. Click **Add/Update** and click **Next**.
7. Select the folder in which the National Language Support package (NLSPackage) files are located.

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

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

Silent installation of language packs on Windows, UNIX, or Linux systems

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

Before you begin

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

Procedure

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

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

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

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

   LANG_SELECTION_LIST
   Language you want to install.
3. Enter the command to install the language pack with a response file (silent installation):
   - For Windows systems:

     `lpinstaller.bat -f path_to_response_file`
   - For UNIX or Linux systems:

     `lpinstaller.sh -c candle_home -f path_to_response_file`

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

Response file example

```
#     IBM Tivoli Monitoring Agent Language Pack Silent Installation Operation
#
#This is a sample response file for silent installation mode for the IBM Tivoli
#Monitoring Common Language Pack Installer.
#.
#This file uses the IBM Tivoli Monitoring Common Agent Language Pack with the
#install package as an example.
#Note:
#This response file is for the INSTALLATION of language packs only.
#This file does not support UNINSTALLATION of language packs in silent mode.
#-------------------------------------------------------------------------------
#-------------------------------------------------------------------------------
#To successfully complete a silent installation of the the example of Common Agent
#localization pack, complete the following steps:
#
#1.Copy ITM_Agent_LP_silent.rsp to the directory where lpinstaller.bat or
#lpinstaller.sh is located (IBM Tivoli Monitoring Agent Language Pack build
#location).
#
#2.Modify the response file so that it is customized correctly and completely for
#your site.
#  Complete all of the following steps in the response file.
#
#3.After customizing the response file, invoke the silent installation using the
#following command:
#For Windows:
#    lpinstaller.bat -f <path_to_response_file>
#For UNIX and Linux:
#    lpinstaller.sh -c <candle_home> -f <path_to_response_file>
```

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

Prerequisites checking

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

For the Microsoft Active Directory agent, the prerequisite checker verifies the following requirements:

- Memory
- Disk
- Operating systems

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

For detailed information about installation prerequisites, see the Prerequisites topic for the agent in the IBM Tivoli Composite Application Manager for Microsoft Applications Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamms.doc_6.3/welcome_msapps63.html).

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

Agent-specific installation and configuration

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

Running as a non-administrator user

This section provides information about running the Microsoft Active Directory agent as a non-administrator user.

About this task

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

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

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

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

Procedure

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

a. Right-click the Monitoring Agent for Active Directory service, and click **Properties**.
b. In the Monitoring Agent for Active Directory Properties window, on the **Log On** tab, click **This Account**. Enter the user credentials.
c. Click **Apply**, and then click **OK**.

9. Restart the agent service.

Configuring caching

This section provides information about enabling and configuring or disabling the cache feature for the Microsoft Active Directory agent.

About this task

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

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

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

Procedure

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

1. In Manage Tivoli Enterprise Monitoring Services (kinconfig.exe), select the Monitoring Agent for Active Directory.
2. Right click and go to **Advanced options**.
3. Select **Edit ENV File** from the options. This opens the K3ZENV file for editing. The **ADO_CACHE_INTERVAL** variable exists in the K3ZENV file.
4. To turn caching OFF, set the **ADO_CACHE_INTERVAL** variable to 0. To turn caching ON, set the **ADO_CACHE_INTERVAL** to any positive integer value. This value forms the caching interval in seconds. For instance, a value of 180 would mean a 3-minute interval.
5. After editing the K3ZENV file, save and close the file to implement the new cache interval value.
6. A message box appears asking if the agent needs to be recycled to include the changes in agent functionality. Clicking **Yes** recycles the agent with the new

caching interval value. Clicking **No** lets the agent continue to run without the changes to the caching interval. When the agent is restarted, the changes are implemented.

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

Configuring ping variables

This section provides information about the variables for ping count, ping timeout, and ping size. These variables can be configured by using environment variables when the Microsoft Active Directory agent is started.

About this task

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

Table 2. Ping variables descriptions and default values

Variable	Description	Default value	Unit
ADO_PING_COUNT	The number of ping requests to make.	1	
ADO_PING_ TIMEOUT	The time to wait for each ping response.	2000	Milli-seconds
ADO_PING_SIZE	The size of the ping packet to send.	32	Bytes

Procedure

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

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

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

Configuring Active Directory logical view

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

Procedure

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

Environment variables for Event Log attributes

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

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

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

Environment variables for LDAP attributes

The following environment variables are introduced for LDAP attributes:

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

Environment variable for Organizational Units attributes

The **OU_INFORMATION_DURATION** environment variable determines the number of days for which information about modified organizational units is displayed on

the Tivoli Enterprise Portal. The value of this variable must be in the range 1 - 30. The default value of this variable is 1 day. If the value of this variable is 0, information about modified organizational units is not displayed on the Tivoli Enterprise Portal.

Environment variable for Replication Conflict Object attributes

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

Environment variables for Sysvol replication

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

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

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

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

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

Chapter 3. Workspaces reference

A workspace is the working area of the Tivoli Enterprise Portal application window. The Navigator tree contains a list of the workspaces provided by the agent.

About workspaces

Use the Navigator tree to select the workspace you want to see. As part of the application window, the status bar shows the Tivoli Enterprise Portal Server name and port number to which the displayed information applies and the ID of the current user.

When you select an item in the Navigator tree, a default workspace is displayed. When you right-click a Navigator item, a menu that includes a Workspace item is displayed. The Workspace item contains a list of workspaces for that Navigator item. Each workspace has at least one view. Some views have links to other workspaces. You can also use the Workspace Gallery tool as described in the *Tivoli Enterprise Portal User's Guide* to open workspaces.

The workspaces in the Navigator are displayed in a Physical view that shows your enterprise as a physical mapping or a dynamically populated logical view that is agent-specific. You can also create a Logical view. The Physical view is the default view.

To select the dynamically populated logical view, select **ADO** from the **View** list in the Navigator. To view the dynamically populated ADO logical view, you must log in to the Tivoli Enterprise Portal as a system administrator.

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

A table view within a workspace corresponds to a group of attributes; the columns in the table view show some or all the attributes available in the attribute group.

Additional information about workspaces

For more information about creating, customizing, and working with workspaces, see "Using workspaces" in the *Tivoli Enterprise Portal User's Guide*.

For a list of the predefined workspaces for this monitoring agent and a description of each workspace, see "Predefined workspaces" on page 18 and the information about each individual workspace.

Some attribute groups for this monitoring agent might not be represented in the predefined workspaces or views for this agent. For a full list of the attribute groups, see "Attributes in each attribute group" on page 27.

Predefined workspaces

The Microsoft Active Directory agent provides the following predefined workspaces, which are organized by Navigator item and are available in both Physical as well as Logical Navigator View (Active Directory View):

- Active Directory workspace
- Address Book workspace
- DHCP workspace
- Directory System Agent workspace
- DNS workspace
- DNS ADIntegrated
  - DNS ADIntegrated workspace
  - DNS ADIntegrated Details workspace
- Domain Controller Availability
  - Active Directory Database Information workspace
  - Domain Controller Availability workspace
  - Event Log workspace
  - Services workspace
  - RID Pool Information workspace
- Domain Controller Performance workspace
- Exchange Directory Service workspace
- File Replication Service
  - Distributed File System Replication workspace
  - Distributed File System Replication Details workspace
  - File Replication Service workspace
- Forest Topology
  - Forest Topology workspace
  - Domain Controllers Details workspace
- Kerberos Key Distribution Center workspace
- Knowledge Consistency Checker workspace
- Lightweight Directory Access Protocol workspace
- LDAP Attributes workspaces
  - LDAP Attributes workspace
  - User History worspace
- Local Security Authority workspace
- Lost and Found Objects workspace
- GPO workspaces
  - Group Policy Object workspace
  - Password Settings Object workspace
- Name Service Provider workspace
- Replication
  - Historical workspace
  - Replication workspace
  - Replication Conflict Objects workspace
- Replication Latency workspace
- Replication Partner

  - Replication Partner workspace
  - Sysvol Replication workspace
- Root Directory Server
  - Root Directory Server workspace
  - Moved or Deleted Organizational Units workspace
- Security Accounts Manager workspace
- Trusts
  - Trust workspace
  - Trust Topology workspace
  - Domain Trusts Details workspace
  - Netlogon Attributes workspace

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.

The Microsoft Active Directory agent provides the following composite workspaces:

- Active Directory server LDAP utilization workspace
- Active Directory server NTDS utilization workspace
- Active Directory server replication utilization workspace
- Active Directory service utilization workspace
- Active Directory system utilization workspace
- Active Directory time difference workspace

Workspace description

The remaining sections of this chapter contain descriptions of each of these predefined workspaces. These workspace descriptions are organized alphabetically.

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

Note: The default workspace for the Active Directory agent was modifiable, which was a defect. The workspace is changed to make it non-modifiable.

Active Directory server LDAP utilization workspace

The Active Directory server LDAP utilization workspace is a composite workspace that provides details about the LDAP utilization. This workspace includes the following views:

- DS Search Sub-Operations/sec chart
- DC LDAP Utilization chart

Active Directory server NTDS utilization workspace

The Active Directory server NTDS utilization workspace is a composite workspace that provides details about the NTDS utilization. This workspace includes the following views:

- lsass Process Memory Usage chart
- lsass Handle Count chart
- DS Search Sub-Operations/sec chart

Active Directory server replication utilization workspace

The Active Directory server replication utilization workspace is a composite workspace that provides details about the replication utilization. This workspace includes the following views:

- Intersite Replication Activity/sec chart
- Intrasite Replication Activity/sec chart

Active Directory service utilization workspace

The Active Directory service utilization workspace is a composite workspace that provides details about the Active Directory service utilization. This workspace includes the following views:

- lsass Process Memory Usage chart
- lsass Percent Processor Time chart
- lsass Handle Count chart

Active Directory system utilization workspace

The Active Directory system utilization workspace is a composite workspace that provides details about the Active Directory system utilization. This workspace includes the following views:

- Processor Queue Length table
- Processor Utilization table
- Physical Memory Availability and Virtual Memory Utilization chart
- Memory Paging Activity/sec

Active Directory time difference workspace

The Active Directory time difference workspace is a composite workspace that provides details about the time difference between the domain controller and the good time server. If the domain controller cannot find the good time server in the domain, the time difference is calculated from the preferred good time server. This workspace includes the following views:

- Time Difference bar graph
- Time Difference 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 bar 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 bar 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 plot chart
- DNS Details table

DNS ADIntegrated workspaces

This section describes the workspaces related to the DNS ADIntegrated navigator item.

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 Summary table
- DNS SRV Records Bad bar chart
- DNS SRV Records Missing bar chart

DNS ADIntegrated Details workspace:
The DNS ADIntegrated workspace monitors the server under investigation and displays SRV records that are invalid or missing. This workspace includes the "DNS ADIntegrated Details" table view.

Domain Controller Availability workspaces

This section describes the workspaces related to the Domain Controller Availability navigator item.

Active Directory Database Information workspace:
The Active Directory Database Information workspace monitors the size of the Microsoft Active Directory database and log files, and provides information about the free space that is available on the disk where the database and the log files are stored. This workspace includes the "Active Directory Database Information" table view.

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

Event Log workspace:
The Event Log workspace monitors the events of Directory Services and DNS Server that are logged by the Windows Event Log service. This workspace includes the "Event Log" table view.

RID Pool Information workspace:
The RID Pool Information workspace displays information about the RID pool.

This workspace includes the following views:

- RID Pool Information table
- Exhausted RID Status circular gauge

Services workspace:
The Services workspace displays the status and configuration information related to each service that is installed on the NT Server. This workspace is associated with the "Domain Controller Availability" navigator item. This workspace includes the "Active Directory Services Details" table view.

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 bar chart
- File Operations Rate bar chart

Exchange Directory Service workspace

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

- Exchange Directory Service bar chart
- Exchange Directory Service Details table

File Replication Service workspaces

This section describes the workspaces related to the File Replication Service navigator item.

Distributed File System Replication workspace:
The Distributed File System Replication workspace compliments the default File Replication Service navigator item workspace. This workspace includes the following views:

- DFS Replicated Folders bar chart
- DFS Replication Connections table
- DFS Replicated Folders table

Distributed File System Replication Details workspace:
The Distributed File System Replication Details workspace monitors the performance of the DFS Replication service. This workspace includes the following views:

- DFS Replication Connection Details table
- DFS Replicated Folders Details table
- DFS Service Volumes Details table

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

- File Replication Service Details table
- FRS Change Orders bar chart

Forest Topology workspaces

This section describes the workspaces related to the Forest Topology navigator item.

Forest Topology workspace:
The Forest Topology workspace is associated with the new navigator item "Forest Topology." This workspace includes the "Forest Topology graph" view.

Domain Controller Details workspace:
The Domain Controllers Details workspace is a hidden workspace that is associated with the navigator item "Forest Topology." This workspace includes the following views:

- Forest Topology graph
- Domain Controllers Details table

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 bar chart
- Kerberos Key Distribution Center Details 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 Bar chart
- Knowledge Consistency Checker Details 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 bar chart
- LDAP Details table

LDAP Attributes workspaces

This section describes the workspaces related to the LDAP attributes.

LDAP Attributes workspace:
The LDAP Attributes workspace monitors various LDAP items. This workspace includes the LDAP attributes details view.

User History workspace:

The User History workspace is an historical view of LDAP data over time. Use this workspace to see the volume of replication activity in a 7-day period. You must configure historical data collection to view this workspace. This workspace includes the following views:

- User History Graph plot chart
- User History 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 bar chart
- Local Security Authority Details 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:

- Lost and Found Objects table
- Lost and Found Objects Details table

GPO workspaces

This section describes the workspaces that are related to the GPO navigator item.

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

- Group Policy Objects table
- Group Policy Objects Details table

Note: A new attribute is added in the Group Policy Objects attribute group. The Group Policy Objects Details table view is updated to show this attribute in the report.

Password Setting Objects workspace:
This workspace displays the values of the attributes that are included in the Password Settings Object attribute group. This workspace includes the Password Setting Objects table view.

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 Service Provider bar chart
- Name Service Provider Details 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 Sec plot chart
- Replication Details table

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 Inbound Details table
- Replication Outbound Details table
- USN Details table

Replication Conflict Objects workspace:
The Replication Conflict Objects workspace displays information about the replication conflict objects that are created due to a replication collision. This workspace includes the "Replication Conflict Objects" 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 bar chart
- Replication Latency Details table

Replication Partner workspaces

This section describes the workspaces related to the Replication Partner navigator item.

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
- Replication Failure bar chart
- Replication Health table

Sysvol Replication workspace:
The Sysvol Replication workspace displays the result of the replication that is performed on the `Sysvol` folder, and the time at which replication tests are performed and verified on the `Sysvol` folder. This workspace includes the "Sysvol Replication" table view.

Root Directory Server workspaces

This section describes the workspaces related to the Root Directory Server navigator item.

Root Directory Server workspace:
The Root Directory Server workspace is associated with the navigator item "Root Directory Server." This workspace includes the following views:

- Root Directory Server Details table
- Containers Details table

Note: A new attribute is added in the Root Directory Server attribute group. The Root Directory Server Details table view is updated to show this attribute in the report.

Moved or Deleted Organizational Units workspace:
The Moved or Deleted Organizational Units workspace displays information about the status, the name, and the distinguished name of the organizational units that are moved or deleted. This workspace includes the "Moved or Deleted Organizational Units" table view.

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 bar chart
- Security Accounts Manager Details table

Trusts workspaces

This section describes the workspaces associated with the Trusts navigator item.

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

- Trusts table
- Trusts Details table

Trust Topology workspace:
The Trust Topology workspace displays a new Trust topology graph that shows the complex trust relationships between domains. This workspace includes the Trust Topology graph view.

Domain Trusts Details workspace:
The Domain Trust Details is a hidden workspace that is associated with the Trusts navigator item. This workspace includes the following views:

- Trust Topology graph view
- Domain Trusts Details table

Netlogon Attributes workspace:
The Netlogon Attributes workspace displays the values of all instances of the netlogon performance counters. This workspace includes the Netlogon Attributes table view.

Chapter 4. Attributes reference

Attributes are organized into attribute groups. Attributes in an attribute group relate to a single object such as an application, or to a single kind of data such as status information.

Attributes in a group can be used in queries, query-based views, situations, policy workflows, take action definitions, and launch application definitions. Chart or table views and situations are two examples of how attributes in a group can be used:

- 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 Properties editor to 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 values you assign to the situation attributes are compared with the values collected by the Microsoft Active Directory agent and registers an *event* if the condition is met. You are alerted to events by indicator icons that are displayed in the Navigator.

Additional information about attributes

For more information about using attributes and attribute groups, see the *Tivoli Enterprise Portal 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.

Attributes in each attribute group

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.

The following attribute groups are included:

- Address Book attributes
- Active Directory Database Information attributes
- Containers attributes
- DHCP attributes
- Directory Services attributes
- Distributed File System Replication attributes

- DFS Replication Connections attributes
- DFS Replication Folders attributes
- DFS Service Volumes attributes
- DNS ADIntegrated attributes
- DNS ADIntegrated Details attributes
- DNS attributes
- Domain Controller Availability attributes
- Domain Controller Performance attributes
- Event Log attributes
- Exchange Directory Services attributes
- File Replication Service attributes
- Forest Topology attributes
- Group Policy Object attributes
- Kerberos Key Distribution Center attributes
- Knowledge Consistency Checker attributes
- Lightweight Directory Access Protocol attributes
- LDAP attributes
- Local Security Authority attributes
- Lost and Found Objects attributes
- Moved or Deleted Organizational Units attributes
- Name Service Provider attributes
- Netlogon attributes
- Password Settings Objects attributes
- Replication attributes
- Replication Conflict Objects attributes
- Replication Partner attributes
- Replication Partner Latency attributes
- RID Pool Information attributes
- Root Directory Server attributes
- Security Accounts Manager attributes
- Services attributes
- Sysvol Replication attributes
- Trust attributes
- Trust Topology attributes

Address Book attributes

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

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

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

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

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

AB Ambiguous Name Resolutions per sec 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 format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

Active Directory Database Information attributes

The Active Directory Database Information attributes provide information about the database and log files of the Microsoft Active Directory.

ADDB Database File Path The full directory path where the Microsoft Active Directory database is stored.

ADDB Database File Size The size (in MB) of the database file.

ADDB Available Disk Space for Database The free space (in MB) that is currently available on the hard disk drive where the Microsoft Active Directory database is stored.

ADDB Database Log File Path The full directory path where the log files of the Microsoft Active Directory are stored.

ADDB Database Log File Size The sum of the size (in MB) of all the log files.

ADDB Available Disk Space for Log Files The free space (in MB) that is currently available on the hard disk drive where the log files of the Microsoft Active Directory are stored.

ADDB Percentage Free Disk Space for Database The percentage of free space that is currently available on the hard disk drive where the Microsoft Active Directory database file is stored.

ADDB Percentage Free Disk Space for Log Files The percentage of free space that is currently available on the hard disk drive where the Microsoft Active Directory database log files are stored.

Server Name The managed system name. The format is hostname:agent_code.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

Containers attributes

The Containers attributes display information about containers and objects.

CNT Class Type The class type of the container. For example, container, sitesContainer, crossRefContainer, and so on.

CNT Common Name The common name of the container in the Active Directory schema.

CNT Create Timestamp The object creation timestamp.

CNT Distinguished Name The distinguishable name of the container.

CNT Modify Timestamp The object modification timestamp.

CNT Partition The directory partition under which the container falls.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 Discovers Sec Rate of DHCP Discovers received by the DHCP server. An integer is a valid entry.

DHCP Duplicates Dropped Sec DHCP duplicates dropped per second.

DHCP Informs Sec Rate of DHCP Informs received by the DHCP server. An integer is a valid entry.

DHCP Milliseconds Packet The average time per packet taken by the DHCP server to send a response. An integer is a valid entry.

DHCP Nacks Sec DHCP Nacks per second.

DHCP Offers Sec Rate of DHCP Offers sent out by the DHCP server. An integer is a valid entry.

DHCP Packets Expired Sec DHCP packets expired per second.

DHCP Packets Received Sec Packets Received/Sec is the rate at which packets are received by the DHCP server. An integer is a valid entry.

DHCP Releases Sec Rate of DHCP Releases received by the DHCP server. An integer is a valid entry.

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.

DHCP V6 Acks sec The rate of DHCP Acks sent by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Active Queue Length The Number of packets in the processing queue of the DHCPV6 server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Advertises sec The rate of DHCP Advertises sent out by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Confirms sec The rate of DHCP Confirms received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Declines Sec Rate of DHCP Declines received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Duplicates Dropped Sec The rate at which the DHCPV6 server received duplicate packets. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Informs sec The rate of DHCP Informs received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Milliseconds Packet The average time per packet taken by the DHCPV6 server to send a response. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Packets Expired Sec The rate at which packets get expired in the DHCPV6 server message queue. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Packets Received Sec The rate at which packets are received by the DHCPV6 server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Rebinds sec The rate of DHCP Rebinds received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Releases sec The rate of DHCP Releases received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Renews sec The rate of DHCP Renews received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Requests sec The rate of DHCP Requests received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DHCP V6 Solicits sec The rate of DHCP Solicits received by the DHCPV6 Server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 sec 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 sec 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 sec The number of directory reads per second. An integer is a valid entry.

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

DS Directory Writes per sec 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 Pct Reads from NTDSAPI The percent of directory reads coming from NTDAPI calls. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DS Pct Searches from NTDSAPI The percent of directory searches coming from NTDAPI calls. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DS Pct Writes from NTDSAPI The percent of directory writes coming from NTDSAPI calls. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

DS Security Descriptor Propagations per sec 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 sec The number of security descriptor propagation suboperations per second. An integer is a valid entry.

DS Server Binds per sec 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 sec 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

Format	Description
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

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

Distributed File System Replication attributes

The DFSR attributes display DFSR information.

Note: This attribute group is available only on Windows 2008 operating system. Data rows are not available on Windows 2003 operating system.

DFSR Connections Bandwidth Savings Using DFS Replication The percentage of bandwidth that was saved by the DFS Replication service for this connection using a combination of remote differential compression (RDC) and other compression technologies that minimize network bandwidth use. An integer is a valid entry.

DFSR Connections Bytes Received sec An estimate of the average number of bytes that were received each second over the past 30 seconds. An integer is a valid entry.

DFSR Connections Compressed Size of Files Received The compressed size of files (in bytes) received on the connection. An integer is a valid entry.

DFSR Connections RDC Compressed Size of Files Received The compressed size (in bytes) of files received with remote differential compression (RDC) for this connection. An integer is a valid entry.

DFSR Connections RDC KBytes Received The bytes that were received on this connection while replicating files using remote differential compression (RDC). An integer is a valid entry.

DFSR Connections RDC Number of Files Received The number files that were received on this connection. An integer is a valid entry.

DFSR Connections RDC Size of Files Received The uncompressed size (in bytes) of files received with remote differential compression (RDC) for this connection. An integer is a valid entry.

DFSR Connections Size of Files Received The uncompressed size (in bytes) of the files received on this connection. An integer is a valid entry.

DFSR Connections Total Files Received The number of files that were received on the connection. An integer is a valid entry.

DFSR Connections Total KBytes Received The total number of bytes received on the connection. An integer is a valid entry.

DFSR Folders Bandwidth Savings Using DFS Replication The percentage of bandwidth that was saved by the DFS Replication service for this replicated folder using a combination of remote differential compression (RDC) and other compression technologies that minimize network bandwidth. An integer is a valid entry.

DFSR Folders Compressed Size of Files Received The compressed size (in bytes) of files received for this replicated folder. An integer is a valid entry.

DFSR Folders Conflict Bytes Cleaned up The total size (in bytes) of the conflict loser files and folders that were deleted from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Conflict Bytes Generated The total size (in bytes) of the files and folders in this replicated folder that were moved to the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Conflict Files Cleaned up The number the conflict loser files and folders that were deleted from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Conflict Files Generated The number of files and folders in this replicated folder that were moved to the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Conflict Folder Cleanups Completed The number of times conflict loser files and folders in the Conflict and Deleted folder were deleted by the DFS Replication service. An integer is a valid entry.

DFSR Folders Conflict Space In Use The total size (in bytes) of the conflict loser files and folders currently in the Conflict and Deleted folder used by the DFS Replication service. An integer is a valid entry.

DFSR Folders Deleted Bytes Cleaned up The total size (in bytes) of replicating deleted files and folders (in bytes) that were cleaned up from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Deleted Bytes Generated The total size (in bytes) of replicated deleted files and folders that were moved to the Conflict and Deleted folder after they were deleted from a replicated folder on a sending member. An integer is a valid entry.

DFSR Folders Deleted Files Cleaned up The number of replicated deleted files and folders that were cleaned up from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Deleted Files Generated The number of replicated deleted files and folders that were moved to the Conflict and Deleted folder after they were deleted from a replicated folder on a sending member. An integer is a valid entry.

DFSR Folders Deleted Space In Use The total size (in bytes) of the deleted files and folders currently in the Conflict and Deleted folder used by the DFS Replication service. An integer is a valid entry.

DFSR Folders File Installs Retried The number of file installs that are being tried again due to sharing violations or other errors encountered when installing the files. An integer is a valid entry.

DFSR Folders File Installs Succeeded The number of files that were successfully received from sending members and installed locally on this server. An integer is a valid entry.

DFSR Folders RDC Compressed Size of Files Received The compressed size (in bytes) of the files received with remote differential compression (RDC) for this replicated folder. An integer is a valid entry.

DFSR Folders RDC KB Received The number of bytes that were received in replicating files using remote differential compression (RDC) for this replicated folder. An integer is a valid entry.

DFSR Folders RDC Number of Files Received The number files that were received for this replicated folder. An integer is a valid entry.

DFSR Folders RDC Size of Files Received The uncompressed size (in bytes) of the files received with remote differential compression (RDC) for this replicated folder. An integer is a valid entry.

DFSR Folders Size of Files Received The uncompressed size (in bytes) of the files received for this replicated folder. An integer is a valid entry.

DFSR Folders Staging Bytes Cleaned up The total size (in bytes) of the files and folders that were cleaned up from the staging folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Staging Bytes Generated The total size (in bytes) of replicated files and folders in the staging folder created by the DFS Replication service since last restart and is monotonically increasing counter. An integer is a valid entry.

DFSR Folders Staging Files Cleaned up The number of files and folders that were cleaned up from the staging folder by the DFS Replication service. An integer is a valid entry.

DFSR Folders Staging Files Generated The number of times replicated files and folders were staged by the DFS Replication service. An integer is a valid entry.

DFSR Folders Staging Space In Use The total size (in bytes) of the files and folders currently in the staging folder used by the DFS Replication service. An integer is a valid entry.

DFSR Folders Total Files Received The number of files that were received by this replicated folder. An integer is a valid entry.

DFSR Folders Updates Dropped The number of redundant file replication update records that were ignored by the DFS Replication service because they did not change the replicated file or folder. An integer is a valid entry.

DFSR Volumes Database Commits The number of database commit operations performed by the DFS Replication service. An integer is a valid entry.

DFSR Volumes Database Lookups The number of database search operations performed by the DFS Replication service. An integer is a valid entry.

DFSR Volumes USN Journal Records Accepted The number of update sequence number (USN) journal records that were processed by the DFS Replication service. An integer is a valid entry.

DFSR Volumes USN Journal Records Read The number of update sequence number (USN) journal records that were read by the DFS Replication service. An integer is a valid entry.

DFSR Volumes USN Journal Unread Percentage The percent of the update sequence number (USN) journal that has not yet been read and processed by the DFS Replication service. An integer is a valid entry.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

DFS Replication Connections attributes

The DFS Replication Connections attributes display information about the number, size, and bandwidth usage of the connections that the DFS Replication service uses. This attribute group is a multi-instance attribute group.

DFRC Connections Bandwidth Savings Using DFS Replication The current percentage of bandwidth that the DFS Replication service saves for the replicated connection. An integer is a valid entry.

DFRC Connections RDC KBytes Received The number of bytes that are currently received on the connection while replicating files by using remote differential compression (RDC). An integer is a valid entry.

DFRC Connections RDC Compressed Size of Files Received The size (in bytes) of compressed files that are currently received with RDC on the connection. An integer is a valid entry.

DFRC Connections RDC Size of Files Received The size (in bytes) of uncompressed files that are currently received with RDC on the connection. An integer is a valid entry.

DFRC Connections RDC Number of Files Received The number of files that are currently received on the connection. An integer is a valid entry.

DFRC Connections Bytes Received Second The average number of bytes that are received per second on the connection. An integer is a valid entry.

DFRC Connections Compressed Size of Files Received The size (in bytes) of compressed files that are currently received on the connection. An integer is a valid entry.

DFRC Connections Size of Files Received The size (in bytes) of uncompressed files that are currently received on the connection. An integer is a valid entry.

DFRC Connections Total Files Received The total number of files that are received on the connection. An integer is a valid entry.

DFRC Connections Total KBytes Received The total number of bytes that are received on the connection. An integer is a valid entry.

DFRC Instance Name The name of the replication connection instance.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year

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

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

DFS Replication Folders attributes

The DFS Replication Folders attributes display information about the number, size, and bandwidth usage of the folders that the DFS Replication service replicates. This attribute group is a multi-instance attribute group.

DFRF Folders Bandwidth Savings Using DFS Replication The current percentage of bandwidth that the DFS Replication service saves for the replicated folder. An integer is a valid entry.

DFRF Folders RDC KBytes Received The number of bytes that are currently received for the folder while replicating files by using remote differential compression (RDC). An integer is a valid entry.

DFRF Folders RDC Compressed Size of Files Received The size (in bytes) of compressed files that are currently received with RDC for the replicated folder. An integer is a valid entry.

DFRF Folders RDC Size of Files Received The size (in bytes) of uncompressed files that are currently received with RDC for the replicated folder. An integer is a valid entry.

DFRF Folders RDC Number of Files Received The current number of files that are received for the replicated folder. An integer is a valid entry.

DFRF Folders Compressed Size of Files Received The size (in bytes) of compressed files that are currently received for the replicated folder. An integer is a valid entry.

DFRF Folders Size of Files Received The size (in bytes) of uncompressed files that are currently received for the replicated folder. An integer is a valid entry.

DFRF Folders Total Files Received The total number of files that are received for the replicated folder. An integer is a valid entry.

DFRF Folders Deleted Space In Use The total size (in bytes) of the deleted files and folders that are currently in the Conflict and Deleted folder. An integer is a valid entry.

DFRF Folders Deleted Bytes Cleaned up The total size (in bytes) of deleted files and folders that are cleaned up from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Deleted Files Cleaned up The current number of deleted files and folders that are cleaned up from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Deleted Bytes Generated The total size (in bytes) of the deleted files and folders that have been moved to the Conflict and Deleted folder after they were deleted from the replicated folder. An integer is a valid entry.

DFRF Folders Deleted Files Generated The current number of deleted files and folders that have been moved to the Conflict and Deleted folder after the files were deleted from the replicated folder. An integer is a valid entry.

DFRF Folders Updates Dropped The current number of replication update records for the redundant files that have been ignored by the DFS Replication service because the update records did not change the replicated file or folder. An integer is a valid entry.

DFRF Folders File Installs Retried The current number of installed files that are retried because of sharing violations and other errors, which occurred when installing the files. An integer is a valid entry.

DFRF Folders File Installs Succeeded The current number of files that are received from sending members and installed locally on the domain server. An integer is a valid entry.

DFRF Folders Conflict Folder Cleanups Completed The number of times the DFS Replication service deletes the conflict loser files and folders from the Conflict and Deleted folder. An integer is a valid entry.

DFRF Folders Conflict Space In Use The total size (in bytes) of the conflict loser files and folders that are currently in the Conflict and Deleted folder. An integer is a valid entry.

DFRF Folders Conflict Bytes Cleaned up The total size (in bytes) of the conflict loser files and folders that are deleted from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Conflict Files Cleaned up The current number of conflict loser files and folders that are deleted from the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Conflict Bytes Generated The total size (in bytes) of the files and folders in the replicated folder that are moved to the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Conflict Files Generated The current number of files and folders in the replicated folder that are moved to the Conflict and Deleted folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Staging Space In Use The total size (in bytes) of the files and folders that are currently in the staging folder. An integer is a valid entry.

DFRF Folders Staging Bytes Cleaned up The total size (in bytes) of the files and folders that are cleaned up from the staging folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Staging Files Cleaned up The current number of files and folders that are cleaned up from the staging folder by the DFS Replication service. An integer is a valid entry.

DFRF Folders Staging Bytes Generated The total size (in bytes) of replicated files and folders in the staging folder that are created by the DFS Replication service since the domain server was restarted. An integer is a valid entry.

DFRF Folders Staging Files Generated The current number of times the replicated files and folders are staged by the DFS Replication service. An integer is a valid entry.

DFRF Instance Name The name of the replication folder instance.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

DFS Service Volumes attributes

The DFS Service Volumes attributes displays information about the database operations that the DFS Replication service performs. This attribute group is a multi-instance attribute group.

DFSV Volumes Database Lookups The current number of search operations that are performed by the DFS Replication service on the database. An integer is a valid entry.

DFSV Volumes Database Commits The current number of commit operations that are performed by the DFS Replication service on the database. An integer is a valid entry.

DFSV Volumes USN Journal Unread Percentage The current percentage of the update sequence number (USN) journal that has not been read and processed by the DFS Replication service. An integer is a valid entry.

DFSV Volumes USN Journal Records Accepted The current number of USN journal records that are processed by the DFS Replication service. An integer is a valid entry.

DFSV Volumes USN Journal Records Read The current number of USN journal records that are read by the DFS Replication service. An integer is a valid entry.

DFSV Instance Name The name of the service volume instance.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second

Format	Description
mmm	Millisecond

Use the simple text strings described in the timestamp format 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 FQDN for this server.

DAI Host Name (Superseded) The FQDN 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 format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

DNS ADIntegrated Details attributes

The DNS ADIntegrated Details attributes include information about missing or invalid SRV records.

DAD SRV Records The SRV records that are either from ADSI or from the DNS server.

DAD Type of SRV Record The type of SRV record. The SRV record types can be global catalog (GC), domain controller (DC), or primary domain controller (PDC).

DAD Bad or Missing Specifies whether the SRV record is missing or invalid.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

DNS attributes

The DNS attributes display DNS information.

DNS AXFR Request Received The total number of full zone transfer requests received by the master DNS server. An integer is a valid entry.

DNS AXFR Request Sent The total number of full zone transfer requests sent by the secondary DNS server. An integer is a valid entry.

DNS AXFR Response Received The total number of full zone transfer responses received by the secondary DNS server. An integer is a valid entry.

DNS AXFR Success Received The total number of successful full zone transfers received by the secondary DNS server. An integer is a valid entry.

DNS AXFR Success Sent The total number of successful full zone transfers of the master DNS server. An integer is a valid entry.

DNS Caching Memory KB DNS caching memory.

DNS Database Node Memory KB The total caching memory used by DNS server. An integer is a valid entry.

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 NoOperation The total number of No-operation/Empty dynamic update requests received by the DNS server. An integer is a valid entry.

DNS Dynamic Update NoOperation Sec The average number of No-operation/Empty dynamic update requests received by the DNS server in each second. An integer is a valid entry.

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 DeltaDNS 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 Dynamic Update Written Database The total number of dynamic updates written to the database by the DNS server. An integer is a valid entry.

DNS Dynamic Update Written Database Sec The average number of dynamic updates written to the database by the DNS server in each second. An integer is a valid entry.

DNS IXFR Request Received The total number of incremental zone transfer requests received by the master DNS server. An integer is a valid entry.

DNS IXFR Request Sent The total number of incremental zone transfer requests sent by the secondary DNS server. An integer is a valid entry.

DNS IXFR Response Received The total number of incremental zone transfer responses received by the secondary DNS server. An integer is a valid entry.

DNS IXFR Success Received The total number of successful incremental zone transfers received by the secondary DNS server. An integer is a valid entry.

DNS IXFR Success Sent The total number of successful incremental zone transfers of the master DNS server. An integer is a valid entry.

DNS IXFR TCP Success Received The total number of successful TCP incremental zone transfers received by the secondary DNS server. An integer is a valid entry.

DNS IXFR UDP Success Received The total number of successful UDP incremental zone transfers received by the secondary DNS server. An integer is a valid entry.

DNS Is Read Only This attribute checks whether the DNS server is read only or writable. The Enum values can be:

- True
- False

DNS Nbstat Memory KB The total Nbstat memory used by DNS server. An integer is a valid entry.

DNS Notify Received The total number of notifies received by the secondary DNS server. An integer is a valid entry.

DNS Notify Sent The total number of notifies sent by the master DNS server. An integer is a valid entry.

DNS Record Flow Memory KB The total record flow memory used by DNS server. An integer is a valid entry.

DNS Recursive Queries The total number of recursive queries received by DNS server. An integer is a valid entry.

DNS Recursive Queries Sec The average number of recursive queries received by DNS server in each second. An integer is a valid entry.

DNS Recursive Query Failure The total number of recursive query failures. An integer is a valid entry.

DNS Recursive Query Failure Sec The average number of recursive query failures in each second. An integer is a valid entry.

DNS Recursive Send TimeOuts The total number of recursive query sending timeouts. An integer is a valid entry.

DNS Recursive TimeOuts Sec The average number of recursive query sending timeouts in each second. An integer is a valid entry.

DNS Response Time DNS response time.

DNS Secure Update Failure The total number of secure updates failed of the DNS server. An integer is a valid entry.

DNS Secure Update Received The total number of secure update requests received by the DNS server. An integer is a valid entry.

DNS Secure Update Received Sec The average number of secure update requests received by the DNS server in each second. An integer is a valid entry.

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

DNS TCP Message Memory KB The total TCP message memory used by DNS server. An integer is a valid entry.

DNS TCP Query Received The total number of TCP queries received by DNS server. An integer is a valid entry.

DNS TCP Query Received Sec The average number of TCP queries received by DNS server in each second. An integer is a valid entry.

DNS TCP Response Sent The total number of TCP responses sent by DNS server. An integer is a valid entry.

DNS TCP Response Sent Sec The average number of TCP responses sent by DNS server in each second. An integer is a valid entry.

DNS Total Query Received DeltaDNS 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 DeltaDNS 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 UDP Message Memory KB The total UDP message memory used by DNS server. An integer is a valid entry.

DNS UDP Query Received The total number of UDP queries received by DNS server. An integer is a valid entry.

DNS UDP Query Received Sec The average number of UDP queries received by DNS server in each second. An integer is a valid entry.

DNS UDP Response Sent The total number of UDP responses sent by DNS server. An integer is a valid entry.

DNS UDP Response Sent Sec The average number of UDP responses sent by DNS server in each second. An integer is a valid entry.

DNS WINS Lookup Received The total number of WINS lookup requests received by the server. An integer is a valid entry.

DNS WINS Lookup Received Sec The average number of WINS lookup requests received by the server in each second. An integer is a valid entry.

DNS WINS Response Sent The total number of WINS lookup responses sent by the server. An integer is a valid entry.

DNS WINS Response Sent Sec The average number of WINS lookup responses sent by the server in each second. An integer is a valid entry.

DNS WINS Reverse Lookup Received The total number of WINS reverse lookup requests received by the server. An integer is a valid entry.

DNS WINS Reverse Lookup Received Sec The average number of WINS reverse lookup requests received by the server in each second. An integer is a valid entry.

DNS WINS Reverse Response Sent The total number of WINS Reverse lookup responses sent by the server. An integer is a valid entry.

DNS WINS Reverse Response Sent Sec The average number of WINS Reverse lookup responses sent by the server in each second. An integer is a valid entry.

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 SOA Request Sent The total number of zone transfer SOA requests sent by the secondary DNS server. An integer is a valid entry.

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 format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

Format	Description
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in the timestamp format 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 Bind Domain Naming Master The current bind status of the Domain Naming Master. The bind status can be Success, Failure, or Not Available.

DCA Bind Infrastructure Master The current bind status of the Infrastructure Master. The bind status can be Success, Failure, or Not Available.

DCA Bind PDC Master The current bind status of the primary domain controller (PDC) Master. The bind status can be Success, Failure, or Not Available.

DCA Bind RID Master The current bind status of the relative ID (RID) Master. The bind status can be Success, Failure, or Not Available.

DCA Bind Schema Master The current bind status of the Schema Master. The bind status can be Success, Failure, or Not Available.

DCA Domain Name Default domain name associated with this server.

DCA Domain Naming Master The Domain Naming Master that is defined in the domain.

DCA Domain Naming Master Bind Time The time (in milliseconds) that is required to bind the Domain Naming Master. The following table gives the possible enum value:

Value	Description
-1	Undefined

DCA DCs In Site The number of domain controller servers in the local site.

DCA DCs In Site Bind The number of domain controller servers that can bind in the local site.

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 Bind The number of Global Catalog servers that are bounded.

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

DCA GCs In Site Bind The number of Global Catalog servers that can bind 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 Global Catalog Server Specifies whether this domain controller is a global catalog server.

DCA Hostname The FQDN for this server.

DCA Hostname (Superseded) The FQDN for this server.

DCA Infrastructure Master The Infrastructure Master that is defined in the domain.

DCA Infrastructure Master Bind Time The time (in milliseconds) that is required to bind the Infrastructure Master to the domain. The following table gives the possible enum value:

Value	Description
-1	Undefined

DCA PDC Master The PDC Master that is defined in the domain.

DCA PDC Master Bind Time The time (in milliseconds) that is required to bind the PDC Master to the domain. The following table gives the possible enum value:

Value	Description
-1	Undefined

DCA Ping Domain Naming Master The ping time for Domain Naming Master. The following table gives the possible enum values:

Value	Description
-1	Undefined
-2	Timed Out

DCA Ping Infrastructure Master The ping time for Infrastructure Master. The following table gives the possible enum values:

Value	Description
-1	Undefined
-2	Timed Out

DCA Ping PDC Master The ping time for PDC Master. The following table gives the possible enum values:

Value	Description
-1	Undefined
-2	Timed Out

DCA Ping RID Master The ping time for RID Master. The following table gives the possible enum values:

Value	Description
-1	Undefined
-2	Timed Out

DCA Ping Schema Master The ping time for Schema Master. The following values are valid: The following table gives the possible enum values:

Value	Description
-1	Undefined
-2	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 RID Master that is defined in the domain.

DCA RID Master Bind Time The time (in milliseconds) that is required to bind the RID Master to the domain. The following table gives the possible enum value:

Value	Description
-1	Undefined

DCA Schema Master The Schema Master that is defined in the domain.

DCA Schema Master Bind Time The time (in milliseconds) that is required to bind the Schema Master to the domain. The following table gives the possible enum value:

Value	Description
-1	Undefined

DCA Site Name The local site name.

DCA Time Difference The time on the domain controller where the agent is installed minus the time on the computer (in the same domain) where the gtimserv flag is set. If the domain controller cannot find the good time server in the domain, then the time difference is calculated from the preferred good time server, which is the PDC of the root domain.

Note: To ensure that the time difference is calculated correctly, Windows Time service must run on the domain controller where the agent is installed and on the time server that is used to calculate the DCA Time Difference attribute value.

DCA Time Difference (Superseded) The time on the domain controller where the agent is installed minus the time on the computer (in the same domain) where the gtimserv flag is set. If the domain controller cannot find the good time server in the domain, then the time difference is calculated from the preferred good time server, which is the PDC of the root domain.

Note: To ensure that the time difference is calculated correctly, Windows Time service must run on the domain controller where the agent is installed and on the time server that is used to calculate the DCA Time Difference attribute value.

DCA Time Server Name The name of the good time server or the preferred good time server. Good time server is the server on which the gtimeserv flag is set, and the preferred good time server is the PDC of the domain.

DCA Time Server Type Specifies whether the type of time server is a good time server or a preferred good time server.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 DB Page Evictions Sec The rate that database file page requests that require the database cache manager to allocate a new page from the database cache force another database page out of the cache. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

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

DCP Database Cache Percent Available The percentage of the database cache that can be allocated to the pages that are newly created or that are read from the database files. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Database Pages Written Per Sec The rate at which database pages are written to the database files from the database cache. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

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.

Note: This attribute is not available on Active Directory 2003 and Active Directory 2008, but is displayed as Undefined on the Tivoli Enterprise Portal client.

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

Note: This attribute is not available on Active Directory 2003 and Active Directory 2008, but is displayed as Undefined on the Tivoli Enterprise Portal client.

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

Note: This attribute is not available on Active Directory 2003 and Active Directory 2008, but is displayed as Undefined on the Tivoli Enterprise Portal client.

DCP Heap Allocations The current number of memory allocations in the MP heaps. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Heap Allocs Per sec The number of operations that the MP heap currently performs to allocate memory per second. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Heap Bytes Allocated The size of all memory allocations (in bytes) in the MP heap minus the overhead on heap memory allocations. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Heap Frees Per sec The number of operations that the MP heap currently performs to release memory per second. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP IO Database Reads In Heap The number of database read operations that are currently queued in the I/O heap of the database engine. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP IO Database Writes In Heap The number of database write operations that are currently queued in the I/O heap of the database engine. This attribute is available for Windows 2012.

DCP IO DB Reads Average Latency The average length of time, in milliseconds, per database read operation. The average length of time, in milliseconds, per database read operation.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO DB Reads Sec The rate of database read operations completed. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO DB Writes Average Latency The average length of time, in milliseconds, per database write operation. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO DB Writes Sec The rate of database write operations completed. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO Log Reads Average Latency The average duration (in milliseconds) that is taken by every log read operation. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP IO Log Reads In Heap The number of log read operations that are currently queued in the I/O heap of the database engine. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP IO Log Reads Sec The rate of logfile read operations completed. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO Log Writes Average Latency The average length of time, in milliseconds, per logfile write operation. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP IO Log Writes In Heap The number of log write operations that are currently queued in the I/O heap of the database engine. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP IO Log Writes Sec The rate of logfile write operations completed. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Page Bytes Committed The amount of the virtual memory (in bytes) that is committed. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Page Bytes Reserved The amount of virtual address space (in bytes) that is reserved. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

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

DCP Log Bytes Write Sec The rate bytes are written to the log. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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 Log Writes Sec The number of instances (per second) that the log buffers are written to the log file(s). An integer is a valid entry.

DCP Pages Converted The count of database pages that have been converted from an older format. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Pages Converted Sec The count of times per second a database page is converted from an older database format. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Record Deletes Per sec The rate at which records in the database tables are currently being marked for deletion. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Record Inserts Per sec The rate at which records are currently being inserted in the database tables. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Record Replaces Per sec The rate at which records in the database tables are currently updated. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Records Converted The count of database records that have been converted from an older format. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Records Converted Sec The count of times per second a database record is converted from an older database format. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Sessions In Use The number of database sessions currently open for use by client threads. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Sessions Percent Used The percentage of database sessions currently open for use by client threads. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DCP Table Closes Per sec The current number of database tables that are closed per second. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

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.

DCP Table Opens Sec The number of database tables opened per second. An integer is a valid entry.

DCP Threads Blocked The number of threads whose execution is currently suspended because a resource that is currently owned by another thread is not yet acquired. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Threads Blocked Per sec The rate at which the execution of threads is suspended because a resource that is currently owned by another thread is not yet acquired. A value of -1 indicates Undefined. This attribute is available for Windows 2012.

DCP Version Buckets Allocated Total number of version buckets allocated. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century

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

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

Event Log attributes

The Event Log attribute group contains event log entries that are related to the Directory Services or the Domain Naming System (DNS) Server of the Microsoft Active Directory.

EVTLOG Category The category of the event.

EVTLOG Description The description of the event. When the total length of the event description exceeds 512 characters, the agent truncates the value and displays only 512 characters on the Tivoli Enterprise Portal client.

EVTLOG Event Timestamp The date and time when the event was generated.

EVTLOG ID The event ID.

EVTLOG Log Name The name of the event log - Directory Services or DNS Server.

EVTLOG Source The event source that is defined by the service.

EVTLOG Type The type of the event. Event types can be Error, Warning, or Audit_Failure.

EVTLOG User The user of the service for which the event is generated.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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. A value of -1 indicates Undefined.

Note: This attribute is not available on Active Directory 2008 and is displayed as Undefined on all supported operating systems.

XDS Reads The percentage of directory reads from XDS. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is not available on Active Directory 2008 and is displayed as Undefined on all supported operating systems.

XDS Searches The percentage of directory searches from XDS. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is not available on Active Directory 2008 and is displayed as Undefined on all supported operating systems.

XDS Writes The percentage of directory writes from XDS. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is not available on Active Directory 2008 and is displayed as Undefined on all supported operating systems.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 Authentications The number of successful authentication checks made on packets received from any partner associated with this replica set member. An integer is a valid entry.

FRS Authentications in Error The cumulative number of authentication check failures detected on packets received from any partner associated with this replica set member. An integer is a valid entry.

FRS Bindings The number of successful RPC bind requests to the FRS server on any partner associated with this replica set member. An integer is a valid entry.

FRS Bindings in Error The cumulative number of unsuccessful RPC bind requests to the FRS server on any partner associated with this replica set member. An integer is a valid entry.

FRS Bytes of Files Installed The total number of bytes of staging file data that have been installed on this replica set member. An integer is a valid entry.

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 Issued The number of local plus remote file updates initiated on this replica set member. An integer is a valid entry.

FRS Change Orders Morphed The number of morphed change orders.

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

FRS Change Orders Propagated The number of local plus remote file updates that were propagated to the outbound log of this replica set member. The update remains pending in the outbound log until it has been delivered to all outbound partners. An integer is a valid entry.

FRS Change Orders Retired The number of local plus remote file updates that were retired on the replica set member.

FRS Change Orders Retried The number of local plus remote file updates that were tried again for some reason on the replica set member. An integer is a valid entry.

FRS Change Orders Retried at Install The number of local plus remote file updates that were tried again due to a stage file install problem on this replica set member. An integer is a valid entry.

FRS Change Orders Retried Fetch The number of local plus remote file updates that were tried again due to a stage file fetch problem on this replica set member. An integer is a valid entry.

FRS Change Orders Retried Generate The number of local plus remote file updates that were tried again due to a stage file generation problem on this replica set member. An integer is a valid entry.

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

FRS Change Orders Retried Rename The number of local plus remote file updates that were tried again due to a problem during the final target file rename or delete operation on this replica set member. An integer is a valid entry.

FRS Change Orders Received The number of received change orders.

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

FRS Communication Timeouts The cumulative number of FRS data or control packets not sent to an outbound partner because the send request timed out. An integer is a valid entry.

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 DS Objects The number of FRS configuration Objects retrieved from the directory service. An integer is a valid entry.

FRS DS Objects in Error The cumulative count of FRS configuration objects retrieved from the directory service that were missing either the distinguished name, object GUID or the relative distinguished name attributes. An integer is a valid entry.

FRS DS Polls The number of times FRS has polled the active directory for FRS configuration information on this computer. An integer is a valid entry.

FRS DS Polls With Changes The number of times FRS has polled the active directory for FRS configuration information and configuration changes were found. An integer is a valid entry.

FRS DS Polls Without Changes The number of times FRS has polled the active directory for FRS configuration information and no configuration changes were found. An integer is a valid entry.

FRS DS Searches The number of times FRS has made a search request to the active directory. An integer is a valid entry.

FRS DS Searches in Error The cumulative number of times FRS has made a search request to the active directory and the request returned with an error condition. An integer is a valid entry.

FRS Fetch Blocks Received The number of blocks of staging file data received from all inbound partners associated with this replica set member. An integer is a valid entry.

FRS Fetch Blocks Received KB The total number of bytes of staging file data received by this replica set member from all inbound partners. An integer is a valid entry.

FRS Fetch Blocks Sent The number of blocks of staging file data sent to any outbound partner associated with this replica set member. An integer is a valid entry.

FRS Fetch Blocks Sent KB The total number of bytes of staging file data sent to the outbound partners of this replica set member. An integer is a valid entry.

FRS Fetch Requests Received The number of staging files received from all inbound partners associated with this replica set member. An integer is a valid entry.

FRS Fetch Requests Sent The number of staging files requested from any inbound partner associated with this replica set member. An integer is a valid entry.

FRS Inbound Change Orders Dampened The number of change orders received from the partner associated with this connection that have been filtered out by the inbound dampening check.

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 Join Notifications Received The number of partner join notifications received from all inbound partners associated with this replica set member. An integer is a valid entry.

FRS Join Notifications Sent The number of inbound partner join requests or outbound partner ready-to-join notifications sent to all partners associated with this replica set member. An integer is a valid entry.

FRS Joins The number of successful joins with any partner associated with this replica set member. An integer is a valid entry.

FRS KB of Staging Fetched The total number of bytes of staging file data received by this replica set member from its inbound partners. An integer is a valid entry.

FRS KB of Staging Generated The total number of bytes of staging file data generated by this replica set member not including the number of bytes produced as part of regeneration. An integer is a valid entry.

FRS KB of Staging Regenerated The total number of bytes of staging file data regenerated by this replica set member for a specific outbound partner request. An integer is a valid entry.

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

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

FRS Outbound Change Orders Dampened The number of change orders sent to the partner associated with this connection that have been filtered out by the outbound dampening check and thus were never sent.

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 Replica Sets Created The cumulative number of replica sets to which this computer has been added as a member. An integer is a valid entry.

FRS Replica Sets Deleted The cumulative number of replica sets from which this computer's membership has been provisionally deleted, but could still be reanimated. An integer is a valid entry.

FRS Replica Sets Removed The cumulative number of replica sets from which this computer's membership has been permanently deleted. An integer is a valid entry.

FRS Replica Sets Started The number of replica sets for which processing has been started. An integer is a valid entry.

FRS Staging Files Fetched The number of staging files requested by this replica set member. An integer is a valid entry.

FRS Staging Files Generated The number of staging files generated by this replica set member. An integer is a valid entry.

FRS Staging Files Generated with Error The cumulative number of staging files generated by this replica set member where an error was detected during generation. An integer is a valid entry.

FRS Staging Files Regenerated The number of staging files regenerated by this replica set member for a specific outbound partner request. An integer is a valid entry.

FRS Threads exited The number of execution threads that have terminated. An integer is a valid entry.

FRS Threads started The number of new execution threads started. An integer is a valid entry.

FRS Unjoins The number of unjoins with any partner associated with this replica set member. An integer is a valid entry.

FRS Usn Reads The number of times FRS has initiated a read on the NTFRS change log. Each volume has its own change log. An integer is a valid entry.

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

FRS Usn Records Examined The number of NTFS change log records examined by FRS. An integer is a valid entry.

FRS Usn Records Rejected The number of NTFS change log records skipped by FRS. An integer is a valid entry.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year

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

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

Forest Topology attributes

The Forest Topology attributes display forest topology information.

FRT Common Name The common name of the active directory entity that is present in the schema.

FRT Distinguished Name The name that uniquely identifies an entry in the directory and is made up of attribute=value pairs, separated by commas.

Note: This attribute is now deprecated by FRT LDAP Distinguished Name

FRT DNS Domain Name The fully qualified DNS Domain Name.

FRT DNS Host Name The fully qualified DNS host name of the domain controller.

FRT Is ReadOnly DC The Boolean value that indicates whether the domain controller is read-only.

Note: The NOT SUPPORTED value that is displayed on the Tivoli Enterprise Portal indicates that the "ReadOnly DC" feature is not available with the current version of the Windows Server Active Directory. This attribute can only be available on Windows Server 2008.

FRT LDAP Distinguished Name The name that uniquely identifies an entry in the directory and is made up of attribute=value pairs, separated by commas.

FRT Parent Domain Parent domain of the active directory entity that exists in the schema.

FRT Site Name Site under which this domain controller falls.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 Creation Time The time when the Group Policy Object was created.

GPO GUID The Group Policy Object GUID.

GPO Modification Time The time when the Group Policy Object was last modified.

GPO Name The Group Policy Object name.

GPO Name (Superseded) The Group Policy Object name.

GPO Status The Group Policy Object Status. The Enum values can be:

- Enabled
- User Configuration Settings Disabled
- Computer Configuration Settings Disabled
- All Settings Disabled
- Not Available

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

Note: This attribute might be displayed as NOT AVAILABLE on the Tivoli Enterprise Portal client. The appearance of the Enum is not specific to any operating system. If the agent cannot find data for the attribute, NOT AVAILABLE is displayed on the Tivoli Enterprise Portal client.

GPO Version The version number for the GPO.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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.

Note: The Knowledge Consistency Checker attribute group is mislabeled as Kerberos Consistency Checker in some instances.

KCC Inter Site Topology Generator The status of the inter-site topology generator. The Enum values for this attribute can be:

- Enabled
- Disabled

KCC Inter Site Topology Generator Server The name of the inter-site topology generator domain controller for a local site. The Enum value for this attribute can be Not Available.

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 Site Name The name of the local site.

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

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 subsytem of the local directory service is using. An integer is a valid entry.

LDAP ATQ Threads LDAP The number of threads that ATQ has currently allocated to servicing LDAP requests. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

LDAP Bind Time The time in msec 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 Closed Connections sec The number of LDAP connections that have been closed in the last second. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

LDAP New Connections sec The number of new LDAP connections that have arrived in the last second. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

LDAP New SSL Connections sec The number of new SSL or TLS connections that arrived in the last second. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

LDAP Searches per sec 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. A value of -1 indicates Undefined.

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

LDAP UDP Operations per sec 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 sec The rate at which LDAP clients perform write operations. An integer is a valid entry.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

LDAP attributes

The LDAP attributes display information about the Lightweight Directory Access Protocol (LDAP).The data for this attribute group is collected after the duration of time that is specified in the **ADO_NUMBEROFOBJECTS_TIMEOUT** environment variable.

LDAP Attributes Disabled User Accounts The number of user accounts that are disabled. An integer is a valid entry. The following value is valid:

Value	Description
Not Available	The value cannot be collected.

LDAP Attributes Expired User Accounts The number of user accounts that have expired. An integer is a valid entry. The following value is valid:

Value	Description
Not Available	The value cannot be collected.

LDAP Attributes Expired Password User Accounts The number of users accounts whose passwords have not been modified in the number of days that are specified in the MAX_PASSWORD_AGE environment variable. An integer is a valid entry. The following values are valid:

Value	Description
Not Available	The value cannot be collected.
Password Never Expires	The password never expires for the user account.

LDAP Attributes Invalid Logon Attempts User Accounts The number of users that attempted to log on to their accounts with an incorrect password. An integer is a valid entry. The following value is valid:

Value	Description
Not Available	The value cannot be collected.

LDAP Attributes Inactive User Accounts The number of user accounts that have not been accessed for the number of days that are specified in the USER_INACTIVE_DAYS environment variable. An integer is a valid entry. The following value is valid:

Value	Description
Not Available	The value cannot be collected.

LDAP Attributes New User Accounts The number of user accounts that have been created in the last 7 days. An integer is a valid entry. The following value is valid:

Value	Description
Not Available	The value cannot be collected.

LDAP Attributes Recycle Bin Status The current status of the recycle bin. The following values are valid:

Value	Description
Enabled	The attribute is enabled.
Disabled	The attribute is disabled.
Not Supported	The attribute is not supported.

LDAP Attributes Offline Domain Join The eligibility of Offline Domain Join. The following values are valid:

Value	Description
Supported	The attribute is supported.
Not Supported	The attribute is not supported.

LDAP Attributes Users Locked The number of users that are currently locked. An integer is a valid entry.

LDAP Attributes Objects In Domain The number of objects that are in domain. An integer is a valid entry.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 Active Directory 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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.

LFO Type The Lost and Found Object type.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

Format	Description
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

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

Moved or Deleted Organizational Units attributes

The Moved or Deleted Organizational Units attributes provide information about the name, the distinguished name, and the status of the organizational units.

OU Collection Timestamp The date and time when the status information (moved or deleted) about the organizational unit is collected.

OU Current Distinguished Name The current distinguished name of the organizational unit.

OU Name The name of the organizational unit.

OU Previous Distinguished Name The previous distinguished name of the organizational unit.

OU Status The status of the organizational unit. The status can be Moved or Deleted.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in the timestamp format 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month
DD	Day

Format	Description
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

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

Netlogon attributes

The Netlogon attributes display information about the performance of the Netlogon authentication feature.

Instance Name The name of the Netlogon perfmon instance.

Semaphore Acquires The total number of times that a semaphore has been obtained for a secure channel while the secure channel is active.

Average Semaphore Hold Time The average time (in seconds) that a semaphore is held for the last sample.

Semaphore Holders The number of threads that currently hold a semaphore.

Semaphore Timeout The total number of times that threads have timed out while the threads waited to obtain a semaphore.

Semaphore Waiters The number of threads that are currently waiting to obtain a semaphore.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

Format	Description
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Password Settings Objects attributes

The Password Settings objects (PSO) attributes display the information that is related to the Active Directory PSO. This attribute group is supported for Windows Server 2008, and later.

Account Lockout Duration The duration (in minutes) after which a locked user account is automatically unlocked. The following table gives the possible enum value:

Value	Description
-1	Permanently Locked

Enforce Password History The number of times that new passwords must be created for a user account before a password can be reused.

Lockout Observation Window The duration (in minutes) after which the counter for failed logon attempts is reset to 0 (zero). The following table gives the possible enum value:

Value	Description
0	Not Available

Lockout Threshold The number of failed logon attempts after which the user account is locked. The following table gives the possible enum value:

Value	Description
0	Not Available

Maximum Password Age The maximum number of days that a password can be used after which the password must be changed. The following table gives the possible enum value:

Value	Description
-1	Never Expires

Minimum Password Age The minimum number of days that a password must be used before the password can be changed.

Minimum Password Length The minimum number of characters that are required in a password. The following table gives the possible enum value:

Value	Description
0	No Password Required

Password Complexity Enabled Indicates whether a password must meet the complexity requirements that can be enforced when the password is created or changed. The following table gives the possible enum values:

Value	Description
0	False
1	True

Password Reversible Encryption Enabled Indicates whether the password-reversible encryption is enabled for user accounts. The following table gives the possible enum values:

Value	Description
0	False
1	True

PSO Creation Time The date and time when the PSO was created.

PSO Modification Time The date and time when the PSO was last modified.

PSO Name The name of the Password Settings object.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the **`NODE`** environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month
DD	Day
HH	Hour

Format	Description
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in the timestamp format 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 The FQDN for this server.

DRA Hostname (Superseded) The FQDN for this server.

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

DRA Inbound Bytes Compressed per sec 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 (within site/sec) The number of incoming replicated bytes that were not compressed at the source. An integer is a valid entry.

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

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

DRA Inbound KBytes Compressed Since Boot After Compressed size in bytes of inbound compressed replication data (size after compression, from DSAs in other sites). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Inbound KBytes Compressed Since Boot Before Original size in bytes of inbound compressed replication data (size before compression, from DSAs in other sites). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Inbound KBytes Not Compressed Since Boot Number of bytes replicated in that were not compressed at the source (from DSAs in the same site). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Inbound KBytes Total Since Boot Total number of bytes replicated in. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Inbound Link Value Updates Remaining in Packet The number of link value 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. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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 sec The rate at which replication updates are received from replication partners. An integer is a valid entry.

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

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

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

DRA Inbound Total Connections The total number of replication connections that are inbound.

DRA Inbound Total Updates Remaining in Packet The number of total (link values and 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. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Inbound Values per sec 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 sec 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 sec After The compressed size of outbound compressed replication data, after compression. An integer is a valid entry.

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

DRA Outbound Bytes Not Compressed (within site/sec) The number of bytes replicated out that were not compressed. An integer is a valid entry.

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

DRA Outbound Connections The total number of outbound replication connections from the computer on which the agent is installed. An integer is a valid entry.

DRA Outbound KBytes Compressed Since Boot After Compressed size in bytes of outbound compressed replication data (size after compression, from DSAs in other sites). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Outbound KBytes Compressed Since Boot Before Original size in bytes of outbound compressed replication data (size before compression, from DSAs in other sites). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Outbound KBytes Not Compressed Since Boot Number of bytes replicated out that were not compressed (for example, from DSAs in the same site). An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Outbound KBytes Total Since Boot Total number of bytes replicated out. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

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

DRA Outbound Total Connections The total number of outbound replication connections. An integer is a valid entry.

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

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

DRA Pending Replication Operations The total number of replication operations on the directory that are queued for this server but not yet performed. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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 Failures on Schema Mismatch The number of sync requests made to neighbors that failed because their schema are not synchronized. An integer is a valid entry.

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 Threads Getting NC Changes The number of threads on the server which are currently attempting to acquire changes from another server. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

DRA Threads Getting NC Changes Holding Semaphore The number of threads on the server which are currently attempting to acquire changes from another server and hold a semaphore required to get these changes. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

Replication Conflict Objects attributes

The Replication Conflict Objects attributes provide information about the conflict objects that are created when two or more updates (for the same object) are simultaneously received by two different domain controllers.

CNFOBJ ADs Path The ADs path of the conflict object.

CNFOBJ Changed Timestamp The date and time when the conflict object was modified.

CNFOBJ Common Name The common name of the conflict object.

CNFOBJ Created Timestamp The date and time when the conflict object was created.

CNFOBJ Distinguished Name The distinguished name of the conflict object.

CNFOBJ Object Category The category of the conflict object.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 (Superseded) The text of the error message for the replication failure of the replication partner. The error message is truncated to 128 bytes.

RPL Fail Reason Text The text of the error message for the replication failure of the replication partner. The error message is truncated to 384 bytes.

RPL Hostname The FQDN for this server.

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

RPL Partner Last Attempt Time 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 host name 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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. When the replication partner clock is later than the local clock the value is positive. When the replication partner clock is earlier than the local clock the value is negative.

RLT Partner FQDN The fully qualified domain name (FQDN) of the replication partner.

RLT Hostname The FQDN for this server.

RLT Partner Name The host name 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

RID Pool Information attributes

The RID Pool Information attributes display information about the availability of RID pool resources in the domain.

Available RID The total number of RIDs that can be created in the domain.

Exhausted RID The exhausted RID plus one.

Exhausted RID Percentage The percentage of RIDs that are exhausted.

Next RID The RID that is available for the next security object.

RID Allocation Pool End The end of the RID pool that is currently allocated to the domain controller.

RID Allocation Pool Start The start of the RID pool that is currently allocated to the domain controller.

RID Block Size The number of RIDs that can be currently issued at one time to the domain controller by the RID master. A value of -1 indicates Undefined. The following table gives the possible enum values:

External value	Internal value	Description
N/A	-2	The monitored domain controller is not the RID FSMO role owner.
Value Exceeds Maximum	2147483647	The RID block size has exceeded 2147483647.

RID Master The name of the RID Master role owner.

RID Previous Allocation Pool End The end of the RID pool that was previously allocated to the domain controller.

RID Previous Allocation Pool Start The start of the RID pool that was previously allocated to the domain controller.

RID Pool Allocation Status Indicates whether the RID pool allocation is enabled. The following table gives the possible enum values:

External value	Internal value	Description
Enabled	-1	RID pool allocation is enabled.
Disabled	0	RID pool allocation is disabled.
Not Set	1	The value is not specified.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the **NODE** environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

Root Directory Server attributes

The Root Directory Server attributes display root directory server information.

RDS Active Directory Version The version of Microsoft Active Directory. The Microsoft Active Directory versions can be Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.

RDS Domain Controller Functionality Indicates the functional level of the domain controller. The valid functional levels are:

- Windows 2000 Mode
- Windows Server 2003 Mode
- Windows Server 2008 Mode
- Windows Server 2008 R2 Mode
- Windows Server 2012 Mode

Note: The NOT AVAILABLE value that is displayed on the Tivoli Enterprise Portal indicates that the information could not be retrieved or the information is not available.

RDS Domain Functionality Indicates the functional level of the domain. The valid functional levels are:

- Windows 2000 Domain Mode
- Windows Server 2003 Interim Domain Mode
- Windows Server 2003 Domain Mode
- Windows Server 2008 Domain Mode
- Windows 2008 R2 Domain Mode
- Windows 2012 Domain Mode

Note: The NOT AVAILABLE value that is displayed on the Tivoli Enterprise Portal indicates that the information could not be retrieved or the information is not available.

RDS Forest Functionality Indicates the functional level of the forest. The valid functional levels are:

- Windows 2000 Forest Mode
- Windows Server 2003 Interim Forest Mode
- Windows Server 2003 Forest Mode
- Windows Server 2008 Forest Mode
- Windows 2008 R2 Forest Mode
- Windows 2012 Forest Mode

RDS Root FQDN The fully qualified root domain name.

RDS Root Domain Name The root domain name.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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 Evaluation Latency The time taken by SAM to evaluate an account group. An integer is a valid entry.

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

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

SAM Domain Local Group Membership Evaluations sec The number of domain local group memberships evaluations per second at authentication time. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

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

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

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

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

SAM Query Displays per sec 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 Resource Group Evaluation Latency The mean latency of the last 100 resource group evaluations performed for authentication. An integer is a valid entry. A value of -1 indicates Undefined.

Note: This attribute is available only on Active Directory 2008, but is displayed as Undefined on Windows 2003 operating system.

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

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

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

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

SAM Universal Group Membership Evaluations per sec 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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.

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.

Server Name The managed system name. The format is *hostname*:*agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month

Format	Description
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

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

Sysvol Replication attributes

The Sysvol Replication attributes provide information about the Sysvol replication test.

SYSRPL Partner Name The name of the replication partner.

SYSRPL Replication Result The result of the Sysvol replication test. The result can be Success or Failure.

SYSRPL Replication Test Start Time The date and time on the domain controller when the Sysvol replication test was started.

SYSRPL Replication Test Verification Time The date and time on the domain controller when the results of Sysvol replication test are verified.

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

Format	Description
C	Century
YY	Year
MM	Month
DD	Day

Format	Description
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use the simple text strings described in the timestamp format 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 format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

Use the simple text strings described in the timestamp format 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. Attributes based on previous values are valid for situations only.

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.

Note: This attribute might be displayed as NOT AVAILABLE on the Tivoli Enterprise Portal client. The appearance of the Enum is not specific to any operating system. If the agent cannot find data for the attribute, NOT AVAILABLE is displayed on the Tivoli Enterprise Portal client.

Trust Dropped Whether this trust was recently dropped. Valid values include TRUE and FALSE. Attributes based on previous values are valid for situations only.

Trust Hostname The FQDN for this server.

Trust Local Domain Default domain name associated with this server.

Trust NetBIOS Name The NetBIOS name of the trusted domain.

Note: This attribute might be displayed as NOT AVAILABLE on the Tivoli Enterprise Portal client. The appearance of the Enum is not specific to any operating system. If the agent cannot find data for the attribute, NOT AVAILABLE is displayed on the Tivoli Enterprise Portal client.

Trust Status The status of the trust that is determined by running the netdom command line utility. Trust status can be Success, Failed, None, or NOT AVAILABLE.

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

Trust Topology attributes

The Trust Topology attributes display the Active Directory trust relationships of a single forest.

Note: The Trust Topology graph will show erroneous topology for the following two conditions:

1. The Active Directory is in an UNSTABLE state; that is, if a domain has been forcefully removed from the active directory setup and the metadata from the remaining domains has not been cleaned up.
2. A Trust relationship is in the process of being created - One side trust has been established, and the other side has not been configured yet. Such a relationship would be non-functional until the reverse trust has been established.

Trust Topology Domain Name The domain name of the trust relationship.

Note: This attribute can be displayed as NOT AVAILABLE on the Tivoli Enterprise Portal client. The appearance of the Enum is not specific to any operating system. If the agent cannot find data for the attribute, NOT AVAILABLE is displayed on the Tivoli Enterprise Portal client.

Trust Topology Trust Direction The direction of the trust relationship. The direction can be DISABLED, TWO WAY TRUST, INBOUND TRUST, or OUTBOUND TRUST.

Trust Topology Trust From The partner domain of the trust relationship that is used for creating a graphical topology view.

Trust Topology Trust Relation The trust relation with the partner domain. Relation can be either INTERNAL or EXTERNAL.

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

Server Name The managed system name. The format is *hostname:agent_code*.

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

In workspace queries, set this attribute equal to the *NODE* environment variable value to populate the workspace with data. This attribute is generally not included in situations unless you want to customize the situation for a specific managed system.

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

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

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

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 with historical data that 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.

The expected number of instances is a guideline that can be different for each attribute group. The expected number of instances of data that the agent returns depends on the application environment that is being monitored. For example, if your attribute group is monitoring each processor on your computer and you have a dual processor computer, the number of instances is two.

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 3 provides the following information required to calculate disk space for the Microsoft Active Directory agent:

- *DB table name* is the table name as it is displayed 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 3. Capacity planning for historical data logged by the Microsoft Active Directory agent

Table	Attribute group	Bytes per row (agent)	Database bytes per row (warehouse)	Aggregate bytes per row (warehouse)
K3ZADDB	Active_Directory_Database_ Information	1692	1776	2119
K3ZNTDSAB	Address_Book	272	139	449
K3ZCNFOBJ	Conflict_Objects	2828	2846	2883
K3ZNTDSCNT	Containers	876	886	923
K3ZNTDSDAD	DAD	372	375	412
K3ZNTDSDAI	DAI	1168	1050	1360
K3ZNTDSDRC	DFRC	404	415	842
K3ZNTDSDRF	DFRF	472	500	1590
K3ZNTDSDFS	DFS	412	314	1989
K3ZNTDSDSV	DFSV	384	390	622
K3ZNTDSDHC	DHCP	376	266	1434
K3ZNTDSDNS	DNS	612	549	3319
K3ZNTDSDS	Directory_Services	332	214	1109
K3ZNTDSDCA	Domain_Controller_Availability	1844	1770	2872

Table 3. Capacity planning for historical data logged by the Microsoft Active Directory agent (continued)

Table	Attribute group	Bytes per row (agent)	Database bytes per row (warehouse)	Aggregate bytes per row (warehouse)
K3ZNTDSDCP	Domain_Controller_Performance	444	438	2509
K3ZEVTLOG	Event_Log	3012	3024	3061
K3ZNTDSXDS	Exchange_Directory_Services	260	124	317
K3ZNTDSFRS	File_Replication_Service	536	469	2969
K3ZNTDSFRT	Forest_Topology	3308	3328	3365
K3ZNTDSGPO	GPO	704	572	609
K3ZNTDSKCC	Kerberos_Consistency_Checker	342	208	362
K3ZNTDSKDC	Kerberos_Key_Distribution_Centre	256	119	273
K3ZNTDSLDP	LDAP	300	174	757
K3ZNTDSLDA	LDAP_Attributes	152	159	547
K3ZNTDSLFO	LFO	372	234	271
K3ZNTDSLSA	Local_Security_Authority	256	119	273
K3ZOU	Moved_Or_Deleted_Organizational_ Unit	1859	1868	1905
K3ZNTLGON	NETLOGON_Attributes	384	390	574
K3ZNTDSNSP	Name_Service_Provider	260	124	317
K3ZNTDSPSO	Password_Setting_Objects	371	379	767
K3ZRID	RID_Pool_Information	213	232	632
K3ZNTDSDRA	Replication	872	800	3129
K3ZNTDSRPL	Replication_Partner	1272	1147	1199
K3ZNTDSRLT	Replication_Partner_Latency	704	575	729
K3ZNTDSRDS	Root_Directory_Server	508	514	551
K3ZNTDSSAM	Security_Accounts_Manager	320	199	977
K3ZNTDSSVC	Services	1368	1246	1283
K3ZSYSRPL	Sysvol_Replication	208	208	284
K3ZNTDSTRS	Trust	580	449	486
K3ZNTDSTTP	Trust_Topology	668	677	714

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

Chapter 5. Situations reference

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 or from the command-line interface using the tacmd commands for situations.

About situations

The monitoring agents that you use to monitor your system environment are shipped with a set of predefined situations that you can use as-is. You can also create new situations to meet your requirements.

Predefined situations contain attributes that check for system conditions common to many enterprises. Using predefined situations can improve the speed with which you can begin using the Microsoft Active Directory agent. You can change the conditions or values being monitored by a predefined situation to the conditions or values best suited to your enterprise.

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. 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.

Additional information about situations

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

Predefined situations

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

- 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
- Distributed File System Replication workspace situation
  - DFSR_Bandwidth_Savings_Low
  - DFSR_File_Installs_Retried_High
  - DFSR_Staging_Space_Low
  - DFSR_USN_Record_Accepted_High
- 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
  - DCA_Schema_Master_Warning situation
  - DCA_Domain_Naming_Master_Crit situation
  - DCA_RID_Master_Warning situation
  - DCA_Infrastructure_Master_Warn situation

  - DCA_Time_Difference_Warning
  - DCA_GCs_In_Site_Bind_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_Ordrs_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
- Group Policy Objects workspace situations
  - GPO_Inconsistent_Warning
- 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_Warn
  - DRA_Outbound_Bytes_Total_Warning (deprecated)
  - 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_Inter_Site_Stat_Crit
  - Repl_Part_Intra_Site_Stat_Crit
  - SYSRPL_Repl_Result_Failure_Crit
- Replication Partner Latency workspace situation
  - Replication_Latent_Warning
  - Repl_Part_Clock_Change_Warning
  - Replication_Partner_Unsync_Warn
- Trust workspace situations
  - Trust_Added_Warning
  - Trust_Dropped_Warning
  - Trust_Failing_Critical
- RID Pool Information workspace situation
  - RID_Block_Size_Warn
  - RID_Consumption_Crit
- Active Directory Database Information workspace situations
  - AD_DB_Log_Perct_Free_Space_Crit
  - AD_DB_Log_Perct_Free_Space_Warn
  - AD_DB_Perct_Free_Space_Crit
  - AD_DB_Perct_Free_Space_Warn
- Knowledge Consistency Checker workspace situation
  - KCC_Intersite_Topology_Generato
- LDAP Attributes workspace situation
  - LDAP_Attributes_Recycle_Bin_War

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

Situations descriptions

Each situation description provides information about the situation that you can use to monitor the condition of systems in your network.

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.

EIF Customize forwarding of the event to an Event Integration Facility receiver. (Available when the Tivoli Enterprise Monitoring Server has been configured to forward events.)

Until Options to close the event after a period of time, or when another situation becomes true.

The situations are organized by the workspace that the situations are associated with.

Active Directory Database Information workspace situations

AD_DB_Log_Perct_Free_Space_Crit situation

Monitors the percentage of free space that is available on the hard disk drive where the Microsoft Active Directory log files are stored. This situation indicates that the percentage of the available free space is very low and has exceeded the critical threshold. The formula for this situation is as follows:

```
ADDB_Percentage_Free_Disk_Space_for_Log Files LT 10
```

AD_DB_Log_Perct_Free_Space_Warn situation

Monitors the percentage of free space that is available on the hard disk drive where the Microsoft Active Directory log files are stored. This situation indicates that the percentage of the available free space is low and has exceeded the warning threshold. The formula for this situation is as follows:

```
ADDB_Percentage_Free_Disk_Space_for_Log_Files LT OR EQ 20

AND

ADDB_Percentage_Free_Disk_Space_for_Log_Files GT OR EQ 10
```

AD_DB_Perct_Free_Space_Crit situation

Monitors the percentage of free space that is available on the hard disk drive where the Microsoft Active Directory database is stored. This situation indicates that the percentage of the available free space is very low and has exceeded the critical threshold. The formula for this situation is as follows:

```
ADDB_Percentage_Free_Disk_Space_for_Database LT 10
```

AD_DB_Perct_Free_Space_Warn situation

Monitors the percentage of free space that is available on the hard disk drive where the Microsoft Active Directory database is stored. This situation indicates that the percentage of the available free space is low and has exceeded the warning threshold. The formula for this situation is as follows:

```
ADDB_Percentage_Free_Disk_Space_for_Database LT OR EQ 20

AND

ADDB_Percentage_Free_Disk_Space_for_Database GT OR EQ 10
```

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 acknowledgments 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

AND

DHCP_Requests_sec_percent_increase LT or EQ 25)

OR

(DHCP_Acks_sec_percent_increase GT 5

AND

DHCP_Acks_sec_percent_increase LT or EQ 25)
```

DHCP_Counters_Sudden_Inc_Warn situation

Monitors the rate of DHCP acknowledgments 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 acknowledgments. 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_Server EQ TRUE
AND
MISSING(Service_Name) EQ (DHCP Server))
```

DHCP_Service_Status_Critical situation

Monitors the DHCP server. The formula for this situation is as follows:

```
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
```

Distributed File System Replication workspace situation

DFSR_USN_Record_Accepted_High situation

This situation monitors the DFS-R update sequence number (USN) Records Accepted. The formula for this situation is as follows:

```
(CHANGE(DFSR_Volumes_USN_Journal_Records_Accepted) GT 5)
```

DFSR_Bandwidth_Savings_Low situation

This situation monitors DFS-R performance. The formula for this situation is as follows:

```
(DFSR_Folders_Bandwidth_Savings_Using_DFS_Replication LT 10
AND
DFSR_Folders_Bandwidth_Savings_Using_DFS_Replication GT 0)
```

OR

```
(DFSR_Connections_Bandwidth_Savings_Using_DFS_Replication LT 10
AND
DFSR_Connections_Bandwidth_Savings_Using_DFS_Replication GT 0)
```

DFSR_File_Installs_Retried_High situation

This situation monitors DFS-R file installs. The formula for this situation is as follows:

```
DFSR_Folders_File_Installs_Retried GT 0
```

DFSR_Staging_Space_Low situation

This situation monitors DFS-R update sequence number (USN) staging space. The formula for this situation is as follows:

```
DFSR_Folders_Staging_Space_In_Use GT 4,000,000
```

AND

```
CHANGE(DFSR_Folders_Staging_Files_Cleaned_up GT 0)
```

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_Server EQ TRUE AND MISSING(Service_Name) EQ DNS
```

DNS_Service_Status_Critical situation

Monitors the DNS server. The formula for this situation is as follows:

```
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_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:

```
DAI_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
```

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_Ping_RID_Master 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 situation

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
```

DCA_Schema_Master_Warning situation

Monitors Schema master role assigned to a DC. The formula for this situation is as follows:

```
DCA_Schema_Master NE DCA_Domain_Naming_Master
```

DCA_Domain_Naming_Master_Crit situation

Monitors Domain naming master role assigned to a DC. The formula for this situation is as follows:

```
DCA_FSMO_Role EQ 'Domain_Naming' AND DCA_Global_Catalog_Server EQ TRUE
```

DCA_RID_Master_Warning situation

Helps monitoring FSMO role. The formula for this situation is as follows:

```
DCA_RID_Master NE DCA_PDC_Master
```

DCA_Infrastructure_Master_Warn situation

Monitors Infrastructure Master role assigned to a DC. The formula for this situation is as follows:

```
(DCA_FSMO_Role EQ 'Infrastructure' AND DCA_Global_Catalog_Server EQ TRUE)
OR
(DCA_FSMO_Role EQ 'RID Pool' AND DCA_Global_Catalog_Server EQ TRUE AND
DCA_RID_Master EQ DCA_Infrastructure_Master)
```

DCA_Time_Difference_Warning situation

Monitors the time difference between the domain controller and the computer where the gtimserv flag is set. The formula for this situation is as follows:

```
DCA_Time_Difference EQ Time Error
```

DCA_GCs_In_Site_Bind_Warning situation

Monitors the status of global catalogs in a specific site. The formula for this situation is as follows:

```
DCA_GCs_In_Site_Bind NE DCA_GCs_In_Site_Pinged
```

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_KB_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 AND

DCP_Table_Open_Cache_Misses_Sec GT 300 AND

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. This situation is applicable only on systems running FRS. 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 cancelled. This situation is applicable only on systems running FRS. The formula for this situation is as follows:

```
FRS_Change_Orders_Aborted_Percent GT 30
```

FRS_Chng_Ordrs_Morphed_Prc_Warn situation

Monitors the percentage of change notifications that morphed. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. The formula for this situation is as follows:

```
FRS_KB_Staging_Space_Free LT 660,000
```

AND

```
FRS_KB_Staging_Space_Free GE 0
```

FRS_KB_Stage_Space_In_Use_Warn situation

Monitors available space in the staging directory that is currently in use. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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_Warn situation

Monitors the number of files installed in idle state. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. 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. This situation is applicable only on systems running FRS. The formula for this situation is as follows:

```
FRS_Usn_Records_Accepted GT 40
```

Group Policy Objects workspace situations

GPO_Inconsistent_Warning situation

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
```

Knowledge Consistency Checker workspace situation

KCC_Intersite_Topology_Generato situation

Monitors the status of the intersite topology generator. The formula for this situation is as follows:

```
KCC_Inter_Site_Topology_Generator EQ Disabled
```

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
```

LDAP Attributes workspace situation

LDAP_Attributes_Recycle_Bin_War situation

Monitors the status of the recycle bin. The formula for this situation is as follows:

```
LDAP_Attributes_Recycle_Bin_Status EQ Disabled
```

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
```

Moved or Deleted Organizational Units workspace situation

OU_Moved_Deleted_Information

Monitors the organizational units that are moved or deleted. The formula for this situation is as follows:

```
OU_Collection_Timestamp EQ Timestamp
```

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 GT 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
AND
DRA_Inbound_Objects_Per_Sec GT 0
```

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
AND
DRA_Inbound_Objects_Per_Sec GT 0
```

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
AND
Inbound_Properties_Total_Per_Sec GT 0
```

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
AND
DRA_Inbound_Properties_Total_Per_Sec GT 0
```

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_Warn 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
```

Note: Use this situation instead of the DRA_Outbound_Bytes_Total_Warning situation, which has been deprecated.

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
AND
DRA_Outbound_Objects_Filtered_Per_Sec GT 0
OR
DRA_Outbound_Objects_Percent_Filtered GT 50
AND
DRA_Outbound_Objects_Per_Sec GT 0
```

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_Before 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_Count EQ 0
```

Rep_Site_BridgeHeads_Warning situation

Monitors the number of bridgehead servers. The formula for this situation is as follows:

```
DRA_Site_BridgeHead_Count 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_Success_Time NE RPL_Partner_Last_Attempt_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
```

SYSRPL_Repl_Result_Failure_Crit situation

Monitors the status of Sysvol replication. The formula for this situation is as follows:

```
SYSRPL_Replication_Result EQ Failure
```

Replication Partner Latency workspace situations

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 5
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 1
OR RLT_Clock_Delta LT -1
```

RID Pool Information workspace situations

RID_Block_Size_Warn situation

Monitors the RID block size to ensure that the value of RID block size does not exceed 15000 in the registry. The formula for this situation is as follows:

```
RID_Block_Size GT 15000
```

RID_Consumption_Crit situation

Indicates that the consumption of RIDs in the global RID pool has reached the critical threshold of 90%. The formula for this situation is as follows:

```
Exhausted_RID_percentage GE 90
OR RID_Pool_Allocation_Status EQ DISABLED
```

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 6. Take Action commands reference

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

About Take Action commands

When included in a situation, the command runs 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.

In advanced automation, policies are used to take 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, the Tivoli Enterprise Portal receives return-code feedback, and advanced automation logic responds with subsequent activities that are prescribed by the feedback.

A basic Take Action command shows the return code of the operation in a message box that is displayed after the action is completed or in a log file. After you close this window, no further information is available for this action.

Additional information about Take Action commands

For more information about working with Take Action commands, see *Take Action commands* in the *Tivoli Enterprise Portal User's Guide*.

For a list of the Take Action commands for this monitoring agent and a description of each command, see "Take Action command descriptions" and the information for each individual command.

Take Action command descriptions

This chapter contains descriptions of each of the Take Action commands, which are listed alphabetically. The following information is provided after the description of each Take Action command:

Authorization role
The required authorization role, plus any required Microsoft Active Directory permissions

Arguments
List of arguments, if any, for the Take Action with a short description and default value for each one. Each argument is positionally dependent and mandatory. The arguments for the MS AD Take Actions are organized according to their respective positions on the GUI. If any argument requires an embedded space, the argument must be enclosed in double quotation marks.

When an argument is not required, a blank argument value must be used. A blank argument value is double quotation marks: "".

Destination systems
Where the command is to be executed: on the Managed System (monitoring agent) where the agent resides or on the Managing System (Tivoli Enterprise Monitoring Server) to which it is connected

Usage notes
Additional relevant notes for using the Take Actions

Fetch Disabled User Accounts

Displays a list of disabled user accounts in the `AD_Disabled_User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- mail
- ADsPath
- mobile

Authorization role
The user must be a domain user with local administrator rights.

Arguments
None

Destination system
Managed system

Usage notes
The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The `Take_Action_log1.log` and `Take_Action_log2.log` files are available at:

- For 32-bit agent:`\\CANDLE_HOME\TMAITM6\logs`
- For 64 bit agent: `\\CANDLE_HOME\TMAITM6_x64\logs`

.

Fetch Expired User Accounts

Displays a list of expired user accounts in the `AD_Expired_User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- mail
- ADsPath

- mobile

Authorization role
The user must be a domain user with local administrator rights.

Arguments
None

Destination system
Managed system

Usage notes
This action displays a list of user accounts that have expired.

The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The `Take_Action_log1.log` and `Take_Action_log2.log` files are available at:

- For 32-bit agent:`\\CANDLE_HOME\TMAITM6\logs`
- For 64 bit agent: `\\CANDLE_HOME\TMAITM6_x64\logs`

.

Fetch Expired Password User Accounts

Displays a list of user accounts whose passwords have expired. The list is displayed in the `AD_Expired_Paswd_User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- mail
- ADsPath
- mobile

Authorization role
The user must be a domain user with local administrator rights.

Arguments
None

Destination system
Managed system

Usage notes
This action displays a list of user accounts whose passwords have not been changed for the number of days that you specified in the **MAX_PASSWORD_AGE** environment variable.

The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The Take_Action_log1.log and Take_Action_log2.log files are available at:

- For 32-bit agent:\\CANDLE_HOME\TMAITM6\logs
- For 64 bit agent: \\CANDLE_HOME\TMAITM6_x64\logs

.

Fetch Inactive User Accounts

Displays a list of inactive user accounts in the AD_Inactive_User_Accounts.csv output file in the logs folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- mail
- ADsPath
- mobile

Authorization role

The user must be a domain user with local administrator rights.

Arguments

None

Destination system

Managed system

Usage notes

This action displays a list of users who have not logged on for the number of days that you specified in the **USER_INACTIVE_DAYS** environment variable.

The Take Action command log files are saved either in the Take_Action_log1.log file or in the Take_Action_log2.log file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The Take_Action_log1.log and Take_Action_log2.log files are available at:

- For 32-bit agent:\\CANDLE_HOME\TMAITM6\logs
- For 64 bit agent: \\CANDLE_HOME\TMAITM6_x64\logs

.

Fetch Invalid Logon Attempts User Accounts

Displays a list of users that have entered the wrong password while logging on to their accounts. The list is displayed in the `AD_ InvalidLogon _User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- badPwdCount
- mail
- ADsPath
- mobile

Authorization role

The user must be a domain user with local administrator rights.

Arguments

None

Destination system

Managed system

Usage notes

The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The `Take_Action_log1.log` and `Take_Action_log2.log` files are available at:

- For 32-bit agent:`\\CANDLE_HOME\TMAITM6\logs`
- For 64 bit agent: `\\CANDLE_HOME\TMAITM6_x64\logs`

.

Fetch Locked User Accounts

Displays a list of locked user accounts. The list is displayed in the `AD_ Locked _User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- mail
- ADsPath
- mobile

Authorization role

The user must be a domain user with local administrator rights.

Arguments

None

Destination system
Managed system

Usage notes
The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The `Take_Action_log1.log` and `Take_Action_log2.log` files are available at:

- For 32-bit agent:`\\CANDLE_HOME\TMAITM6\logs`
- For 64 bit agent: `\\CANDLE_HOME\TMAITM6_x64\logs`

.

Fetch New User Accounts

Displays a list of user accounts that have been created in the last 7 days. The list is displayed in the`AD_New_User_Accounts.csv` output file in the `logs` folder. The output file displays the details of the following columns:

- sAMAccountName
- userPrincipalName
- givenName
- whenCreated
- mail
- ADsPath
- mobile

Authorization role
The user must be a domain user with local administrator rights.

Arguments
None

Destination system
Managed system

Usage notes
The Take Action command log files are saved either in the `Take_Action_log1.log` file or in the `Take_Action_log2.log` file. When the size of any one log files exceeds 2 MB, the agent uses the other log file automatically.

For example, the agent starts logging events in the first log file. When the size of the first log file exceeds 2 MB, the agent starts logging events in the second log file. When the size of the second log file exceeds 2MB, the agent automatically flushes the first log file, and starts logging events in the first log file.

The `Take_Action_log1.log` and `Take_Action_log2.log` files are available at:

- For 32-bit agent:`\\CANDLE_HOME\TMAITM6\logs`
- For 64 bit agent: `\\CANDLE_HOME\TMAITM6_x64\logs`

Chapter 7. Policies reference

Policies are used as an advanced automation technique for implementing more complex workflow strategies than you can create through simple automation. All agents do not provide predefined policies, but you can create policies for any agent.

A *policy* is a set of automated system processes that can take 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 , the Tivoli Enterprise Portal receives return-code feedback, and advanced automation logic responds with subsequent activities prescribed by the feedback.

For more information about working with policies, see *Automation with policies* in the *Tivoli Enterprise Portal 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 provide predefined policies.

Chapter 8. Tivoli Common Reporting for the monitoring agent

You can use the Tivoli Common Reporting application to generate reports for the Microsoft Active Directory agent. For more information about Tivoli Common Reporting, such as prerequisites, importing reports, and running reports, see the *IBM Tivoli Monitoring Administrator's Guide V6.2.3*.

IBM Tivoli Monitoring for Microsoft Applications reports are historical reports that include summarized data that is collected in the Tivoli Data Warehouse. These reports are built to run only against the IBM Tivoli Monitoring for Microsoft Active Directory agent.

The reports can be administered and run on Tivoli Common Reporting V1.3, V2.1, V2.1.1, Fix Pack 6, and V3.1.

For more information about Tivoli Common Reporting, see the developerWorks website (http://www.ibm.com/developerworks/spaces/tcr).

This version of Tivoli Common Reporting includes Cognos Business Intelligence and Reporting V8.4.

Cognos-based report packages

The Cognos-based Tivoli Common Reporting tool is used to create, view, and manage reports for the Tivoli group of products.

You can use the Cognos reports to analyze resource information such as availability, utilization, performance, and so on. With Cognos reports, you can evaluate the key metrics of the computers that are on the managed environment of your organization.

You can use the Tivoli Common Reporting tool to:

- Create custom reports by using the drag-and-drop feature integrated with the web-based editor.
- Schedule, share, secure, and administer reports in a single interface.
- Save the report in HTML, PDF, Excel, XML, or CSV file formats.
- Share reports by email or save the reports in a file system for later use.

The following databases are supported for all reports:

- DB2 V9.5 and V9.7, Fix Pack 2
- Oracle 10g and 11g
- SQL Server 2000, 2005, and 2008

You can use Tivoli Common Reporting V1.3, V2.1, V2.1.1, Fix Pack 6, and V3.1 software that is shipped with *IBM Tivoli Monitoring V6.2.3*, or later to administer, run, and edit Cognos reports. For more information about Tivoli Common Reporting, see the Tivoli Common Reporting Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html).

Prerequisites

Before you run the Cognos-based reports, ensure that the prerequisites that are required for installing and running Tivoli Common Reporting packages are met.

Procedure

1. Install Tivoli Common Reporting. To install and configure Tivoli Common Reporting, see the documentation in the IBM Tivoli Common Reporting Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html).

   To ensure that Tivoli Common Reporting is running, go to: `https://machine_name:port_number/ibm/console/`.
2. Obtain the reports package from the product media and extract the package.

   The Cognos reports are available in the following package: `Product Media root/REPORTS/K3Z/ITCAMMA_ActiveDirectory_V710_Cognos_Reports`.
3. Copy this package in a directory on any drive of the same computer where the Tivoli Common Reporting Server is installed, and extract the package in the same directory.

   The directory contents include:

   - Database scripts required to prepare the Tivoli Data Warehouse for Cognos reports.
   - A report installer that imports the reports into Tivoli Common Reporting and sets up the database connection.
4. Open the `setup.batch` file, and verify that the specified drive is the same drive where the Tivoli Common Reporting Server is installed. If the specified drive is not correct, edit the `setup.batch` file to specify the correct drive.
   For example, change the `TCR_DEFAULT_DIR=C:\IBM\tivoli\tip` to `TCR_DEFAULT_DIR=F:\IBM\tivoli\tip` if the Tivoli Common Reporting Server is installed on the F drive.
5. Configure historical collection for Microsoft Active Directory agent and the IBM Tivoli Warehouse Summarization and Pruning Agent. After IBM Tivoli Monitoring V6.2.3, Fix Pack 1, or later is installed and the Microsoft Active Directory agent is installed and configured, configure historical collection. Also, configure the Warehouse Summarization and Pruning agent with or without shifts enabled. For more information about how to enable historical collection and configure the Warehouse Summarization and Pruning agent in IBM Tivoli Monitoring, see the following documentation:

   - http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/adminuse/history_manage_intro.htm
   - http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/adminuse/history_manage_collection.htm

     Note: Historical collection and daily and hourly summarization must be enabled for all attribute groups of Microsoft Active Directory agent.

   To ensure that the required views are present, run the following query against the Tivoli Data Warehouse:

   - DB2: Select distinct "VIEWNAME" from SYSCAT.VIEWS where "VIEWNAME" like ' %V'
   - Oracle: Select distinct "OBJECT_NAME" from OBJ where "OBJECT_TYPE" like '%V'
   - MS SQL Server: Select distinct "NAME" from SYS.OBJECTS where "TYPE_DESC" like '%V'

6. Prepare the Tivoli Data Warehouse to support Cognos dimensions.

   Preparing the Tivoli Data Warehouse for Tivoli Common Reporting includes creating the IBM_TRAM dimensions, which are required for running the Cognos reports and using the data models.

   See "Creating shared dimension tables and populating the time dimensions table" in the *IBM Tivoli Monitoring Administrator's Guide* at the IBM Tivoli Monitoring V6.2.3, Fix Pack 1 Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/adminuse/tcr_reports_dimensionsshared.htm).

7. Connect to the Tivoli Data Warehouse by using the database client over Open Database Connectivity (ODBC).

   Cognos uses ODBC to connect to the database. Install a database client on the Tivoli Common Reporting Server and connect it to the Tivoli Data Warehouse.

   See "Connecting to the Tivoli Data Warehouse using the database client over ODBC" in the *IBM Tivoli Monitoring Administrator's Guide* at the IBM Tivoli Monitoring V6.2.3, Fix Pack 1 Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3fp1/adminuse/tcr_tdwconnect.htm).

   Important: All prerequisites described here must be met or the reports cannot run.

Importing Cognos report packages

You must import the Cognos report package that contains the Microsoft Active Directory agent data model and reports into Tivoli Common Reporting. Before you import the Cognos report package, ensure that all the prerequisites have been met. Otherwise, reports cannot run.

For Tivoli Common Reporting V1.3, use one of the following options to import the Cognos report package:

- Importing by running the reports installer – For information about running the reports installer to import the Cognos report package, see "Installing and running IBM Cognos reports" in the *IBM Tivoli Monitoring Administrator's Guide* at the IBM Tivoli Monitoring V6.2.2, Fix Pack 2 Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.2fp2/tcr_install_itm.htm)
- Importing manually – For information about manually importing the reports package, see "Importing report packages" at the IBM Tivoli Systems Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr_cog.doc/ttcr_cog_import.html).

For Tivoli Common Reporting V2.1, or later, see "Importing report packages" at the Tivoli Common Reporting Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_import.html).

If you are using a schema other than ITMUSER, you must complete the following steps for the data model and reports to run:

1. Verify that you have completed the following steps:
   a. Altered the schema name in the database scripts when you prepared the Tivoli Data Warehouse for Cognos dimensions in Step 6 of "Prerequisites" on page 136.

b. Installed the reports package by using the Reports installer as explained in "Importing reports by using the report installer" topic in the *IBM Tivoli Monitoring Administrator's Guide*. To verify that you have installed the reports package, go to Tivoli Common Reporting and make sure you can see "ITCAMMA ActiveDirectory V710 Cognos Reports" in the Public Folders of IBM Cognos Connection.

2. Install and configure the Cognos Framework Manager, which is the data modeling tool. See the instructions at the Tivoli Common Reporting Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_import.html).
3. Open the Framework Manager. Select **File** > **Open**. Browse to the extracted ITCAMMA ActiveDirectory V710 Cognos Reports reports package. Browse to the model folder and select the `ITCAMMA ActiveDirectory V710 Cognos Reports.cpf` file.
4. If you are prompted to enter login credentials, enter your tipadmin user ID and password.
5. After the IBM Tivoli Monitoring for Active Directory data model in the Framework Manager opens, expand **Data Sources** under **Tivoli Reporting and Analytics Model** in the Project Viewer.
6. Select **TDW** under **Data Sources**.
7. When you select **TDW**, the Properties view is updated with information about the Tivoli Data Warehouse data source. By default, the Properties view is located at the bottom center of the screen. If the Properties view is not visible, select **View** > **Properties**.
8. In the Properties, edit the Schema field. Change it from `ITMUSER` to your schema name.
9. Save the project.
10. In the Project Viewer, expand **Packages**.
11. Right-click **ITCAMMA ActiveDirectory V710 Cognos Reports**.
12. Select **Publish Packages**. The Publish Wizard opens.
13. Keep the default selection and click **Next**.
14. Click **Next** on the next screen.
15. Clear the **Verify the package before publishing** check box.
16. Click **Publish**. A window is displayed that alerts you that `A package with that name already exists` and asks `Do you want to publish this package?`
17. Click **Yes**.
18. Go back to Tivoli Common Reporting and check if the Modified field of "ITCAMMA ActiveDirectory V710 Cognos Reports" in the Public Folders of IBM Cognos Connection shows the time of publishing.

After completing these steps, you can run any report from the IBM Tivoli Monitoring for ITCAMMA ActiveDirectory V710 Cognos Reports package.

Cognos data models and reports

When all the prerequisites are met, you can use the Tivoli Integrated Portal interface to create, modify, and manage Cognos reports.

In Tivoli Common Reporting, the historical data that is collected by the agent is used to build ad hoc reports and queries. The package that you import into Tivoli Common Reporting contains a Cognos data model. All the reports that you create in Tivoli Common Reporting are based on the data model.

Cognos data models are virtual star schema models that contain facts and dimensions. Facts are measurable quantities that can be aggregated, such as CPU utilization and number of processors. Dimensions are the main identifiers by which facts can be grouped, aggregated, and organized. For example, time and server are dimensions by which the fact CPU utilization can be grouped.

The facts in the data model are organized into the folders by their summarization type, such as Daily and Hourly. The Daily and the Hourly folders contain attribute groups that correspond to tables or views in the data warehouse. Each attribute group contains a group of facts and measures.

The data model is built on top of the data warehouse to organize data. The data model contains the Tivoli Reporting and Analytics Model (TRAM) Shared Dimensions, which are shared across Tivoli by products such as Time.

To create reports in Tivoli Common Reporting tool, you can use one of the following report authoring tools:

- Query Studio: A web-based product that is used mostly for ad hoc reporting. Users can create simple queries and reports, and apply basic formatting to the reports.
- Report Studio: A web-based tool that is used by technical users and professional report writers for creating advanced reports. Users can retrieve data from multiple databases and create sophisticated reports that have multiple pages and multiple queries.

Reports for the monitoring agent

You can verify whether the reporting functionality is installed and configured correctly by running the reports for the Microsoft Active Directory agent. The Microsoft Active Directory agent reporting package that you imported into Tivoli Common Reporting includes 10 reports.

Note: Before you run the reports, ensure that the database connection with the Tivoli Data Warehouse is defined and tested.

By using these reports, you can monitor the reporting activity and see what a typical Cognos report includes. These reports are available in the Common Reporting panel in Tivoli Common Reporting. The following tables describe these reports.

Table 4. Lightweight Directory Access Protocol report

Name	Lightweight Directory Access Protocol report
Description	This report displays information about the Lightweight Directory Access Protocol (LDAP).
Purpose	You can use this report to get information about the load on Active Directory.

Table 4. Lightweight Directory Access Protocol report (continued)

Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Aggregation Selection** **Aggregation Type** Select the aggregation type as Maximum or Average. **Display Options** **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list.
Tables/Views Used	LDAP_%V

Table 4. Lightweight Directory Access Protocol report (continued)

Output	This report displays information about the LDAP client session, LDAP search, and LDAP successful binds for a server for a report period. You can select the maximum (MAX) or average (AVG) aggregation type from the parameters. By default, the report displays information about all the servers with the average values of LDAP client session, LDAP search, and the LDAP successful binds for the report period that you have selected. The table below the charts displays the load summary on Active Directory. Click on the bar to drill down to the Active Directory Authentication report.
Usage	The administrators and mangers can use this report to determine the load on Active Directory that is created by the LDAP search and LDAP client session.

Table 5. Active Directory Authentication report

Name	Active Directory Authentication report
Description	This report displays information about the authentication activity on the Active Directory server.
Purpose	You can use this report to find authentication information on the Active Directory server.

Table 5. Active Directory Authentication report (continued)

Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Aggregation Type** Select the aggregation type as Maximum or Average. **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list.
Tables or views used	• Name_Service_Provider_%V • K3ZNTDSKDC_%V
Output	This report displays information about the authentication activity in the domain. It displays a line chart for Kerberos authentication (KDC) and NTLM authentication for the selected server, summarization type, and the selected report period. The Kerberos authentication table displays information about the average authentication request and the ticket request arrived. You can select the maximum or average aggregation type from the parameters. By default, this report displays the average values.

Table 5. Active Directory Authentication report (continued)

Usage	The IT administrators and managers can use this report to identify the login authentication request on the Active Directory server.

Table 6. Flexible Single Master Operation Role Availability report

Name	Flexible Single Master Operation Role Availability report
Description	This report displays information about the availability of the Flexible Single Master Operation (FSMO) server roles of Active Directory.
Purpose	You can use this report to identify if there is a problem in the availability of FSMO servers.
Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list.
Tables or views used	Domain_Controller_Availability_%V

Table 6. Flexible Single Master Operation Role Availability report (continued)

Output	This report displays information about the FSMO server availability. Each chart displays information about one FSMO Server. The table below each chart contains information about the values displayed in the chart. Move the mouse pointer over the chart to see the values of the FSMO server availability in the hover help.
Usage	The IT administrator can use this report to identify unreachable FSMO servers on multiple Active Directory servers.

Table 7. Replication Failure on Directory Partition report

Name	Replication Failure on Directory Partition report
Description	This Report displays information about the replication failure on the directory partition of the domain controller
Purpose	You can use this report to identify the performance of the Active Directory servers.
Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select an end date from the calendar and an end time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list.

Table 7. Replication Failure on Directory Partition report (continued)

Tables or views used	Replication_Partner_%V
Output	This report displays the average number of replication failures on the directory partition for the selected server with the selected report period, and the summarization type. Move the mouse pointer over the graph to see the value in the hover help.
Usage	The IT administrator can use this report to identify the performance of all the domain controller in terms of replication failures.

Table 8. Replication Failure on Partners report

Name	Replication Failure on Partners report
Description	This Report displays information about the replication failure on Replication Partners of the selected domain controller.
Purpose	You can use this report to identify the performance of the Replication Partners.

Table 8. Replication Failure on Partners report (continued)

Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select an end date from the calendar and an end time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list.
Tables or views used	Replication_Partner_%V
Output	This report displays the maximum number of replication failures on Replication Partner for the selected server, report period and the summarization type. Move the mouse pointer over the graph to see the values in the hover help. If there is no data available for the selected parameter, then an appropriate message is displayed.
Usage	The IT administrator can use this report to identify the performance of all Replication Partners of the selected domain controller in terms of replication failures.

Table 9. Service Availability report

Name	Service Availability report
Description	This report displays the availability of the selected services on multiple servers.

Table 9. Service Availability report (continued)

Purpose	You can use this report to identify the availability of essential services on Active Directory server.
Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Service Name** Select the name of the service from the **Service Name** list.
Tables or views used	Services_%V
Output	This report displays information about the availability of the selected service on different Active Directory server for the selected report period. The table below the chart displays the values of all the states of the selected service on multiple servers. This report displays the availability of the selected service for top 25 servers.
Usage	The managers can use this report to get the summary of the service availability in terms of percentage, which is basic and essential service for performing Active Directory.

Table 10. DNS Performance report

Name	DNS Performance report

Table 10. DNS Performance report (continued)

Description	The report displays the DNS performance of Active Directory server.
Purpose	You can use this report to identify failure and success operations performed by DNS.
Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list. **Number of Servers** Select multiple servers from the list.
Tables or views used	DNS_%V

Table 10. DNS Performance report (continued)

Output	This report displays information about the Average DNS response time, Average Dynamic Update failure percent and Average Dynamic Transfer failure percent for the selected servers with selected report period and summarization type. The table below the chart displays aggregated average response time; dynamic update failure percent and dynamic transfer failure percent. The threshold line is defined for DNS response time, dynamic update failure percent and dynamic transfer failure percent. These lines appear as red dotted color lines. DNS Average Response Line chart displays data for ten servers. DNS Dynamic Update failure and Average Dynamic Transfer update failure chart displays data for top ten servers by values.
Usage	The IT administrators and managers can use this report for managing the application and DNS server performance. This report can be used to keep track of the number of query requests handled by the server and the time that the DNS takes to respond the request.

Table 11. Global Catalog Server Availability report

Name	Global Catalog Server Availability report
Description	This report displays information about the availability of the Global Catalog (GC) servers of the Active Directory.
Purpose	You can use this report to identify if there is a problem in the availability of the GC servers.

Table 11. Global Catalog Server Availability report (continued)

Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list. **Number of Servers** Select multiple servers from the list.
Tables or views used	K3ZNTDSDCA_%V
Output	This report displays information about the number of total Global Catalog available, number of down Global Catalog and the number of pinged Global catalog for the selected server, the selected report period, and the selected summarization type. The table below the chart displays information about the chart. If there is no data available for the selected parameter, appropriate message is displayed.
Usage	The IT administrators and managers can use this report to identify if there are problems in the Active Directory domain.

Table 12. Trust Availability report

Name	Trust Availability report
Description	This report displays information about the availability of trust across the domain controllers
Purpose	You can use this report to get trust availability information between domain controllers.
Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Summarization Selection** **Summarization Type** Select the summarization type, such as Hourly, Daily, Weekly, Monthly, Quarterly, Yearly, or Default from the list. If you select the Default option, the summarization type is calculated according to the number of days in the date range. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list. You can select all the server instances at a time by selecting the **All** option from the list. **Number of Servers** Select multiple servers from the list.
Tables or views used	Trust _%V

Table 12. Trust Availability report (continued)

Output	This report displays information about the availability of the trust in Active Directory. The stacked bar chart displays Trust availability (or success), Trust Failed, and Trust unknown in term of percentage for the selected server and for the selected report period. The table below the chart displays the detailed information of trust like Trust NetBIOS Name, Trust Domain, Trust Direction, Trust Type, Trust Status, Trust Local Domain and Trust Host Name.
Usage	The IT administrators and managers can use this report to view information about the status of the trust. The administrator can also use this report to check if the trust between two domains is failed.

Table 13. Replication Latency Heat Map report

Name	Replication Latency Heat Map report
Description	This report displays information about the replication latency .The replication latency is the time period for an update that occurs on the originating domain controller to reach all other domain controllers that need it.
Purpose	You can use this report to calculate the replication delay in Active Directory domain

Table 13. Replication Latency Heat Map report (continued)

Parameters	**Date Range** **Report period** Select the report period from a predefined date range, such as Last Week, Current Month, Last 30 Days, and so on. You can also enter a start date, an end date, and the time for the reporting period. **Start Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **End Date** Select a start date from the calendar and the start time from the time widget. You must select both date and time. **Resource Selection** **Server Name** Select the name of the server from the **Server Name** list. **RTL Partner Name** Select the RTL partner name from the **RTL Partners** list. **Shift Period** If shift period is enabled, the hourly tables display the Shift Period as 1 (off-peak hours) or 2 (peak hours), depending on the peak and off-peak hours that are configured in the data warehouse. In the daily tables, the value 1 corresponds to peak hours, the value 2 corresponds to off-peak hours, and the value -1 corresponds to the summarized value for that day. If shifts are not enabled, the default value is -1. **Vacation Period** If Vacation Period is not enabled, the default value is -1 (All Days). You can enter the value 0 (Work Days) or 1 (Vacation Days), if Vacation Period is enabled. **Thresholds** The threshold values that are represented by the various status colors are entered. Default values in minutes are as follows: • Good: Less than or Equal to 1 • Fair: Between 1 and 3 • Warning: Between 3 and 5 • Bad: Between 5 and 10
Tables or views used	Replication_Partner_Latency_HV
Output	The Number of Lock Requests/Timeouts in a Sec heat map displays the lock requests per second and lock timeouts per second. The first column in the chart represents dates during the selected time period and the other columns represent 24 hours of the day starting from zero. The last column represents the average value for available latency record. You can specify the threshold values for the colors in the parameters. Heat chart displays data in minutes. Move the mouse pointer over a particular icon, to see the attribute value for a particular hour in hover help.
Usage	The IT administrators and managers can use this report to view the trend of the replication latency.

Chapter 9. Troubleshooting

This chapter explains how to troubleshoot the IBM Tivoli Composite Application Manager (ITCAM) for Microsoft Applications: Active Directory Agent. Troubleshooting 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 the Prerequisites topic for the agent in the information center.

This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information. Also see "Support information" on page 180 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 156 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 Composite Application Manager for Microsoft Applications: Microsoft 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 troubleshooting features

The primary troubleshooting feature in the IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent is logging. *Logging* refers to the text messages and trace data generated by the Microsoft 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" for more information.

Problem classification

The following types of problems might occur with the Microsoft Active Directory agent:

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

This chapter 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 Troubleshooting Guide* for general troubleshooting 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 157
- "Examples: using trace logs" on page 159
- "RAS trace parameters" on page 160

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 158 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 IBM Tivoli Composite Application Manager for Microsoft Active Directory agent, 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” 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 Microsoft Active Directory agent 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 Microsoft Active Directory agent 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 Microsoft Active Directory agent 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 158 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 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. On the 64-bit computer, the RAS1 log files are located in the *install_dir*\tmaitm6_x64\logs path. **Note:** File names for RAS1 logs include a hexadecimal time stamp.	Traces activity of the monitoring agent.
	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 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 Microsoft Active Directory agent, 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 157 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

This section provides examples to demonstrate using trace logs.

About this task

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 Microsoft Active Directory agent. 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 "RAS trace parameters" provide these entries.

Procedure

On the Windows system, complete the following steps 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.

RAS trace parameters

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

See"Overview of log file management" on page 156 to ensure that you understand log rolling and can reference the correct log files when you manage log file generation.

Setting RAS trace parameters by using the GUI

On Windows systems, you can use the graphical user interface to set trace options.

About this task

The IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent uses RAS1 tracing and generates the logs described in "Principal trace log files" on page 157. The default RAS1 trace level is ERROR.

Procedure

1. Open the Manage Tivoli Enterprise Monitoring Services window.

2. Select **Advanced** > **Edit Trace Parms**. The Tivoli Enterprise Monitoring Server Trace Parameters window is displayed.
3. Select a new trace setting in the pull-down menu in the **Enter RAS1 Filters** field or type a valid string.
   - 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.
4. Modify the value for Maximum Log Size Per File (MB) to change the log file size (changes LIMIT value).
5. Modify the value for Maximum Number of Log Files Per Session to change the number of log files per startup of a program (changes COUNT value).
6. Modify the value for Maximum Number of Log Files Total to change the number of log files for all startups of a program (changes MAXFILES value).
7. 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. The **KDC_DEBUG** setting and the **Maximum error tracing** setting can generate a large amount of trace logging. Use these settings only temporarily, while you are troubleshooting problems. Otherwise, the logs can occupy excessive amounts of hard disk space.
8. Click **OK**. You see a message reporting a restart of the monitoring agent so that your changes take effect.

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

Manually setting RAS trace parameters

You can manually edit the RAS1 trace logging parameters.

About this task

The Microsoft Active Directory agent uses RAS1 tracing and generates the logs described in “Principal trace log files” on page 157. The default RAS1 trace level is ERROR.

Procedure

1. Open the trace options file:
   - **Windows systems:**

     install_dir\tmaitm6\K3ZENV_*instance name*
   - **UNIX systems:**

     install_dir /config/3z_*instance name*.config
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:

- **MAXFILES**: The total number of files that are to be kept for all startups of a specific program. When this value is exceeded, the oldest log files are discarded. The default value is 9.
- **LIMIT**: The maximum size, in megabytes (MB) of a RAS1 log file. The 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. The default is 3.
  - **PRESERVE**: The number of files that are not to be reused in the rolling cycle of one program startup. The 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.

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

Problems and workarounds

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

- "Installation and configuration troubleshooting"
- "Agent troubleshooting" on page 168
- "Workspace troubleshooting" on page 173
- "Troubleshooting for remote deployment" on page 172
- "Situation troubleshooting" on page 174

Note: You can resolve some problems by ensuring that your system matches the system requirements listed in the Prerequisites topic for the agent in the information center for IBM Tivoli Composite Application Manager for Microsoft Applications.
This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Installation and configuration troubleshooting

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 IBM Tivoli OMEGAMON®, Version 350, agents.	Fixpacks for OMEGAMON, Version 350, are delivered as each monitoring agent is upgraded to IBM Tivoli Monitoring. **Note:** The IBM Tivoli Monitoring download image or CD includes application fix packs for the monitoring agents that are installed from that CD (for example, the agents for operating systems such as Windows, Linux, UNIX, and IBM 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 IBM 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 V350 monitoring agents must be upgraded to a new Linux on IBM zSeries® 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.
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 Microsoft Active Directory agent 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.

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

Problem	Solution
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.
Installation errors occur when installing a previous version of the monitoring agent after installing the 6.1.2 version of the agent.	Verify that the remote agent is at a lower version before attempting to run the remote installation with the -v option. For example if V6.1.2 is already present, do not force the V6.1.1 agent installation. After an inadvertent backlevel to V6.1.1, run the V6.1.2 installation (or higher) to upgrade the agent.
Historical Data is not getting collected for the new attributes.	Historical Data collection needs to be re-configured to include new attributes in the existing attribute groups that have been configured for data collection in the Tivoli Enterprise Monitoring Server when an upgrade is performed. If this is not re-configured, historical data is not collected for the configured attributes on the portal and erroneous data is collected for the new attribute groups.
If you install the Active Directory Agent, and configure it with a non-admin user, then the Tivoli Enterprise Portal shows that the agent has stopped.	Perform the following steps to run the agent with a non-admin user: 1. Create a user in the Active Directory agent. By default, this user is a member of the **Domain** user's group. 2. Assign this user to the **Performance Monitors** user's group. 3. Navigate to the candle home folder `//Install Directory/IBM/ITM/`. 4. In the **Security** tab, click **Edit.** 5. Add the non-admin user and assign write permission to the user. 6. Configure the agent service with this non-admin user and start the agent. The agent will show data for all attribute groups. **Note:** If you remove the user from the **Performance Monitors** user's group and from the candle home folder with write permission, then the agent shows only non-perfmon data. This is an expected behavior. If you remove write permission from the candle home folder, then the agent does not show any data on the Tivoli Enterprise Portal.

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

Problem	Solution
You have installed the Microsoft Active Directory agent on your computer and have configured historical data collection for the following attribute groups: • Directory Services attribute group • Distributed File Replication Service Volumes (DFSV) In the Configuration panel of the History Collection Configuration window, if you change the collection location of the Directory Services attribute group in the **Collection Location** list from Tivoli Enterprise Monitoring Agent to Tivoli Enterprise Monitoring Server or vice versa, the following error message is displayed: `KFWITM521E Collection: collection setting_variable cannot store data in the selected location, please select another collection location.` **Note:** This problem does not occur on if you have used IBM Tivoli Monitoring v6.2.2, Fix Pack 7, V6.2.2, Fix Pack 8, or V6.2.3, Fix Pack 1.	Complete the following steps to resolve this problem: 1. Stop the collection of historical data for the Directory Services attribute group. 2. Delete the collection setting. 3. Create a new collection setting with the desired location for the Directory Services attribute group.
You have installed an agent of ITCAM for Microsoft Applications remotely from the Tivoli Enterprise Portal Client. On the **Agent** tab of the Managed System Configuration window, you selected the **Use this account** option, and typed the account information in the "user@domain.com" format (for example, `administrator@itmagents.com`). The Deployment Status Detail view shows the agent deployment status as `failed`; however, the agent is configured and installed with the LocalSystem account instead of the specified user account.	Specify the account information in the `domain\user` format.
When you use the Installation Launch Pad to install a 32-bit agent on a 32-bit computer, the following message is displayed: `The following components cannot be installed because the installation action failed. IBM Tivoli Composite Application Manager for Microsoft Applications V6.2.3 for Windows on 64-bit AMD and Intel systems (x64)`	No action is required. You can ignore this message and continue with the installation.

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 Troubleshooting 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

About this task

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 host name
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network host name portion of the agent name. For example, instead of just the host name myhost1 being used, the resulting host name 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 file 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 troubleshooting

This section lists problems that might occur with agents.

This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting 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. (Continued on the next page)
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. (Continued)	If ephemeral endpoints are used, the Warehouse Proxy Agent is accessible from the Tivoli Enterprise Monitoring Server associated with the agents using ephemeral connections either by running the Warehouse Proxy Agent on the same computer or by using the Firewall Gateway feature. (The Firewall Gateway feature relays the Warehouse Proxy Agent connection from the Tivoli Enterprise Monitoring Server computer to the Warehouse Proxy Agent computer if the Warehouse Proxy Agent cannot coexist on the same computer.)

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)" might support only ASCII characters. For example "Attribute (Unicode)" will support unicode but "Attribute" without "(Unicode)" might only support 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.
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.
When editing a workspace, adding a query, or editing a query, the **Add Attributes** window does not list the newly added attributes by the agent.	To display all the available attributes follow the directions below: 1. Open the Query Editor. 2. Select the required navigator item to edit the required query or click on **Create Query** to create a new query. 3. The click **Add Attributes** to add required attributes.
Tivoli Enterprise Portal Server shows different icon after creation of incoming realm trust as compared with outgoing trust for the same domain.	The change in the icon is unavoidable as it is a part of the topology graph design. This icon represents an 'implied' node, since it has a relation to it (the To-From relation defined for the topology graph) and is not present in the node identifier column. Currently there is no workaround for this problem.
LDAP Successful Bind attribute appears with value `0` on portal though this attribute is absent in Perfmon on Windows 2003 system while it appears as `Undefined` on Windows 2008 system.	Currently there is no workaround for this problem.
If you are logged in to the Tivoli Enterprise Portal as a domain user, Proxy Agent Service stops working on IBM Tivoli Monitoring V6.2.2.	Currently there is no workaround for this problem.
You have installed the ITCAM for Microsoft Applications agent and the Windows OS agent in the IPV6 environment. In the **Agent Management Services** navigator, the IP address in the **Agents' Runtime Status** view is displayed in the IPV4 format instead of the IPV6 format.	There is no solution to this problem.

Table 18. Agent problems and solutions (continued)

Problem	Solution
You see the Microsoft Active Directory agent in a different logical view on the Tivoli Enterprise Portal, if you move the agent from one site to another site.	Use the following steps to move the Active Directory agent from one site to another: 1. From the Tivoli Management Services window, stop the Microsoft Active Directory agent. 2. On the Tivoli Enterprise Portal, select the Active Directory logical view. 3. Right-click the server that corresponds to the Microsoft Active Directory agent that you want to move and Select **Clear offline entry**. 4. Move the Microsoft Active Directory agent to the other site. 5. From the Tivoli Management Services window, start the Microsoft Active Directory agent. 6. On the Tivoli Enterprise Portal Active Directory logical view, click **Update**.
When you add or remove instances from the following Perfmon objects, the Tivoli Enterprise Portal does not display the updated list of instances: • DFS Replication Connections • DFS Replication Folders • DFS Service Volumes	Recycle the Microsoft Active Directory agent after you add or remove an instance from the following Perfmon objects: • DFS Replication Connections • DFS Replication Folders • DFS Service Volumes
Perform the following steps to start the 64-bit agent: 1. Unconfigure the agent. 2. Reconfigure and start the agent. You have installed a 64-bit agent of ITCAM for Microsoft Applications V6.2.3, on a computer that has preinstalled ITCAM for Microsoft Applications agents on the same computer. When you try to uninstall and reinstall the 64-bit agent of ITCAM for Microsoft Applications V6.2.3, on the computer, the 64-bit agent does not start automatically.	Perform the following steps to start the 64-bit agent: 1. Unconfigure the agent. 2. Reconfigure and start the agent.
If you have installed the Microsoft Active Directory agent V6.3 on a domain controller that has a domain name with 64 characters, the Take action commands do not work.	Upgrade the IBM Tivoli Monitoring Server from version 6.2.2, Fix Pack 2 to version 6.2.3, Fix Pack 1.

Table 18. Agent problems and solutions (continued)

Problem	Solution
You have installed the Microsoft Active Directory agent on your computer and configured historical data collection for the following attribute groups: • Directory Services • Distributed file Replication Service Volumes In the **Configuration** panel of the History Collection Configuration window, if you change the collection location of the Directory Services attribute group in the **Collection Location** list from **Tivoli Enterprise Monitoring Agent** to **Tivoli Enterprise Monitoring Server** or vice versa, the following error message is displayed: `KFWITM521E Collection: DS, cannot store data in the selected location, please select another collection location.` **Note:** This problem does not occur on if you have used IBM Tivoli Monitoring v6.2.2, Fix Pack 7, V6.2.2, Fix Pack 8, or V6.2.3, Fix Pack 1.	Stop the collection of historical data for the Directory Services attribute group, and then change the location for data collection.
When you remotely install the monitoring agent, you cannot see the options to perform remote operations in the physical and logical views of a navigator item on the Tivoli Enterprise Portal. When you connect the Windows OS agent and the monitoring agent for the first time to Tivoli Enterprise Monitoring Server, the options to perform remote operations are available in the physical view. However, when you assign the logical view to the managed system and update the logical view, the options to perform remote operations disappear from the logical and physical views of a navigator item.	Complete one of the following tasks to resolve this problem: • Use the command line interface to perform remote operations. • Compete the following steps to resolve this problem: 1. Stop the monitoring agent. 2. Remove the entries for the agent from the logical and physical views and update the navigator items. 3. Start the monitoring agent.

Table 18. Agent problems and solutions (continued)

Problem	Solution
You have enabled the self-describing agent feature for the Tivoli Enterprise Portal Server. When you upgrade the monitoring agent support for Tivoli Enterprise Portal Server to version 6.3, the support files are not automatically upgraded to version 6.3.	Upgrade the monitoring agent support manually to version 6.3 of Tivoli Enterprise Portal Server.

Troubleshooting for remote deployment

Table 19 lists problems that might occur with remote deployment. This section provides information about troubleshooting remote deployment of the monitoring agent. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting 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 Microsoft Active Directory agent, 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.
Remote deployment feature does not work with IBM Tivoli Monitoring 6.2.1.	IBM Tivoli Monitoring 6.2.1 Interim Fix 2 needs to be applied to enable remote deployment feature.
In the "*xxx*agent.exe Properties" window, the following agent information is not updated: • Copyright • File Version • Product Version • Language • Date Modified This problem occurs on both Windows 32-bit and 64-bit operating systems. **Note:** On Windows 2003 systems, the agent information is shown in the **Version** tab; however, on Windows 2008 systems, the agent information is shown in the **Details** tab.	There is no solution to this problem.

Table 19. Remote deployment problems and solutions (continued)

Problem	Solution
While configuring attributes for historical data collection in the History Collection Configuration window, if you select **TEMS** in the **Collection Location** field, the attribute group tables are not created in the Tivoli Data Warehouse. This problem occurs only when TEMS is on z/OS systems.	In the History Collection Configuration window, select **TEMA** in the **Collection Location** field.

Workspace troubleshooting

Table 20 shows problems that might occur with workspaces. This chapter provides agent-specific troubleshooting information. See the IBM Tivoli Monitoring Troubleshooting Guide

Table 20. Workspace problems and solutions

Problem	Solution
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, "Agent installation and configuration," on page 7 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.
The Hidden workspace Domain Controllers Details from the Trust Topology graphs shows the Domain Controllers Details only if the source domain is within the local forest that is with an internal trust relation.	Currently there is no workaround for this problem.
You cannot log in as a **VITUSER**.	The user ID VIRTUSER is created in the TEPS when you install program the logical view program, but to be able to use it, you must set it up as an OS account (or LDAP account) on the TEMS. Please refer to User Administration chapter in the ITM 6.2.1 User's Guide at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.1/itm_user276.htm#admin_user_id_add.

Table 20. Workspace problems and solutions (continued)

Problem	Solution
The agents are renamed in physical navigator tree.	To make identification easier and navigation more intuitive, the host name where the Active Directory agents are running is appended to the name of the agent itself, in the logical navigator view. This change propagates to the physical navigator view as well. You can revert this change by right-clicking the **node** and selecting **Properties**.
You cannot add the Active Directory node in the Active Directory Logical view.	Update the Tivoli Enterprise Monitoring Agent host entry in the DNS of the Tivoli Enterprise Portal Server.
The LDAP Searches attribute is displayed as a line graph with respect to the Active Directory node scale in the Active Directory LDAP Utilization composite workspaces, and the % Processor Time attribute is displayed as a line graph with respect to the Active Directory node scale in the following composite workspaces: • Active Directory NTDS Utilization • Active Directory Service Utilization	Currently there is no workaround for this problem.
You have installed the Tivoli Enterprise Monitoring Server on a z/OS system. In the Configuration panel of the History Collection Configuration window, if you have selected **Tivoli Enterprise Monitoring Server** from the **Collection Location** list, then the Tivoli Enterprise Portal does not display historical data for the following attribute groups: • Address Book • Directory system Agent	Reconfigure the history collection and set the collection location to Tivoli Enterprise Monitoring Agent for these attribute groups.
The site name and host name attributes are concatenated. When the total length exceeds 64 characters, the agent truncates the value of the following 10 attributes of the Domain Controller Availability attribute group and displays only 64 characters on the Tivoli Enterprise Portal client for the Flexible Single Master Operations (FSMO) roles: • DCA PDC Master • DCA Domain Naming Master • DCA RID Master • DCA Schema Master • DCA Infrastructure Master • DCA Previous PDC Master • DCA Previous Domain Naming Master • DCA Previous RID Master • DCA Previous Schema Master • DCA Previous Infrastructure Master	There is no solution to this problem.

Situation troubleshooting

This section provides information about both general situation problems and problems with the configuration of situations. See the *IBM Tivoli Monitoring Troubleshooting Guide* for more information about troubleshooting 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 "RAS trace parameters" on page 160. 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 Tivoli Enterprise Console 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 6.1.2 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 6.1.2 Event Sync installed on your Tivoli Enterprise Console server. 2. Obtain updated baroc files from IBM Tivoli Monitoring 6.1.2 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 6.1.2 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.
User defined values for state and description of a situation change to their predefined value after you upgrade the ADO agent.	There is no equivalent upgrade file for k3z_kcj.sql, so any predefined situation severity change made by the customer will be reverted to the original predefined value during an upgrade.
You cannot trigger situations that have strings in the formula, in IBM Tivoli Monitoring V6.2.1.	Use the **SCAN** operator in IBM Tivoli Monitoring V6.2.2. The **SCAN** operator triggers the situation even when the formula string contains substrings. E.g. If you compare a string like **ps30932** or **aps3093** with the formula string **ps30932**, the situation will be triggered.
A modified formula is seen for the following situations in the User's Guide, Online help, and Tivoli Enterprise Portal if you do a fresh agent installation: • DRA_Inbound_Obj_Appl_Pct_Warn • DRA_Inbound_Prop_Appl_Pct_Warn • DRA_Inbound_Obj_Filt_Pct_Warn • DRA_Inbound_Prop_Filt_Pct_Warn • DRA_Outbound_Obj_Filt_Pct_Warn • DHCP_Counters_Abnormal_Inc_Warn If you upgrade the agent, updated formulas are seen only in the Online help, but not in the Tivoli Enterprise Portal.	Currently there is not solution for this problem.
If the expert advice for a situation contains a hyperlink to an external web site (for example, a Microsoft TechNet website) and you click the hyperlink, the web site opens in an external window. However, the external window stops responding.	The external window starts responding after you close the Preview window and the Situation Editor window.

Problems with configuration of situations

Table 22 lists problems that might occur with situations.

This section provides information for troubleshooting for agents. Be sure to consult the *IBM Tivoli Monitoring Troubleshooting Guide* for more general troubleshooting 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 monitoring server has been seeded for the agent support. If not, seed the server for the agent support, 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.
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.

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

Problem	Solution
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.

Tivoli Common Reporting troubleshooting

Table 24 on page 179 contains a list of problems that might occur with the Tivoli Common Reporting predefined reports for Microsoft Active Directory agent.

For information about troubleshooting for the Tivoli Common Reporting tool, see http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/tcr_welcome.html.

Table 24. Tivoli Common Reporting for Microsoft Active Directory agent problems and solutions

Problem	Solution
When you simultaneously query two tables in the Query Studio interface, no data is displayed. However, when you query the two tables separately, data is displayed.	This problem occurs when a relationship between the tables is not defined. To resolve this problem, ensure that all the ad hoc queries have at least one identifier.
When you create an ad hoc query by dragging some columns in the Query Studio interface, the following error message is displayed: `RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions' status='-232'.`	This is an SQL error related to arithmetic flow. This error is generated because the average or the sum for certain columns is more than the threshold size that is defined in the database. To resolve this error, use the limited columns and add a standard timestamp while creating an ad hoc query.
If a view or a table for the selected summarization type does not exist in the database for a report, the report does not open and the following error message is displayed: `RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions' status='-232'.`	To resolve this problem, complete the following tasks: • Verify that the summarization and pruning agent is working correctly. • Generate data for all the summarization types. • Verify that the warehouse is collecting historical data.
When you run a report, the report is not displayed in the correct format and the following error message is displayed: `RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions' status='-232'.`	This problem occurs due to incorrect data source. To resolve this problem, complete the following tasks: • Verify that the datasource configuration parameters are configured correctly. • Verify that the specified values for the parameters of the summarization and pruning agent such as database URL, driver user, and password match with the values of these parameters on the database.
If data is not available in the database for the selected parameters, the following error message is displayed after querying these parameters: `Empty data set No data returned by query. Try another set of parameters.`	To resolve this error, complete the following tasks: • Configure the summarization and pruning agent and verify that it is working correctly. • Generate data for all the summarization types in the database.
Reports are not generated correctly in the Microsoft Excel format.	There are some limitations to generate reports in the Microsoft Excel format. To view these limitations, see the IBM Cognos Business Intelligence Information Center (http://publib.boulder.ibm.com/infocenter/cbi/v10r1m0/index.jsp?topic=%2Fcom.ibm.swg.im.cognos.ug_cr_rptstd.10.1.0.doc%2Fug_cr_rptstd_id32474excel_limitations.html).
When you view a report spanning multiple pages in the PDF format, the report parameters section is displayed at the top of each page.	No solution is available for this problem at this time.

Table 24. Tivoli Common Reporting for Microsoft Active Directory agent problems and solutions (continued)

Problem	Solution
Charts are not displayed correctly in Microsoft Excel 2007.	No solution is available for this problem at this time.
Labels for some charts are displayed in the HTML output, but are not displayed in the PDF output.	The font size is rendered differently in the HTML and the PDF output. In the PDF output, some fonts are not displayed because of the large font size. To resolve this issue, reduce the font size by completing the following steps: 1. Open the report in Report Studio. 2. Click the chart. 3. In the chart properties, select **Font**. 4. Modify the font properties, such as family, size, weight, and style. 5. Save the settings, and run the report in the PDF format.
If you drag the K3Z_GPO_Name_v710 column to the report area during an ad hoc query, the following error message is displayed: `UDA-SQL-0115 Inappropriate SQL request. UDA-SQL-0564[Microsoft OLE DB Provider for SQL Server]Deferred prepare could not be completed.UDA-SQL-0564 [Microsoft OLE DB Provider forSQL Server]Statement(s) could not be prepared. (SQLSTATE=42000, SQLERRORCODE=8180)UDA-SQL-0564 [Microsoft OLE DB Provider forSQL Server]Invalid column name <'column name'> (SQLSTATE=42S22, SQLERRORCODE=207)`	There is no solution to this problem.

Support information

If you have a problem with your IBM software, you want to resolve it quickly.

IBM provides the following ways for you to obtain the support you need:

Online

The following websites contain troubleshooting information:

- Go to the IBM Software Support website (http://www.ibm.com/support/entry/portal/software) and follow the instructions.
- Go to the Application Performance Management Wiki (http://www.ibm.com/developerworks/servicemanagement/apm/index.html). Feel free to contribute to this wiki.

IBM Support Assistant

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install

the ISA software, go to the IBM Support Assistant website (http://www.ibm.com/software/support/isa).

Appendix A. Upgrading for warehouse summarization

The Microsoft Active Directory agent 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 chapter 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 25 contains a list of the time periods and the suffixes for the summary tables and views.

Table 25. 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 25. 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 26 shows the expansion to summary columns of some of the most commonly used attribute types.

Table 26. 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. Event mapping

The Tivoli Event Integration Facility (EIF) interface is used to forward situation events to Tivoli Netcool/OMNIbus or Tivoli Enterprise Console.

EIF events specify an event class and the event data is specified as name value pairs that identify the name of an event slot and the value for the slot. An event class can have subclasses. IBM Tivoli Monitoring provides the base event class definitions and a set of base slots that are included in all monitoring events. Agents extend the base event classes to define subclasses that include agent-specific slots. For Microsoft Active Directory agent events, the event classes correspond to the agent attribute groups, and the agent-specific slots correspond to the attributes in the attribute group.

A description of the event slots for each event class is provided in this topic. The situation editor in the Tivoli Enterprise Portal can be used to perform custom mapping of data to EIF slots instead of using the default mapping described in this topic. For more information about EIF slot customization, see the*Tivoli Enterprise Portal User's Guide* .

Tivoli Enterprise Console requires that event classes and their slots are defined in BAROC (Basic Recorder of Objects in C) files. Each agent provides a BAROC file that contains event class definitions for the agent and is installed on the Tivoli Enterprise Monitoring Server in the `TECLIB` directory (`install_dir/cms/TECLIB` for Windows systems and `install_dir/tables/TEMS_hostname/TECLIB` for UNIX systems) when application support for the agent is installed. The BAROC file for the agent and the base BAROC files provided with Tivoli Monitoring must also be installed onto the Tivoli Enterprise Console. For details, see "Setting up event forwarding to Tivoli Enterprise Console" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Each of the event classes is a child of K3Z_Base and is defined in the `BegiN_PAC_AVA_CODE_LOWER_EnD.baroc` (version vNext) file. The K3Z_Base event class can be used for generic rules processing for any event from the IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent.

Table 27. 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
Containers	ITM_Containers event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_cnt_partition: STRING • k3z_cnt_common_name: STRING • k3z_cnt_distinguished_name: STRING • k3z_cnt_class_type: STRING • k3z_cnt_create_timestamp: STRING • k3z_cnt_modify_timestamp: STRING
DAD	ITM_DAD event class with these slots: • server_name: STRING • timestamp: STRING • k3z_dad_srv_records: STRING • k3z_dad_type_of_record: INTEGER • k3z_dad_type_of_record_enum: STRING • k3z_dad_bad_or_missing: INTEGER • k3z_dad_bad_or_missing_enum: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DAI	ITM_DAI event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: 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
DFRC	ITM_DFRC event class with these slots: • server_name: STRING • timestamp: STRING • k3z_dfrc_connections_bandwidth_savings_using_dfs_replication: INTEGER • k3z_dfrc_connections_rdc_kbytes_received: INTEGER • k3z_dfrc_connections_rdc_compressed_size_of_files_received: INTEGER • k3z_dfrc_connections_rdc_size_of_files_received: INTEGER • k3z_dfrc_connections_rdc_number_of_files_received: INTEGER • k3z_dfrc_connections_bytes_received_second: INTEGER • k3z_dfrc_connections_compressed_size_of_files_received: INTEGER • k3z_dfrc_connections_size_of_files_received: INTEGER • k3z_dfrc_connections_total_files_received: INTEGER • k3z_dfrc_connections_total_kbytes_received: INTEGER • k3z_dfrc_instance_name: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DFRF	ITM_DFRF event class with these slots: • server_name: STRING • timestamp: STRING • k3z_dfrf_folders_bandwidth_savings_using_dfs_ replication: INTEGER • k3z_dfrf_folders_rdc_kbytes_ received: INTEGER • k3z_dfrf_folders_rdc_compressed_size_of_ files_received: INTEGER • k3z_dfrf_folders_rdc_size_of_files_ received: INTEGER • k3z_dfrf_folders_rdc_number_of_files_ received: INTEGER • k3z_dfrf_folders_compressed_size_of_ files_received: INTEGER • k3z_dfrf_folders_size_of_files_ received: INTEGER • k3z_dfrf_folders_total_files_ received: INTEGER • k3z_dfrf_folders_deleted_ space_in_use: INTEGER • k3z_dfrf_folders_deleted_ bytes_cleaned_up: INTEGER • k3z_dfrf_folders_deleted_ files_cleaned_up: INTEGER • k3z_dfrf_folders_deleted_ bytes_generated: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DFRF (continued)	ITM_DFRF event class with these slots: • k3z_dfrf_folders_deleted_files_ generated: INTEGER • k3z_dfrf_folders_updates_ dropped: INTEGER • k3z_dfrf_folders_file_installs_ retried: INTEGER • k3z_dfrf_folders_file_installs_ succeeded: INTEGER • k3z_dfrf_folders_conflict_folder_ cleanups_completed: INTEGER • k3z_dfrf_folders_conflict_space_ in_use: INTEGER • k3z_dfrf_folders_conflict_bytes_ cleaned_up: INTEGER • k3z_dfrf_folders_conflict_files_ cleaned_up: INTEGER • k3z_dfrf_folders_conflict_bytes_ generated: INTEGER • k3z_dfrf_folders_conflict_files_ generated: INTEGER • k3z_dfrf_folders_staging_space_ in_use: INTEGER • k3z_dfrf_folders_staging_bytes_ cleaned_up: INTEGER • k3z_dfrf_folders_staging_files_ cleaned_up: INTEGER • k3z_dfrf_folders_staging_bytes_ generated: INTEGER • k3z_dfrf_folders_staging_files_ generated: INTEGER • k3z_dfrf_instance_name: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DFS	ITM_DFS event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_dfsr_volumes_database_lookups: INTEGER • k3z_dfsr_volumes_database_commits: INTEGER • k3z_dfsr_volumes_usn_journal_unread_ percentage: INTEGER • k3z_dfsr_volumes_usn_journal_records_ accepted: INTEGER • k3z_dfsr_volumes_usn_journal_records_ read: INTEGER • k3z_dfsr_connections_bandwidth_savings_ using_dfs_replication: INTEGER • k3z_dfsr_connections_rdc_kbytes_received: INTEGER • k3z_dfsr_connections_rdc_compressed_ size_of_files_received: INTEGER • k3z_dfsr_connections_rdc_size_of_files_ received: INTEGER • k3z_dfsr_connections_rdc_number_of_files_ received: INTEGER • k3z_dfsr_connections_bytes_received_ second: INTEGER • k3z_dfsr_connections_compressed_size_of_ files_received: INTEGER • k3z_dfsr_connections_size_of_files_ received: INTEGER • k3z_dfsr_connections_total_files_received: INTEGER • k3z_dfsr_connections_total_kbytes_ received: INTEGER • k3z_dfsr_folders_bandwidth_savings_ using_dfs_replication: INTEGER • k3z_dfsr_folders_rdc_kbytes_received: INTEGER • k3z_dfsr_folders_rdc_compressed_size_of_ files_received: INTEGER • k3z_dfsr_folders_rdc_size_of_files_received: INTEGER • k3z_dfsr_folders_rdc_number_of_files_ received: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DFS (Continued)	ITM_DFS event class with these slots: • k3z_dfsr_folders_compressed_size_ of_files_received: INTEGER • k3z_dfsr_folders_size_of_files_received: INTEGER • k3z_dfsr_folders_total_files_received: INTEGER • k3z_dfsr_folders_deleted_space_in_use: INTEGER • k3z_dfsr_folders_deleted_bytes_ cleaned_up: INTEGER • k3z_dfsr_folders_deleted_files_cleaned_up: INTEGER • k3z_dfsr_folders_deleted_bytes_generated: INTEGER • k3z_dfsr_folders_deleted_files_generated: INTEGER • k3z_dfsr_folders_updates_dropped: INTEGER • k3z_dfsr_folders_file_installs_retried: INTEGER • k3z_dfsr_folders_file_installs_succeeded: INTEGER • k3z_dfsr_folders_conflict_folder_ cleanups_completed: INTEGER • k3z_dfsr_folders_conflict_space_in_use: INTEGER • k3z_dfsr_folders_conflict_bytes_cleaned_up: INTEGER • k3z_dfsr_folders_conflict_files_cleaned_up: INTEGER • k3z_dfsr_folders_conflict_bytes_generated: INTEGER • k3z_dfsr_folders_conflict_files_generated: INTEGER • k3z_dfsr_folders_staging_space_in_use: INTEGER • k3z_dfsr_folders_staging_bytes_cleaned_up: INTEGER • k3z_dfsr_folders_staging_files_cleaned_up: INTEGER • k3z_dfsr_folders_staging_bytes_generated: INTEGER • k3z_dfsr_folders_staging_files_generated: INTEGER
DFSV	ITM_DFSV event class with these slots: • server_name: STRING • timestamp: STRING • k3z_dfsv_volumes_database_lookups: INTEGER • k3z_dfsv_volumes_database_commits: INTEGER • k3z_dfsv_volumes_usn_journal_unread_percentage: INTEGER • k3z_dfsv_volumes_usn_journal_records_accepted: INTEGER • k3z_dfsv_volumes_usn_journal_records_read: INTEGER • k3z_dfsv_instance_name: STRING

Table 27. 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_ enum: STRING • k3z_dhcp_discovers_sec: INTEGER • k3z_dhcp_informs_sec: INTEGER • k3z_dhcp_milliseconds_ packet: INTEGER • k3z_dhcp_offers_sec: INTEGER • k3z_dhcp_packets_received_ sec: INTEGER • k3z_dhcp_releases_sec: INTEGER • k3z_dhcp_v6_declines_sec: INTEGER • k3z_dhcp_v6_declines_sec_ enum: STRING • k3z_dhcp_v6_duplicates_ dropped_sec: INTEGER • k3z_dhcp_v6_duplicates_ dropped_sec_enum: STRING • k3z_dhcp_v6_packets_ expired_sec: INTEGER • k3z_dhcp_v6_packets_ expired_sec_enum: STRING • k3z_dhcp_v6_active_ queue_length: INTEGER • k3z_dhcp_v6_active_ queue_length_enum: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DHCP (continued)	ITM_DHCP event class with these slots: • k3z_dhcp_v6_acks_ sec: INTEGER • k3z_dhcp_v6_acks_ sec_enum: STRING • k3z_dhcp_v6_requests_sec: INTEGER • k3z_dhcp_v6_requests_sec_enum: STRING • k3z_dhcp_v6_informs_sec: INTEGER • k3z_dhcp_v6_informs_sec_ enum: STRING • k3z_dhcp_v6_milliseconds_ packet: INTEGER • k3z_dhcp_v6_milliseconds_ packet_enum: STRING • k3z_dhcp_v6_packets_ received_sec: INTEGER • k3z_dhcp_v6_packets_ received_sec_enum: STRING • k3z_dhcp_v6_releases_ sec: INTEGER • k3z_dhcp_v6_releases_ sec_enum: STRING • k3z_dhcp_v6_rebinds_ sec: INTEGER • k3z_dhcp_v6_rebinds_ sec_enum: STRING • k3z_dhcp_v6_confirms_ sec: INTEGER • k3z_dhcp_v6_confirms_ sec_enum: STRING • k3z_dhcp_v6_renews_ sec: INTEGER • k3z_dhcp_v6_renews_ sec_enum: STRING • k3z_dhcp_v6_advertises_ sec: INTEGER • k3z_dhcp_v6_advertises_ sec_enum: STRING • k3z_dhcp_v6_solicits_sec: INTEGER • k3z_dhcp_v6_solicits_ sec_enum: STRING

Table 27. 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 • k3z_ds_pct_writes_from_ ntdsapi: INTEGER • k3z_ds_pct_writes_from_ ntdsapi_enum: STRING • k3z_ds_pct_searches_from_ ntdsapi: INTEGER • k3z_ds_pct_searches_from_ ntdsapi_enum: STRING • k3z_ds_pct_reads_from_ ntdsapi: INTEGER • k3z_ds_pct_reads_from_ ntdsapi_enum: STRING

Table 27. 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

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DNS (continued)	ITM_DNS event class with these slots: • 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_ 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 • k3z_dns_axfr_request_ received: INTEGER • k3z_dns_axfr_request_ sent: INTEGER • k3z_dns_axfr_response_ received: INTEGER • k3z_dns_axfr_success_ received: INTEGER • k3z_dns_axfr_success_ sent: INTEGER • k3z_dns_database_node_ memory_kb: INTEGER • k3z_dns_dynamic_update_ nooperation: INTEGER • k3z_dns_dynamic_update_ nooperation_sec: INTEGER • k3z_dns_dynamic_update_ written_database: INTEGER • k3z_dns_dynamic_update_ written_database_sec: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DNS (continued)	ITM_DNS event class with these slots: • k3z_dns_ixfr_request_ received: INTEGER • k3z_dns_ixfr_request_ sent: INTEGER • k3z_dns_ixfr_response_ received: INTEGER • k3z_dns_ixfr_success_ received: INTEGER • k3z_dns_ixfr_success_ sent: INTEGER • k3z_dns_ixfr_tcp_success_ received: INTEGER • k3z_dns_ixfr_udp_success_ received: INTEGER • k3z_dns_nbstat_memory_kb: INTEGER • k3z_dns_notify_received: INTEGER • k3z_dns_notify_sent: INTEGER • k3z_dns_record_flow_ memory_kb: INTEGER • k3z_dns_recursive_queries: INTEGER • k3z_dns_recursive_ queries_sec: INTEGER • k3z_dns_recursive_ query_failure: INTEGER • k3z_dns_recursive_ query_failure_sec: INTEGER • k3z_dns_recursive_ send_timeouts: INTEGER • k3z_dns_recursive_ timeout_sec: INTEGER • k3z_dns_secure_update_ failure: INTEGER • k3z_dns_secure_update_ received: INTEGER • k3z_dns_secure_update_ received_sec: INTEGER • k3z_dns_tcp_message_ memory_kb: INTEGER • k3z_dns_tcp_query_ received: INTEGER • k3z_dns_tcp_query_ received_sec: INTEGER • k3z_dns_tcp_response_ sent: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
DNS (continued)	ITM_DNS event class with these slots: • k3z_dns_tcp_response_ sent_sec: INTEGER • k3z_dns_udp_message_ memory_kb: INTEGER • k3z_dns_udp_query_ received: INTEGER • k3z_dns_udp_query_ received_sec: INTEGER • k3z_dns_udp_response_ sent: INTEGER • k3z_dns_udp_response_ sent_sec: INTEGER • k3z_dns_wins_lookup_ received: INTEGER • k3z_dns_wins_lookup_ received_sec: INTEGER • k3z_dns_wins_response_ sent: INTEGER • k3z_dns_wins_response_ sent_sec: INTEGER • k3z_dns_wins_reverse_ lookup_received: INTEGER • k3z_dns_wins_reverse_lookup_ received_sec: INTEGER • k3z_dns_wins_reverse_response_ sent: INTEGER • k3z_dns_wins_reverse_response_ sent_sec: INTEGER • k3z_dns_zone_transfer_soa_ request_sent: INTEGER • k3z_dns_is_read_ only: INTEGER

Table 27. 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

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Domain_Controller_Availability (continued)	ITM_Domain_Controller_Availability event class with these slots: • 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 • k3z_dca_global_catalog_ server: STRING • k3z_dca_global_catalog_ server_enum: STRING • k3z_dca_dcs_in_site: INTEGER • k3z_dca_time_difference: REAL • k3z_dca_time_difference_ enum: STRING • k3z_dca_time_server_ name: STRING • k3z_dca_time_server_name_ enum: STRING • k3z_dca_time_server_ type: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Domain_Controller_Availability (continued)	ITM_Domain_Controller_Availability event class with these slots: • k3z_dca_time_server_type_ enum: STRING • k3z_dca_bind_pdc_master: INTEGER • k3z_dca_bind_pdc_master_ enum: STRING • k3z_dca_bind_domain_ naming_master: INTEGER • k3z_dca_bind_domain_ naming_master_enum: STRING • k3z_dca_bind_rid_master: INTEGER • k3z_dca_bind_rid_ master_enum: STRING • k3z_dca_bind_schema_ master: INTEGER • k3z_dca_bind_schema_ master_enum: STRING • k3z_dca_bind_infrastructure_ master: INTEGER • k3z_dca_bind_infrastructure_ master_enum: STRING • k3z_dca_gcs_in_ site_bind: INTEGER • k3z_dca_gcs_bind: INTEGER • k3z_dca_ping_rid_master_ enum: STRING • k3z_dca_ping_domain_naming_ master_enum: STRING • k3z_dca_ping_infrastructure_master _enum: STRING • k3z_dca_ping_schema_master _enum: STRING • k3z_dca_ping_pdc_master _enum: STRING • k3z_dca_time_difference _v630: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Domain_Controller_Availability (continued)	ITM_Domain_Controller_Availability event class with these slots: • k3z_dca_time_difference _v630_enum: STRING • k3z_dca_pdc_master_bind _time: INTEGER • k3z_dca_pdc_master_bind _time_enum: STRING • k3z_dca_domain_naming _master_bind_time: INTEGER • k3z_dca_domain_naming_ master_bind_time_enum: STRING • k3z_dca_rid_master_bind _time: INTEGER • k3z_dca_rid_master_bind _time_enum: STRING • k3z_dca_schema_master _bind_time: INTEGER • k3z_dca_schema_master_ bind_time_enum: STRING • k3z_dca_infrastructure_ master_bind_time: INTEGER • k3z_dca_infrastructure_master _bind_time_enum: STRING • k3z_dca_hostname_v630: STRING

Table 27. 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 • k3z_dcp_log_writes_sec: INTEGER • k3z_dcp_table_opens_sec: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Domain_Controller_Performance (continued)	ITM_Domain_Controller_Performance event class with these slots: • k3z_dcp_pages_converted_sec: INTEGER • k3z_dcp_pages_converted_ sec_enum: STRING • k3z_dcp_pages_converted: INTEGER • k3z_dcp_pages_converted_ enum: STRING • k3z_dcp_records_converted_sec: INTEGER • k3z_dcp_records_converted_ sec_enum: STRING • k3z_dcp_records_converted: INTEGER • k3z_dcp_records_converted_ enum: STRING • k3z_dcp_sessions_in_use: INTEGER • k3z_dcp_sessions_in_use_ enum: STRING • k3z_dcp_sessions_percent_used: INTEGER • k3z_dcp_sessions_percent_ used_enum: STRING • k3z_dcp_log_bytes_write_sec: INTEGER • k3z_dcp_log_bytes_write_ sec_enum: STRING • k3z_dcp_version_buckets_ allocated: INTEGER • k3z_dcp_version_buckets_ allocated_enum: STRING • k3z_dcp_db_page_evictions _sec: INTEGER • k3z_dcp_db_page_eviction s_sec_enum: STRING • k3z_dcp_io_db_reads_sec: INTEGER • k3z_dcp_io_db_reads_sec _enum: STRING • k3z_dcp_io_db_reads_average _latency: INTEGER • k3z_dcp_io_db_reads_average_ latency_enum: STRING • k3z_dcp_io_log_reads_sec: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Exchange_Directory_Services	ITM_Exchange_Directory_Services event class with these slots: • k3z_dcp_io_log_reads_ sec_enum: STRING • k3z_dcp_io_db_writes_sec: INTEGER • k3z_dcp_io_db_writes_sec_enum: STRING • k3z_dcp_io_db_writes_ average_latency: INTEGER • k3z_dcp_io_db_writes_average_ latency_enum: STRING • k3z_dcp_io_log_writes_ sec: INTEGER • k3z_dcp_io_log_writes_ sec_enum: STRING • k3z_dcp_io_log_writes_ average_latency: INTEGER • k3z_dcp_io_log_writes_average_ latency_enum: STRING • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_xds_client_ sessions: INTEGER • k3z_xds_client_ sessions_enum: STRING • k3z_xds_reads: INTEGER • k3z_xds_reads_enum: STRING • k3z_xds_searches: INTEGER • k3z_xds_searches_enum: STRING • k3z_xds_writes: INTEGER • k3z_xds_writes_enum: STRING

Table 27. 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 • k3z_frs_authentications: INTEGER • k3z_frs_authentications_in_error: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
File_Replication_Service (continued)	ITM_File_Replication_Service event class with these slots: • k3z_frs_bindings: INTEGER • k3z_frs_bindings_in_error: INTEGER • k3z_frs_bytes_of_files_ installed: INTEGER • k3z_frs_kb_of_staging_fetched: INTEGER • k3z_frs_kb_of_staging_ generated: INTEGER • k3z_frs_kb_of_staging_ regenerated: INTEGER • k3z_frs_change_orders_ issued: INTEGER • k3z_frs_change_orders_ propagated: INTEGER • k3z_frs_change_orders_ retried: INTEGER • k3z_frs_change_orders_ retried_fetch: INTEGER • k3z_frs_change_orders_ retried_generate: INTEGER • k3z_frs_change_orders_ retried_at_install: INTEGER • k3z_frs_change_orders_ retried_rename: INTEGER • k3z_frs_communication_ timeouts: INTEGER • k3z_frs_ds_objects: INTEGER • k3z_frs_ds_objects_in_error: INTEGER • k3z_frs_ds_polls: INTEGER • k3z_frs_ds_polls_with_changes: INTEGER • k3z_frs_ds_polls_without_ changes: INTEGER • k3z_frs_ds_searches: INTEGER • k3z_frs_ds_searches_ in_error: INTEGER • k3z_frs_fetch_blocks_ received: INTEGER • k3z_frs_fetch_blocks_ received_kb: INTEGER • k3z_frs_fetch_blocks_ sent: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
File_Replication_Service (continued)	ITM_File_Replication_Service event class with these slots: • k3z_frs_fetch_blocks_ sent_kb: INTEGER • k3z_frs_fetch_requests_ received: INTEGER • k3z_frs_fetch_requests_ sent: INTEGER • k3z_frs_inbound_change_ orders_dampened: INTEGER • k3z_frs_join_notifications_ received: INTEGER • k3z_frs_join_notifications_sent: INTEGER • k3z_frs_joins: INTEGER • k3z_frs_outbound_change_ orders_dampened: INTEGER • k3z_frs_replica_sets_ created: INTEGER • k3z_frs_replica_sets_ deleted: INTEGER • k3z_frs_replica_sets_ removed: INTEGER • k3z_frs_replica_sets_ started: INTEGER • k3z_frs_staging_files_ fetched: INTEGER • k3z_frs_staging_files_ generated: INTEGER • k3z_frs_staging_files_ generated_with_error: INTEGER • k3z_frs_staging_files_ regenerated: INTEGER • k3z_frs_threads_exited: INTEGER • k3z_frs_threads_started: INTEGER • k3z_frs_unjoins: INTEGER • k3z_frs_usn_reads: INTEGER • k3z_frs_usn_records_ examined: INTEGER • k3z_frs_usn_records_ rejected: INTEGER

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Forest Topology	ITM_Forest_Topology event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_frt_dns_host_name: STRING • k3z_frt_dns_domain_ name: STRING • k3z_frt_distinguished_name: STRING • k3z_frt_site_name: STRING • k3z_frt_common_ name: STRING • k3z_frt_is_readonly_dc: STRING • k3z_frt_is_readonly_ dc_enum: STRING • k3z_frt_parent_domain: STRING • k3z_frt_ldap_distinguished_ name: STRING
GPO	ITM_GPO event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_gpo_name: STRING • k3z_gpo_guid: STRING • k3z_gpo_sysvol_ version: INTEGER • k3z_gpo_sysvol_ version_enum: STRING • k3z_gpo_version: INTEGER • k3z_gpo_status: INTEGER • k3z_gpo_status_ enum: STRING • k3z_gpo_creation_ time: STRING • k3z_gpo_modification_ time: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
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 • k3z_kcc_inter_site_ topology_generator: INTEGER • k3z_kcc_inter_site_topology _generator_enum: STRING • k3z_kcc_site_name: STRING • k3z_kcc_inter_site_topology _generator_server: STRING • k3z_kcc_inter_site_topology _generator_server_enum: STRING
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

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Lightweight Directory Access Protocol	ITM_Lightweight_Directory_Access_Protocol event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • 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_enum: STRING • k3z_ldap_successful_ binds_per_sec: INTEGER • k3z_ldap_udp_operations_ per_sec: INTEGER • k3z_ldap_writes: INTEGER • k3z_ldap_writes_per_sec: INTEGER • k3z_ldap_atq_threads_ldap: INTEGER • k3z_ldap_atq_threads_ ldap_enum: STRING • k3z_ldap_new_connections_sec: INTEGER • k3z_ldap_new_connections_ sec_enum: STRING • k3z_ldap_closed_connections_ sec: INTEGER • k3z_ldap_closed_connections_ sec_enum: STRING • k3z_ldap_new_ssl_connections_sec: INTEGER • k3z_ldap_new_ssl_connections_ sec_enum: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
LDAP Attributes	ITM_LDAP_Attributes event class with these slots: • k3z_ldap_attributes_recycle_ bin_status: INTEGER • k3z_ldap_attributes_offline_ domain_join: INTEGER • k3z_ldap_attributes_users_ locked: INTEGER • k3z_ldap_attributes_objects_ in_domain: INTEGER • timestamp: STRING • server_name: STRING • parameter: STRING • k3z_value: STRING • k3z_ldap_attributes_recycle_bin _status_enum: STRING • k3z_ldap_attributes_offline_ domain_join_enum: STRING • k3z_ldap_attributes_disabled_ user_accounts: INTEGER • k3z_ldap_attributes_disabled_ user_accounts_enum: STRING • k3z_ldap_attributes_expired_ user_accounts: INTEGER • k3z_ldap_attributes_expired_ user_accounts_enum: STRING • k3z_ldap_attributes_expired_ password_user_accounts: INTEGER • k3z_ldap_attributes_expired_ password_user_accounts_enum: STRING • k3z_ldap_attributes_inactive_ user_accounts: INTEGER • k3z_ldap_attributes_inactive_ user_accounts_enum: STRING • k3z_ldap_attributes_invalid_logon_ attempts_user_accounts: INTEGER • k3z_ldap_attributes_invalid_logon_ attempts_user_accounts_enum: STRING • k3z_ldap_attributes_new_ user_accounts: INTEGER • k3z_ldap_attributes_new_ user_accounts_enum: STRING
LFO	ITM_LFO event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_lfo_name: STRING • k3z_lfo_type: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
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 27. 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

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Replication (continued)	ITM_Replication event class with these slots: • 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 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Replication (continued)	ITM_Replication event class with these slots: • k3z_dra_sync_failures_on_schema_mismatch: INTEGER • k3z_dra_inbound_kbytes_total_ since_boot: INTEGER • k3z_dra_inbound_kbytes_total_ since_boot_enum: STRING • k3z_dra_inbound_kbytes_not_compressed_ since_boot: INTEGER • k3z_dra_inbound_kbytes_not_compressed_ since_boot_enum: STRING • k3z_dra_inbound_kbytes_compressed_ since_boot_before: INTEGER • k3z_dra_inbound_kbytes_compressed_ since_boot_before_enum: STRING • k3z_dra_inbound_kbytes_compressed_ since_boot_after: INTEGER • k3z_dra_inbound_kbytes_compressed_ since_boot_after_enum: STRING • k3z_dra_outbound_kbytes_total_ since_boot: INTEGER • k3z_dra_outbound_kbytes_total_ since_boot_enum: STRING • k3z_dra_outbound_kbytes_not_compressed_ since_boot: INTEGER • k3z_dra_outbound_kbytes_not_compressed_ since_boot_enum: STRING • k3z_dra_outbound_kbytes_compressed_ since_boot_before: INTEGER • k3z_dra_outbound_kbytes_compressed_ since_boot_before_enum: STRING • k3z_dra_outbound_kbytes_compressed_ since_boot_after: INTEGER • k3z_dra_outbound_kbytes_compressed_ since_boot_after_enum: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Replication (continued)	ITM_Replication event class with these slots: • k3z_dra_pending_replication_ operations: INTEGER • k3z_dra_pending_replication_ operations_enum: STRING • k3z_dra_threads_getting_nc_ changes: INTEGER • k3z_dra_threads_getting_nc_ changes_enum: STRING • k3z_dra_threads_getting_nc_ changes_holding_semaphore: INTEGER • k3z_dra_threads_getting_nc_ changes_holding_semaphore_enum: STRING • k3z_dra_inbound_link_value_ updates_remaining_in_packet: INTEGER • k3z_dra_inbound_link_value_ updates_remaining_in_packet_enum: STRING • k3z_dra_inbound_total_updates_ remaining_in_packet: INTEGER • k3z_dra_inbound_total_updates_ remaining_in_packet_enum: STRING • k3z_dra_inbound_total_connections: INTEGER • k3z_dra_outbound_total_connections: INTEGER • k3z_dra_outbound_connections: INTEGER
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 • k3z_rpl_fail_reason_text_v623: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Replication_Partner_Latency	ITM_Replication_Partner_Latency event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_rlt_partner_name: STRING • k3z_rlt_partner_site_name: STRING • k3z_rlt_clock_delta: INTEGER • k3z_rlt_replication_latency: INTEGER • k3z_rlt_replication_latency_enum: STRING • k3z_rlt_clock_change_delta: INTEGER • k3z_rlt_hostname: STRING • k3z_rlt_partner_fqdn: STRING
Root Directory Server	ITM_Root_Directory_Server event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_rds_root_domain_name: STRING • k3z_rds_domain_controller_ functionality: INTEGER • k3z_rds_domain_controller_ functionality_enum: STRING • k3z_rds_domain_functionality: INTEGER • k3z_rds_domain_functionality_enum: STRING • k3z_rds_forest_functionality: INTEGER • k3z_rds_forest_functionality_ enum: STRING • k3z_rds_root_fqdn: STRING

Table 27. 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 • k3z_sam_domain_local_group_membership_ evaluations_sec: INTEGER • k3z_sam_domain_local_group_membership_ evaluations_sec_enum: STRING • k3z_sam_resource_group_ evaluation_latency: INTEGER • k3z_sam_resource_group_ evaluation_latency_enum: STRING

Table 27. 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 • server_name: STRING • timestamp: STRING • k3z_sysrpl_partner_name: STRING • k3z_sysrpl_replication_result: INTEGER • k3z_sysrpl_replication_ result_enum: STRING • k3z_sysrpl_replication_ test_start_time: STRING • k3z_sysrpl_replication_ test_verification_time: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Trust	ITM_Trust event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • k3z_value: STRING • k3z_trust_netbios_name: STRING • k3z_trust_netbios_name_enum: STRING • k3z_trust_domain_name: STRING • k3z_trust_domain_name_enum: STRING • k3z_trust_direction: STRING • k3z_trust_direction_enum: STRING • k3z_trust_type: STRING • k3z_trust_type_enum: STRING • k3z_trust_status: STRING • k3z_trust_status_enum: STRING • k3z_trust_added: STRING • k3z_trust_added_enum: STRING • k3z_trust_dropped: STRING • k3z_trust_dropped_enum: STRING • k3z_trust_local_domain: STRING • k3z_trust_hostname: STRING
Trust Topology	ITM_Trust_Topology event class with these slots: • server_name: STRING • timestamp: STRING • k3z_trust_topology_domain_name: STRING • k3z_trust_topology_domain_ name_enum: STRING • k3z_trust_topology_trust_from: STRING • k3z_trust_topology_trust_type: STRING • k3z_trust_topology_trust_type_enum: STRING • k3z_trust_topology_trust_direction: STRING • k3z_trust_topology_trust_direction_enum: STRING • k3z_trust_topology_trust_relation: STRING • k3z_trust_topology_trust_relation_enum: STRING
Sysvol Replication	ITM_Sysvol_Replication event class with these slots: • server_name: STRING • timestamp: STRING • k3z_sysrpl_partner_name: STRING • k3z_sysrpl_replication_result: INTEGER • k3z_sysrpl_replication_result_enum: STRING • k3z_sysrpl_replication_test_start_time: STRING • k3z_sysrpl_replication_test_verification_time: STRING

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Event Log	ITM_Event_Log event class with these slots: • server_name: STRING • timestamp: STRING • k3z_evtlog__log_name: STRING; • k3z_evtlog_source: STRING • k3z_evtlog_type: INTEGER • k3z_evtlog_type_enum: STRING • k3z_evtlog_event_id: INTEGER • k3z_evtlog_category: STRING • k3z_evtlog_user: STRING • k3z_evtlog_description: STRING • k3z_evtlog_event_timestamp: STRING
Active Directory Database Information	ITM_Active_Directory_Database_Information event class with these slots: • server_name: STRING • timestamp: STRING • k3z_addb_database_file_path: STRING • k3z_addb_database_file_size: REAL • k3z_addb_database_file_size_enum: STRING • k3z_addb_available_disk_space_for_database: REAL • k3z_addb_database_log_file_path: STRING • k3z_addb_database_log_file_size: REAL • k3z_addb_database_log_file_size_enum: STRING • k3z_addb_available_disk_space_for_log_files: REAL • k3z_addb_percentage_free_disk_space _for_database: REAL • k3z_addb_percentage_free_disk_space _for_database_enum: STRING • k3z_addb_percentage_free_disk_space _for_log_files: REAL • k3z_addb_percentage_free_disk_space _for_log_files_enum: STRING
Conflict Objects	ITM_Conflict_Objects event class with these slots: • server_name: STRING • timestamp: STRING • k3z_cnfobj_common_name: STRING • k3z_cnfobj_distinguished_name: STRING • k3z_cnfobj_object_category: STRING • k3z_cnfobj_ads_path:STRING • k3z_cnfobj_created_timestamp: STRING • k3z_cnfobj_changed_timestamp: STRING;

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Moved Or Deleted Organizational Unit	ITM_Moved_Or_Deleted_Organizational_Unit event class with these slots: • server_name: STRING • timestamp: STRING • k3z_ou_collection_timestamp: STRING • k3z_ou_name: STRING • k3z_ou_current_distinguished_name: STRING • k3z_ou_current_distinguished_name_enum: STRING • k3z_ou_previous_distinguished_name: STRING • k3z_ou_status: INTEGER • k3z_ou_status_enum: STRING
RID Pool Information	ITM_RID_Pool_Information event class with these slots: • server_name: STRING • timestamp: STRING • k3z_rid_master: STRING • k3z_available_rid: INTEGER • k3z_exhausted_rid: INTEGER • k3z_rid_allocation_pool_start: INTEGER • k3z_rid_allocation_pool_end: INTEGER • k3z_next_rid: INTEGER • k3z_rid_previous_allocation_pool_start: INTEGER • k3z_rid_previous_allocation_pool_end: INTEGER • k3z_rid_rid_block_size: INTEGER • k3z_rid_rid_block_size_enum: STRING • k3z_rid_rid_pool_allocation_status: INTEGER • k3z_rid_rid_pool_allocation_status_enum: STRING • k3z_exhausted_rid_percentage: REAL;
Netlogon Attributes	ITM_NETLOGON_Attributes event class with these slots: • server_name: STRING • timestamp: STRING • k3z_ntlgon_instance_name: STRING • k3z_ntlgon_semaphore_waiters: INTEGER • k3z_ntlgon_semaphore_holders: INTEGER • k3z_ntlgon_semaphore_timeout: INTEGER • k3z_ntlgon_semaphore_acquires: INTEGER • k3z_ntlgon_average_semaphore_hold_time: INTEGER;

Table 27. Overview of attribute groups to event classes and slots (continued)

Attribute group	Event class and slots
Password Setting Objects	ITM_Password_Setting_Objects event class with these slots: • server_name: STRING • timestamp: STRING • k3z_pso_name: STRING • k3z_enforce_password_history: INTEGER • k3z_enforce_password_history_enum: STRING • k3z_minimum_password_length: INTEGER • k3z_minimum_password_length_enum: STRING • k3z_password_complexity_enabled: INTEGER • k3z_password_complexity_enabled_enum: STRING • k3z_password_reversible_encryption_enabled: INTEGER • k3z_password_reversible_encryption_enabled_enum: STRING • k3z_lockout_threshold: INTEGER • k3z_lockout_threshold_enum: STRING • k3z_account_lockout_duration: INTEGER • k3z_account_lockout_duration_enum: STRING • k3z_lockout_observation_window: INTEGER • k3z_lockout_observation_window_enum: STRING • k3z_minimum_password_age: INTEGER • k3z_minimum_password_age_enum: STRING • k3z_maximum_password_age: INTEGER • k3z_maximum_password_age_enum: STRING • k3z_when_created: STRING • k3z_when_changed: STRING;

Appendix C. Discovery Library Adapter for the Microsoft Active Directory agent

The Tivoli Management Services Discovery Library Adapter (DLA) discovers resources and relationships, and creates a Discovery Library Book file for the agent.

About the DLA

The Book file follows the Discovery Library IdML schema and is used to populate the Configuration Management Database (CMDB) and Tivoli Business Service Manager products. The Tivoli Management Services DLA discovers Active Directory resources. For all VMware systems that are active and online at the Tivoli Enterprise Portal Server, information is included in the discovery book for those resources. The Tivoli Management Services DLA discovers active resources. It is run on demand and can be run periodically to discover resources that were not active during previous discoveries.

The DLA discovers Active Directory components.

More information about DLAs

The following sources contain additional information about using the DLA program with all monitoring agents:

- The *IBM Tivoli Monitoring Administrator's Guide* contains information about using the Tivoli Management Services Discovery Library Adapter.
- For information about using a DLA with Tivoli Application Dependency Discovery Manager (TADDM), see the TADDM Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.taddm.doc_7.2/welcome_page/welcome.html).

DLA data model class types represented in CDM

The source application data objects map to classes in the Common Data Model (CDM) for the Microsoft Active Directory agent.

The following information is provided for each class:

CDM class name
Class name for which the agent is providing information

Relationships
CDM relationships (hierarchical) between currently identified model objects

CDM attributes, agent attributes, descriptions, and examples
CDM and agent attributes that are required to create an instance of a resource, descriptions of the attributes, and examples of the attributes

DLA data model classes for Microsoft Active Directory agent

Each agent that uses the Discovery Library Adapter has DLA data model classes defined for the agent.

The Microsoft Active Directory agent has the following Discovery Library Adapter data model classes:

- ActiveDirectory
- ServiceAccessPoint
- BindAddress
- IpAddress

ActiveDirectory class

The ActiveDirectory class represents an instance of the domain controller.

CDM class name

sys.ActiveDirectory

Relationships

provides

- Source: sys.ComputerSystem
- Target: sys.ActiveDirectoryDomain
- Example: 10.77.88.99-ComputerSystem provides IBM001:3Z-ActiveDirectory

bindsTo

- Source: net.BindAddress
- Target: net.IpAddress
- Example: 10.77.88.99-389-BindAddress bindsTo 10.77.88.99-IpAddress

accessedVia

- Source: sys.ServiceAccessPoint
- Target: net.BindAddress
- Example: IBM001:3Z-10.77.88.99-ServiceAccessPoint accessedVia 10.77.88.99-389-BindAddress

accessedVia

- Source: sys.ActiveDirectory
- Target: sys.ServiceAccessPoint
- Example: IBM001:3Z-ActiveDirectory accessedVia IBM001:3Z-10.77.88.99-ServiceAccessPoint

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: ManagedSystemName
  Agent attribute: MSYSN
  Description: The name of the managed system.
  Example: IBM 0123
- CDM attribute: Name
  Agent attribute: None
  Description: The name of the domain controller.
  Example: Microsoft Active Directory

ServiceAccessPoint class

The ServiceAccessPoint class represents the instance of the services that are used by the Microsoft Active Directory.

CDM class name

sys.ServiceAccessPoint

Relationships

provides

- Source: `sys.ComputerSystem`
- Target: `sys.ActiveDirectoryDomain`
- Example: `10.77.88.99-ComputerSystem provides IBM001:3Z-ActiveDirectory`

bindsTo

- Source: `net.BindAddress`
- Target: `net.IpAddress`
- Example: `10.77.88.99-389-BindAddress bindsTo 10.77.88.99-IpAddress`

accessedVia

- Source: `sys.ServiceAccessPoint`
- Target: `net.BindAddress`
- Example: `IBM001:3Z-10.77.88.99-ServiceAccessPoint accessedVia 10.77.88.99-389-BindAddress`

accessedVia

- Source: `sys.ActiveDirectory`
- Target: `sys.ServiceAccessPoint`
- Example: `IBM001:3Z-ActiveDirectory accessedVia IBM001:3Z-10.77.88.99-ServiceAccessPoint`

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: Name
  Agent attribute: None
  Description: The name of the service access point.
  Example: `Microsoft Active Directory`
- CDM attribute: ProductName
  Agent attribute: None
  Description: The name of the product.
  Example: `Microsoft Active Directory`
- CDM attribute: VendorName
  Agent attribute: None
  Description: The name of the vendor.
  Example: `Microsoft`
- CDM attribute: ProductVersion
  Agent attribute: None
  Description: The version of the product.
  Example: `1.0`

BindAddress class

The BindAddress class represents an IP protocol endpoint on which a service is provided.

CDM class name

net.BindAddress

Relationships

provides

- Source: `sys.ComputerSystem`
- Target: `sys.ActiveDirectoryDomain`

- Example: 10.77.88.99-ComputerSystem provides IBM001:3Z-ActiveDirectory

bindsTo

- Source: net.BindAddress
- Target: net.IpAddress
- Example: 10.77.88.99-389-BindAddress bindsTo 10.77.88.99-IpAddress

accessedVia

- Source: sys.ServiceAccessPoint
- Target: net.BindAddress
- Example: IBM001:3Z-10.77.88.99-ServiceAccessPoint accessedVia 10.77.88.99-389-BindAddress

accessedVia

- Source: sys.ActiveDirectory
- Target: sys.ServiceAccessPoint
- Example: IBM001:3Z-ActiveDirectory accessedVia IBM001:3Z-10.77.88.99-ServiceAccessPoint

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: Name
  Agent attribute: None
  Description: The name of the IP protocol endpoint.
  Example: Microsoft Active Directory
- CDM attribute: PortNumber
  Agent attribute: None
  Description: The port number.
  Example: 389
- CDM attribute: Path
  Agent attribute: None
  Description: The path of the service.
  Example: C:\windows\system32\lsass.exe

IpAddress class

The IpAddress class represents the instance of an IP address.

CDM class name

net.IpAddress

Relationships

provides

- Source: sys.ComputerSystem
- Target: sys.ActiveDirectoryDomain
- Example: 10.77.88.99-ComputerSystem provides IBM001:3Z-ActiveDirectory

bindsTo

- Source: net.BindAddress
- Target: net.IpAddress
- Example: 10.77.88.99-389-BindAddress bindsTo 10.77.88.99-IpAddress

accessedVia

- Source: sys.ServiceAccessPoint

- Target: `net.BindAddress`
- Example: `IBM001:3Z-10.77.88.99-ServiceAccessPoint accessedVia 10.77.88.99-389-BindAddress`

accessedVia

- Source: `sys.ActiveDirectory`
- Target: `sys.ServiceAccessPoint`
- Example: `IBM001:3Z-ActiveDirectory accessedVia IBM001:3Z-10.77.88.99-ServiceAccessPoint`

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: StringNotation
  Agent attribute: IPADDR
  Description: The IP address of the managed system.
  Example: `10.77.88.99`

Appendix D. Integration with Tivoli Business Service Manager

Microsoft Active Directory agent provides data to create, update the status of, and view IBM Tivoli Business Service Manager services.

The Tivoli Management Services Discovery Library Adapter (DLA) and Discovery Library Toolkit provides data for the Tivoli Business Service Manager service models. The Tivoli Integration Facility (EIF) probe updates the status of these services, and you use the Tivoli Enterprise Portal to view the data for the services. To implement the integration of the agent with Tivoli Business Service Manager, perform the integration tasks.

Components for integrating with Tivoli Business Service Manager

The data for integrating with Tivoli Business Service Manager is supplied through the following components: Tivoli Management Services Discovery Library Adapter (DLA) and Discovery Library Toolkit, Tivoli Event Integration Facility (EIF) probe, and Tivoli Enterprise Portal Server.

Tivoli Management Services Discovery Library Adapter (DLA) and Discovery Library Toolkit

By using data from the Tivoli Management Services Discovery Library Adapter, you can build Tivoli Business Service Manager service models that include resources monitored by the Active Directory.

The DLA files can be imported directly into Tivoli Business Service Manager using the Discovery Library Toolkit or they can be loaded into IBM Tivoli Application Dependency Discovery Manager (TADDM) and then fed into Tivoli Business Service Manager using the Discovery Library Toolkit.

See the following sources for more information about the DLA and Discovery Library Toolkit:

- Resources and relationships that are discovered by the Active Directory and included in Tivoli Management Services DLA files: "DLA data model classes for Microsoft Active Directory agent" on page 227
- Using the Tivoli Management Services DLA: *IBM Tivoli Monitoring Administrator's Guide*
- Using the Discovery Library Toolkit: *Tivoli Business Service Manager Customization Guide*

Tivoli Event Integration Facility (EIF) probe

Situation events detected by the Active Directory can update the status of services in Tivoli Business Service Manager.

The situation events are forwarded from IBM Tivoli Monitoring to the Netcool/OMNIbus Probe for the Tivoli Event Integration Facility. The Active Directory provides a probe rules file that updates its events with information to identify the affected service in Tivoli Business Service Manager. The EIF probe then

forwards the events to the Netcool/OMNIbus ObjectServer. Tivoli Business Service Manager monitors the Netcool/OMNIbus ObjectServer for new events and updates the status of affected services.

See the following sources for more information about event integration:

- Installation (using an existing EIF probe and Netcool/OMNIbus ObjectServer installation or using Tivoli Business Service Manager to install these components): Netcool/OMNIbus Information Center or the *Tivoli Business Service Manager Installation Guide*.
- Setting up event integration between IBM Tivoli Monitoring, the EIF probe, and the Netcool/OMNIbus ObjectServer: *IBM Tivoli Monitoring Installation and Setup Guide*.
- Configuring the EIF probe to use the Active Directory rules file after the EIF probe has been installed and configured for event integration with IBM Tivoli Monitoring: "Configuring the Tivoli Event Integration Facility (EIF) probe to enrich events" on page 235

Tivoli Enterprise Portal

You can use the integration of the Tivoli Enterprise Portal Server with Tivoli Business Service Manager to view the services in the Tivoli Business Service Manager console.

For more detailed examination and analysis, you can easily link from the Tivoli Business Service Manager console to the Tivoli Enterprise Portal Server to view the data within the Active Directory.

Tasks to integrate the agent with Tivoli Business Service Manager

To integrate the Microsoft Active Directory agent with Tivoli Business Service Manager, you must install and configure the required components. Then, you can view the data in the Tivoli Enterprise Portal.

To integrate the Microsoft Active Directory agent with Tivoli Business Service Manager and view the data, complete the following tasks:

- Install the Discovery Library Toolkit on theTivoli Business Service Manager server.
- Configure the Tivoli Event Integration Facility (EIF) probe to enrich Microsoft Active Directory agent events.
- Create a service in the Tivoli Business Service Manager console that you want to monitor.
- Create a data source mapping for each data source that you want to access within the Tivoli Business Service Manager.
- Configure an additional IBM Tivoli Monitoring web service for each Tivoli Enterprise Portal Server.
- View data in the Tivoli Enterprise Portal for the services that you have created to monitor through Tivoli Business Service Manager.

Installing the Discovery Library Toolkit on the Tivoli Business Service Manager

You must install the Discovery Library Toolkit on the Tivoli Business Service Manager server.

The Discovery Library Toolkit imports data from the DLA files and TADDM, which includes information about the hardware and the applications that are discovered by the source.

See "Installing the Discovery Library Toolkit" in the *Tivoli Business Service Manager Installation Guide*.

Configuring the Tivoli Event Integration Facility (EIF) probe to enrich events

The Netcool/OMNIbus Probe for Tivoli Event Integration Facility (EIF) forwards the Microsoft Active Directory agent events that are received from IBM Tivoli Monitoring to the Netcool/OMNIbus ObjectServer. Tivoli Business Service Manager monitors the Netcool/OMNIbus ObjectServer for new events, and updates the status of affected services. The Microsoft Active Directory agent provides a probe rules `include` file that updates its events with information to identify the affected service in Tivoli Business Service Manager.

Before you begin

Install and configure the Netcool/OMNIbus ObjectServer and EIF probe and set up event integration between IBM Tivoli Monitoring and Netcool/OMNIbus.

About this task

To enable event enrichment, configure the EIF probe to use the rules file for the agent.

Procedure

1. Locate the Microsoft Active Directory agent rules file (`k3z_tbsm.rules`) on a computer system where the Microsoft Active Directory agent, Tivoli Enterprise Monitoring Server, or Tivoli Enterprise Portal Server is installed. The file is in the following locations:
   - On Windows systems

     The file is in the *installdir*`\cms\TECLIB` directory of the monitoring server, in the *installdir*`\cnps\TECLIB` directory of the portal server, or in the *installdir*`\TMAITM6\EIFLIB` directory of the agent, where *installdir* is the IBM Tivoli Monitoring or ITCAM for Microsoft Applications installation directory.
   - On Linux and UNIX systems

     The file is in the *installdir*`/tables/`*cicatrsq*`/TECLIB` directory of the monitoring server or in the *installdir*`/`*platform*`/`*xx*`/TECLIB` directory of the agent, where *installdir* is the IBM Tivoli Monitoring or ITCAM for Microsoft Applications directory, *platform* is the architecture directory for the agent, and *xx* is the product code for the agent.
2. Copy the `k3z_tbsm.rules` file to the following directory on the computer system where the EIF probe is installed:
   - On Windows systems

     `%OMNIHOME%\probes\`*arch*
   - On UNIX systems

     `$OMNIHOME/probes/`*arch*

   Where:

OMNIHOME
System-defined variable defining the installation location of Netcool/OMNIbus

arch Operating system directory where the probe is installed; for example, solaris2 when running on a Solaris system, and win32 for a Windows system.

3. Edit the `tivoli_eif.rules` file and uncomment the `include` statement for `k3z_tbsm.rules`. (The `tivoli_eif.rules` file is located in the same directory as the `k3z_tbsm.rules` file.) If you are using a version of the `tivoli_eif.rules` file without an `include` statement for `k3z_tbsm.rules`, add the following line after the `include` statement for `itm_event.rules`:

   ```
   include "k3z_tbsm.rules"
   ```

4. Restart the EIF probe.

Creating a service in Tivoli Business Service Manager

You must create a service in the Tivoli Business Service Manager console for each service that you want to monitor.

To create the services that you want to monitor in the Tivoli Business Service Manager console, see "Configuring services" in the *IBM Tivoli Business Service Manager Service Configuration Guide*.

Creating a data source mapping for each data source

You can create a data source mapping for each data source that you want to access within Tivoli Business Service Manager.

Also, you can create the data fetchers and use the data to create incoming status rules that are populated in your service templates.

For more information, see "Data sources" and "Data fetchers" in the *IBM Tivoli Business Service Manager Service Configuration Guide*.

Configuring additional IBM Tivoli Monitoring web services

You can configure additional IBM Tivoli Monitoring web services for each Tivoli Enterprise Portal Server.

To configure an additional IBM Tivoli Monitoring web service for each Tivoli Enterprise Portal server, see "Configure TBSM charts" in the *IBM Tivoli Business Service Manager Scenarios Guide*.

Viewing data in the Tivoli Enterprise Portal

From Tivoli Business Service Manager, you can open the Tivoli Enterprise Portal and view the Microsoft Active Directory agent.

You can also launch Tivoli Business Service Manager from the Tivoli Enterprise Portal.

For more information about launching applications, see "Launching to and from applications" in the *Tivoli Business Service Manager Customization Guide*.

Appendix E. Documentation library

A variety of publications are relevant to the use of theIBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent.

The *IBM Tivoli Monitoring, OMEGAMON XE, and Composite Application Manager products: Documentation Guide* contains information about accessing and using publications. You can find the Documentation Guide in the following information centers:

- IBM Tivoli Monitoring and OMEGAMON XE (http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp)
- IBM Tivoli Composite Application Manager (http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp)

To open the Documentation Guide in the information center, select **Using the publications** in the **Contents** pane.

To find a list of new and changed publications, click **What's new in the information center** 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 versions** under the name of the product in the **Contents** pane.

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

The documentation for this agent and other product components is located in the IBM Tivoli Composite Application Manager for Microsoft Applications Information Center (http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamms.doc_6.3/welcome_msapps63.html).

One document is specific to the Microsoft Active Directory agent. The IBM Tivoli Composite Application Manager for Microsoft Applications: Microsoft Active Directory Agent User's Guide provides agent-specific information for configuring, using, and troubleshooting the Microsoft Active Directory agent.

The *Offering Guide* also provides information about installing and configuring the component products in the offering.

The **Prerequisites** topic in the information center contains information about the prerequisites for each component.

Use the information in the user's guide for the agent with the *Tivoli Enterprise Portal User's Guide* to monitor Active Directory resources.

Prerequisite publications

See the following publications to gain the required prerequisite knowledge:

- *IBM Tivoli Monitoring Troubleshooting Guide*
- *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*
- *IBM Tivoli Monitoring: Upgrading from V5.1.2*

- *IBM Tivoli Monitoring Universal Agent User's Guide*
- *IBM Tivoli Monitoring Universal Agent API and Command Programming Reference Guide*
- *Tivoli Enterprise Portal User's Guide*
- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring Agent Builder User's Guide*
- *IBM Tivoli Monitoring Command Reference*
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*
- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM(r) Tivoli(r) Monitoring High Availability Guide for Distributed Systems*
- *IBM Tivoli Monitoring: Messages*
- *IBM Tivoli Monitoring Troubleshooting Guide*
- *IBM Tivoli Monitoring Universal Agent User's Guide*
- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*
- *IBM Tivoli Monitoring: i5/OS Agent User's Guide*
- *IBM Tivoli Monitoring: Linux OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX Logs OS Agent User's*
- *IBM Tivoli Monitoring: Windows OS Agent User's Guide*
- *Tivoli Enterprise Portal User's Guide*
- *IBM(r) Tivoli(r) Performance Analyzer User's Guide*
- *IBM(r)Tivoli(r) Warehouse Proxy Agent User's Guide*
- *IBM(r)Tivoli(r) Warehouse Summarization and Pruning Agent User's Guide*

Related publications

The publications in related information centers provide useful information.

See the following information centers, which you can find by accessing Tivoli Documentation Central (http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home):

- IBM Tivoli Monitoring
- IBM Tivoli Netcool/OMNIbus
- IBM Tivoli Application Dependency Discovery Manager
- IBM Tivoli Enterprise Console

Other sources of documentation

See the following sources of technical documentation about monitoring products:

- Service Management Connect (SMC)

  See the introductory information about SMC (http://www.ibm.com/developerworks/servicemanagement/).

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

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

  - Become involved with transparent development, an ongoing, open engagement between external users and developers of Tivoli products where you can access early designs, sprint demos, product roadmaps, and pre-release code.
  - Connect one-on-one with the experts to collaborate and network about Tivoli and Integrated Service Management.
  - Benefit from the expertise and experience of others using blogs.
  - Collaborate with the broader user community using wikis and forums.
- IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary/) is an online catalog that contains integration documentation as well as other downloadable product extensions.
- IBM Redbook publications (http://www.redbooks.ibm.com/) include Redbooks® publications, Redpapers, and Redbooks technotes that provide information about products from platform and solution perspectives.
- Technotes (http://www.ibm.com/support/entry/portal/software), which are found through the IBM Software Support website, provide the latest information about known product limitations and workarounds.
- Tivoli wikis

  Tivoli Wiki Central (http://www.ibm.com/developerworks/wikis/display/tivoli/Home) is the home for interactive wikis that offer best practices and scenarios for using Tivoli products. The wikis contain white papers contributed by IBM employees, and content created by customers and business partners.

  Two of these wikis are of particular relevance to IBM Tivoli Monitoring:
  - Tivoli Distributed Monitoring and Application Management Wiki (http://www-10.lotus.com/ldd/tivmonitorwiki.nsf) provides information about IBM Tivoli Monitoring and related distributed products, including IBM Tivoli Composite Application Manager products.
  - Tivoli System z® Monitoring and Application Management Wiki (http://www.ibm.com/developerworks/wikis/display/tivoliomegamon/Home) provides information about the OMEGAMON XE products, Tivoli NetView® for z/OS, Tivoli Monitoring Agent for z/TPF, and other System z monitoring and application management products.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

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

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

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

Trademarks

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

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

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

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

Index

N

O

P

R

S

T

U

V

W

Product Number: 1234-SS1

Printed in USA

SC23-8879-07